Nous sommes déjà des cyborgs mais nous pouvons reprendre le contrôle

Avec un certain sens de la formule, Aral Balkan allie la sévérité des critiques et l'audace des propositions. Selon lui nos corps « augmentés » depuis longtemps font de nous des sujets de la surveillance généralisée maintenant que nos vies sont sous l'emprise démultipliée du numérique.

Selon lui, il nous reste cependant des perspectives et des pistes pour retrouver la maîtrise de notre « soi », mais elles impliquent, comme on le devine bien, une remise en cause politique de nos rapports aux GAFAM, une tout autre stratégie d'incitation aux entreprises du numérique de la part de la Communauté européenne, le financement d'alternatives éthiques, etc.

Ce qui suit est la version française d'un article qu'a écrit Aral pour le numéro 32 du magazine de la Kulturstiftung des Bundes (Fondation pour la culture de la République fédérale d'Allemagne). Vous pouvez également lire la version allemande.

Article original en anglais : Slavery 2.0 and how to avoid it : a practical guide for cyborgs

Traduction Framalang : goofy, jums, Fifi, MO, FranBAG, Radical Mass

L'esclavage 2.0 et comment y échapper : guide pratique pour les

cyborgs.

par Aral Balkan

Il est très probable que vous soyez un cyborg et que vous ne le sachiez même pas.

Vous avez un smartphone ?
Vous êtes un cyborg.
Vous utilisez un ordinateur ? Ou le Web ?
Cyborg !

En règle générale, si vous utilisez une technologie numérique et connectée aujourd'hui, vous êtes un cyborg. Pas besoin de vous faire greffer des microprocesseurs, ni de ressembler à Robocop. Vous êtes un cyborg parce qu'en utilisant des technologies vous augmentez vos capacités biologiques.

À la lecture de cette définition, vous pourriez marquer un temps d'arrêt : « Mais attendez, les êtres humains font ça depuis bien avant l'arrivée des technologies numériques ». Et vous auriez raison.

Nous étions des cyborgs bien avant que le premier bug ne vienne se glisser dans le premier tube électronique à vide du premier ordinateur central.

Galilée et sa lunette, tableau de Justus Sustermans, image via Wikimedia Commons (Public Domain]

L'homme des cavernes qui brandissait une lance et allumait un feu était le cyborg originel. Galilée contemplant les cieux avec son télescope était à la fois un homme de la Renaissance et un cyborg. Lorsque vous mettez vos lentilles de contact le matin, vous êtes un cyborg.

Tout au long de notre histoire en tant qu'espèce, la technologie a amélioré nos sens. Elle nous a permis une meilleure maîtrise et un meilleur contrôle sur nos propres vies et sur le monde qui nous entoure. Mais la technologie a tout autant été utilisée pour nous opprimer et nous exploiter, comme peut en témoigner quiconque a vu un jour de près le canon du fusil de l'oppresseur.

« La technologie », d'après la première loi de la technologie de Melvin Kranzberg, « n'est ni bonne ni mauvaise, mais elle n'est pas neutre non plus. »

Qu'est-ce qui détermine alors si la technologie améliore notre bien-être, les droits humains et la démocratie ou bien les

dégrade ? Qu’est-ce qui distingue les bonnes technologies des mauvaises ? Et, tant qu’on y est, qu’est-ce qui différencie la lunette de Galilée et vos lentilles de contact Google et Facebook ? Et en quoi est-ce important de se considérer ou non comme des cyborgs ?

Nous devons tous essayer de bien appréhender les réponses à ces questions. Sinon, le prix à payer pourrait être très élevé. Il ne s’agit pas de simples questions technologiques. Il s’agit de questions cruciales sur ce que signifie être une personne à l’ère du numérique et des réseaux. La façon dont nous choisirons d’y répondre aura un impact fondamental sur notre bien-être, tant individuellement que collectivement. Les réponses que nous choisirons détermineront la nature de nos sociétés, et à long terme pourraient influencer la survie de notre espèce.

Propriété et maîtrise du « soi » à l’ère numérique et connectée

Imaginez : vous êtes dans un monde où on vous attribue dès la naissance un appareil qui vous observe, vous écoute et vous suit dès cet instant. Et qui peut aussi lire vos pensées.

Au fil des ans, cet appareil enregistre la moindre de vos réflexions, chaque mot, chaque mouvement et chaque échange. Il envoie toutes ces informations vous concernant à un puissant ordinateur central appartenant à une multinationale. À partir de là, les multiples facettes de votre personnalité sont collectionnées par des algorithmes pour créer un avatar numérique de votre personne. La multinationale utilise votre avatar comme substitut numérique pour manipuler votre comportement.

Votre avatar numérique a une valeur inestimable. C’est tout ce qui fait de vous qui vous êtes (à l’exception de votre corps de chair et d’os). La multinationale se rend compte qu’elle n’a pas besoin de disposer de votre corps pour vous posséder.

Les esprits critiques appellent ce système l'Esclavage 2.0.

À longueur de journée, la multinationale fait subir des tests à votre avatar. Qu'est-ce que vous aimez ? Qu'est-ce qui vous rend heureux ? Ou triste ? Qu'est-ce qui vous fait peur ? Qui aimez-vous ? Qu'allez-vous faire cet après-midi ? Elle utilise les déductions de ces tests pour vous amener à faire ce qu'elle veut. Par exemple, acheter cette nouvelle robe ou alors voter pour telle personnalité politique.

La multinationale a une politique. Elle doit continuer à survivre, croître et prospérer. Elle ne peut pas être gênée par des lois. Elle doit influencer le débat politique. Heureusement, chacun des politiciens actuels a reçu le même appareil que vous à la naissance. Ainsi, la multinationale dispose aussi de leur avatar numérique, ce qui l'aide beaucoup à parvenir à ses fins.

Ceci étant dit, la multinationale n'est pas infaillible. Elle peut toujours faire des erreurs. Elle pourrait de façon erronée déduire, d'après vos pensées, paroles et actions, que vous êtes un terroriste alors que ce n'est pas le cas. Quand la multinationale tombe juste, votre avatar numérique est un outil d'une valeur incalculable pour influencer votre comportement. Et quand elle se plante, ça peut vous valoir la prison.
Dans les deux cas, c'est vous qui perdez !

Ça ressemble à de la science-fiction cyberpunk dystopique, non ?

Remplacez « multinationale » par « Silicon Valley ». Remplacez « puissant ordinateur central » par « *cloud* ». Remplacez « appareil » par « votre smartphone, l'assistant de votre smart home, votre smart city et votre smart ceci-cela, etc. ».

Bienvenue sur Terre, de nos jours ou à peu près.

Le capitalisme de surveillance

Nous vivons dans un monde où une poignée de multinationales ont un accès illimité et continu aux détails les plus intimes de nos vies. Leurs appareils, qui nous observent, nous écoutent et nous pistent, que nous portons sur nous, dans nos maisons, sur le Web et (de plus en plus) sur nos trottoirs et dans nos rues. Ce ne sont pas des outils dont nous sommes maîtres. Ce sont les yeux et les oreilles d'un système socio-techno-économique que Shoshana Zuboff appelle « le capitalisme de surveillance ».

Tout comme dans notre fiction cyberpunk dystopique, les barons voleurs de la Silicon Valley ne se contentent pas de regarder et d'écouter. Par exemple, Facebook a annoncé à sa conférence de développeurs en 2017 qu'ils avaient attelé 60 ingénieurs à littéralement lire dans votre esprit[1].

J'ai demandé plus haut ce qui sépare la lunette de Galilée de vos lentilles de contact produites par Facebook, Google ou d'autres capitalistes de surveillance. Comprendre la réponse à cette question est crucial pour saisir à quel point le concept même de personnalité est menacé par le capitalisme de surveillance.

Lorsque Galilée utilisait son télescope, lui seul voyait ce qu'il voyait et lui seul savait ce qu'il regardait. Il en va de même lorsque vous portez vos lentilles de contact. Si Galilée avait acheté son télescope chez Facebook, Facebook Inc. aurait enregistré tout ce qu'il voyait. De manière analogue, si vous allez achetez vos lentilles de contact chez Google, des caméras y seront intégrées et Alphabet Inc. verra tout ce que vous voyez. (Google ne fabrique pas encore de telles lentilles, mais a déposé un brevet[2] pour les protéger. En attendant, si vous êtes impatient, Snapchat fait des lunettes à caméras intégrées.)

Lorsque vous rédigez votre journal intime au crayon, ni le crayon ni votre journal ne savent ce que vous avez écrit. Lorsque vous écrivez vos réflexions dans des Google Docs, Google en connaît chaque mot.

Quand vous envoyez une lettre à un ami par courrier postal, la Poste ne sait pas ce que vous avez écrit. C'est un délit pour un tiers d'ouvrir votre enveloppe. Quand vous postez un message instantané sur Facebook Messenger, Facebook en connaît chaque mot.

Si vous vous identifiez sur Google Play avec votre smartphone Android, chacun de vos mouvements et de vos échanges sera méticuleusement répertorié, envoyé à Google, enregistré pour toujours, analysé et utilisé contre vous au tribunal du capitalisme de surveillance.

On avait l'habitude de lire les journaux. Aujourd'hui, ce sont eux qui nous lisent. Quand vous regardez YouTube, YouTube vous regarde aussi.

Vous voyez l'idée.

À moins que nous (en tant qu'individus) n'ayons notre technologie sous contrôle, alors « smart » n'est qu'un euphémisme pour « surveillance ». Un smartphone est un mouchard, une maison intelligente est une salle d'interrogatoire et une ville intelligente est un dispositif panoptique.

Google, Facebook et les autres capitalistes de surveillance sont des fermes industrielles pour êtres humains. Ils gagnent des milliards en vous mettant en batterie pour vous faire pondre des données et exploitent cette connaissance de votre intimité pour vous manipuler votre comportement.

Ce sont des scanners d'être humains. Ils ont pour vocation de vous numériser, de conserver cette copie numérique et de l'utiliser comme avatar pour gagner encore plus en taille et

en puissance.

Nous devons comprendre que ces multinationales ne sont pas des anomalies. Elles sont la norme. Elles sont le courant dominant. Le courant dominant de la technologie aujourd'hui est un débordement toxique du capitalisme américain de connivence qui menace d'engloutir toute la planète. Nous ne sommes pas vraiment à l'abri de ses retombées ici en Europe.

Nos politiciens se laissent facilement envoûter par les millions dépensés par ces multinationales pour abreuver les lobbies de Bruxelles. Ils sont charmés par la sagesse de la *Singularity University* (qui n'est pas une université). Et pendant ce temps-là, nos écoles entassent des *Chromebooks* pour nos enfants. On baisse nos taxes, pour ne pas handicaper indûment les capitalistes de surveillance, au cas où ils voudraient se commander une autre Guinness. Et les penseurs de nos politiques, institutionnellement corrompus, sont trop occupés à organiser des conférences sur la protection des données – dont les allocutions sont rédigées par Google et Facebook – pour protéger nos intérêts. Je le sais car j'ai participé à l'une d'elles l'an passé. L'orateur de Facebook quittait tout juste son boulot à la CNIL, la commission française chargée de la protection des données, réputée pour la beauté et l'efficacité de ses chaises musicales.

Il faut que ça change.

Je suis de plus en plus convaincu que si un changement doit venir, il viendra de l'Europe.

La *Silicon Valley* ne va pas résoudre le problème qu'elle a créé. Principalement parce que des entreprises comme Google ou Facebook ne voient pas leurs milliards de bénéfices comme un problème. Le capitalisme de surveillance n'est pas déstabilisé par ses propres critères de succès. Ça va comme sur des roulettes pour les entreprises comme Google et Facebook. Elles se marrent bien en allant à la banque, riant au visage des

législateurs, dont les amendes cocasses excèdent à peine un jour ou deux de leur revenu. D'aucuns diraient que « passible d'amende » signifie « légal pour les riches ». C'est peu de le dire lorsqu'il s'agit de réglementer des multinationales qui brassent des milliers de milliards de dollars.

De manière analogue, le capital-risque ne va pas investir dans des solutions qui mettraient à mal le business immensément lucratif qu'il a contribué à financer.

Alors quand vous voyez passer des projets comme le soi-disant *Center for Humane Technology*, avec des investisseurs-risques et des ex-employés de Google aux commandes, posez-vous quelques questions. Et gardez-en quelques-unes pour les organisations qui prétendent créer des alternatives éthiques alors qu'elles sont financées par les acteurs du capitalisme de surveillance. Mozilla, par exemple, accepte chaque année des centaines de millions de dollars de Google[3]. Au total, elle les a délestés de plus d'un milliard de dollars. Vous êtes content de lui confier la réalisation d'alternatives éthiques ?

Si nous voulons tracer une autre voie en Europe, il faut financer et bâtir notre technologie autrement. Ayons le courage de nous éloigner de nos amis d'outre-Atlantique. Ayons l'aplomb de dire à la *Silicon Valley* et à ses lobbyistes que nous n'achetons pas ce qu'ils vendent.

Et nous devons asseoir tout ceci sur de solides fondations légales en matière de droits de l'homme. J'ai dit « droits de l'homme » ? Je voulais dire droits des cyborgs.

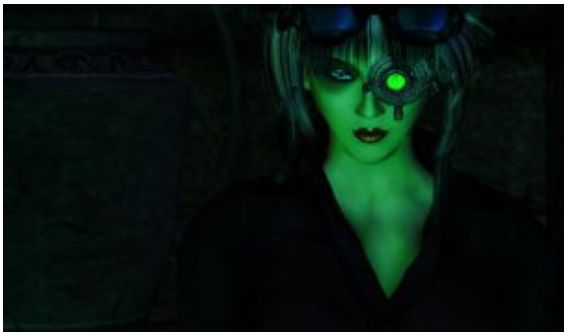
Les droits des cyborgs sont des droits de l'homme

La crise juridique des droits de l'homme que nous rencontrons nous ramène au fond à ce que nous appelons « humain ».

Traditionnellement, on trace les limites de la personne humaine à nos frontières biologiques. En outre, notre système légal et judiciaire tend à protéger l'intégrité de ces frontières et, par là, la dignité de la personne. Nous appelons ce système le droit international des droits de l'Homme.

Malheureusement, la définition de la personne n'est plus adaptée pour nous protéger complètement à l'ère du numérique et des réseaux.

Dans cette nouvelle ère, nous étendons nos capacités biologiques par des technologies numériques et en réseau. Nous prolongeons nos intellects et nos personnes par la technologie moderne. C'est pour ça que nous devons étendre notre concept des limites de la personne jusqu'à inclure les technologies qui nous prolongent. En étendant la définition de la personne, on s'assure que les droits de l'homme couvrent et donc protègent la personne dans son ensemble à l'ère du numérique et des réseaux.



« Cyborg-gal-avi » par Pandora Popstar/Lainy Voom, licence CC BY-NC-SA 2.0

En tant que cyborgs, nous sommes des êtres fragmentaires. Des parties de nous vivent dans nos téléphones, d'autres quelque part sur un serveur, d'autres dans un PC portable. C'est la somme totale de tous ces fragments qui compose l'intégralité de la personne à l'ère du numérique et des réseaux.

Les droits des cyborgs sont donc les droits de l'homme tels qu'appliqués à la personne cybernétique. Ce dont nous n'avons pas besoin, c'est d'un ensemble de « droits numériques » – probablement revus à la baisse. C'est pourquoi, la Déclaration universelle des droits cybernétiques n'est pas un document autonome, mais un addendum à la Déclaration universelle des droits de l'Homme.

La protection constitutionnelle des droits cybernétiques étant un but à long terme, il ne faut pas attendre un changement constitutionnel pour agir. Nous pouvons et devons commencer à nous protéger en créant des alternatives éthiques aux technologies grand public.

Pour des technologies éthiques

Une technologie éthique est un outil que vous possédez et que vous contrôlez. C'est un outil conçu pour vous rendre la vie plus facile et plus clémente. C'est un outil qui renforce vos capacités et améliore votre vie. C'est un outil qui agit dans votre intérêt – et jamais à votre détriment.

Une technologie non éthique est au contraire un outil aux mains de multinationales et de gouvernements. Elle sert leurs intérêts aux dépens des vôtres. C'est un miroir aux alouettes conçu pour capter votre attention, vous rendre dépendant, pister chacun de vos mouvements et vous profiler. C'est une ferme industrielle déguisée en parc récréatif.

La technologie non éthique est nuisible pour les êtres humains, le bien-être et la démocratie.

Semer de meilleures graines

La technologie éthique ne pousse pas sur des arbres, il faut la financer. La façon de la financer a de l'importance.
La technologie non éthique est financée par le capital risque. Le capital risque n'investit pas dans une entreprise, il

investit dans la vente de l'entreprise. Il investit aussi dans des affaires très risquées. Un investisseur risque de la *Silicon Valley* va investir, disons, 5 millions de dollars dans 10 start-ups différentes, en sachant que 9 d'entre elles vont capoter. Alors il (c'est habituellement un « lui/il ») a besoin que la 10e soit une licorne à un milliard de dollars pour que ça lui rapporte 5 à 10 fois l'argent investi (Ce n'est même pas son argent, mais celui de ses clients.). Le seul modèle d'affaires que nous connaissions dans les nouvelles technologies qui atteigne une croissance pareille est la mise en batterie des gens. L'esclavage a bien payé. L'esclavage 2.0 paie bien aussi.

Pas étonnant qu'un système qui attache autant de valeur à un mode de croissance de type prolifération cancéreuse ait engendré des tumeurs telles que Google et Facebook. Ce qui est stupéfiant, c'est que nous semblions célébrer ces tumeurs au lieu de soigner le patient. Et plus déconcertant encore, nous nous montrons obstinément déterminés à nous inoculer la même maladie ici en Europe.

Changeons de direction.

Finançons des alternatives éthiques

À partir des biens communs

Pour le bien commun.

Oui, cela signifie avec nos impôts. C'est en quelque sorte ce pour quoi ils existent (pour mettre en place des infrastructures partagées et destinées au bien commun qui font progresser le bien-être de nos populations et nos sociétés). Si le mot « impôt » vous effraie ou sonne trop vieux jeu, remplacez-le simplement par « financement participatif obligatoire » ou « philanthropie démocratisée ».

Financer une technologie éthique à partir des biens communs ne signifie pas que nous laissions aux gouvernements le pouvoir

de concevoir, posséder ou contrôler nos technologies. Pas plus que de nationaliser des entreprises comme Google et Facebook. Démantelons-les ! Bien sûr. Régulons-les ! Évidemment. Mettons en œuvre absolument tout ce qui est susceptible de limiter autant que possible leurs abus.

Ne remplaçons pas un *Big Brother* par un autre.

À l'inverse, investissons dans de nombreuses et petites organisations, indépendantes et sans but lucratif, et chargeons-les de concevoir les alternatives éthiques. Dans le même temps, mettons-les en compétition les unes avec les autres. Prenons ce que nous savons qui fonctionne dans la *Silicon Valley* (de petites organisations travaillant de manière itérative, entrant en compétition, et qui échouent rapidement) et retirons ce qui y est toxique : le capital risque, la croissance exponentielle, et les sorties de capitaux.

À la place des *startups*, lançons des entreprises durables, des *stayups* en Europe.

À la place de sociétés qui n'ont comme possibilités que d'échouer vite ou devenir des tumeurs malignes, finançons des organisations qui ne pourront qu'échouer vite ou devenir des fournisseurs durables de bien social.

Lorsque j'ai fait part de ce projet au Parlement européen, il y a plusieurs années, celui-ci a fait la sourde oreille. Il n'est pas encore trop tard pour s'y mettre. Mais à chaque fois que nous repoussons l'échéance, le capitalisme de surveillance s'enchevêtre plus profondément encore dans le tissu de nos vies.

Nous devons surmonter ce manque d'imagination et fonder notre infrastructure technologique sur les meilleurs principes que l'humanité ait établis : les droits de l'homme, la justice sociale et la démocratie.

Aujourd'hui, l'UE se comporte comme un département de recherche et développement bénévole pour la *Silicon Valley*. Nous finançons des startups qui, si elles sont performantes, seront vendues à des sociétés de la *Silicon Valley*. Si elles échouent, le contribuable européen réglera la note. C'est de la folie.

La Communauté Européenne doit mettre fin au financement des *startups* et au contraire investir dans les *stayups*. Qu'elle investisse 5 millions d'euros dans dix entreprises durables pour chaque secteur où nous voulons des alternatives éthiques. À la différence des *startups*, lorsque les entreprises durables sont performantes, elles ne nous échappent pas. Elles ne peuvent être achetées par Google ou Facebook. Elles restent des entités non lucratives, soutenables, européennes, œuvrant à produire de la technologie en tant que bien social.

En outre, le financement d'une entreprise durable doit être soumis à une spécification stricte sur la nature de la technologie qu'elle va concevoir. Les biens produits grâce aux financements publics doivent être des biens publics. La *Free Software Foundation Europe* sensibilise actuellement l'opinion sur ces problématiques à travers sa campagne « argent public, code public ». Cependant, nous devons aller au-delà de l'*open source* pour stipuler que la technologie créée par des entreprises durables doit être non seulement dans le domaine public, mais également qu'elle ne peut en être retirée. Dans le cas des logiciels et du matériel, cela signifie l'utilisation de licences copyleft. Une licence copyleft implique que si vous créez à partir d'une technologie publique, vous avez l'obligation de la partager à l'identique. Les licences *share-alike*, de partage à l'identique, sont essentielles pour que nos efforts ne soient pas récupérés pour enjoliver la privatisation et pour éviter une tragédie des communs. Des corporations aux poches sans fond ne devraient jamais avoir la possibilité de prendre ce que nous créons avec des deniers publics, habiller tout ça de quelques millions

d’investissement et ne plus partager le résultat amélioré.

En fin de compte, il faut préciser que les technologies produites par des entreprises *stayups* sont des technologies pair-à-pair. Vos données doivent rester sur des appareils que vous possédez et contrôlez. Et lorsque vous communiquez, vous devez le faire en direct (sans intervention d’un « homme du milieu », comme Google ou Facebook). Là où ce n’est techniquement pas possible, toute donnée privée sous le contrôle d’une tierce partie (par exemple un hébergeur web) doit être chiffrée de bout à bout et vous seul devriez en détenir la clé d’accès.

Même sans le moindre investissement significatif dans la technologie éthique, de petits groupes travaillent déjà à des alternatives. Mastodon, une alternative à Twitter fédérée et éthique, a été créée par une seule personne d’à peine vingt ans. Quelques personnes ont collaboré pour créer un projet du nom de Dat qui pourrait être la base d’un web décentralisé. Depuis plus de dix ans, des bénévoles font tourner un système de nom de domaine alternatif non commercial appelé OpenNIC[4] qui pourrait permettre à chacun d’avoir sa propre place sur le Web…

Si ces graines germent sans la moindre assistance, imaginez ce qui serait à notre portée si on commençait réellement à les arroser et à en planter de nouvelles. En investissant dans des *stayups*, nous pouvons entamer un virage fondamental vers la technologie éthique en Europe.

Nous pouvons construire un pont de là où nous sommes vers là où nous voulons aller.

D’un monde où les multinationales nous possèdent par procuration à un monde où nous n’appartenons qu’à nous-mêmes.

D’un monde où nous finissons toujours par être la propriété d’autrui à un monde où nous demeurons des personnes en tant

que telles.

Du capitalisme de surveillance à la *pairocratie*.

Les algos peuvent vous pourrir la vie

Les algorithmes[1] ne sont guère qu'une série d'instructions pas-à-pas généralement exécutées par un programme sur une machine. Cependant leur complexité et leur opacité pour le commun des mortels sont redoutables, et bien plus encore leur omniprésence dans tous les compartiments de notre vie, y compris la plus intime. Si le code fait la loi, c'est justement parce que les algorithmes sont à la fois puissants, invasifs et sont devenus aujourd'hui indispensables.
L'article ci-dessous ne met pas l'accent sur les nombreux domaines où nous utilisons des algorithmes sans en avoir conscience, il pointe davantage les risques et menaces qu'ils représentent lorsque ce sont les algorithmes qui déterminent notre existence, à travers quelques exemples parmi bien d'autres. Il pose également l'intéressante question de la responsabilité de ceux qui élaborent les algorithmes. Suffira-t-il de réclamer des concepteurs d'algorithmes un sympathique engagement solennel à la manière de celui des acteurs du Web ?

Les codeurs dont les algos contrôlent nos vies, qui les contrôle ? Pouvons-nous avoir un droit de regard sur les algorithmes qui désormais menacent de régir nos vies ?

Les algorithmes sont formidables mais peuvent aussi ruiner des vies

Extrait de l'essai (en anglais) The Formula: How Algorithms Solve All Our Problems—and Create More par **Luke Dormehl.**

Source : article du magazine **Wired** Algorithms are great and all, but can also ruin our lives

Traduction Framalang : Wan, r0u, goofy, Sphinx, sinma, Omegax, ylluss, audionuma

Le 5 avril 2011, John Gass, 41 ans, a reçu un courrier du service d'enregistrement des véhicules motorisés (Registry of Motor Vehicles ou RMV) de l'État du Massachusetts. La lettre informait M. Gass que son permis de conduire avait été annulé, qu'il lui était désormais interdit de conduire et que cela prenait effet immédiatement. Le seul problème, c'est qu'en bon conducteur n'ayant pas commis d'infraction grave au code de la route depuis des années, M. Gass n'avait aucune idée du motif de ce courrier.

Après plusieurs appels téléphoniques frénétiques, suivis par une entrevue avec les fonctionnaires du service, il en a appris la raison : son image avait été automatiquement signalée par un algorithme de reconnaissance faciale conçu

pour parcourir une base de données de millions de permis de conduire de l'État, à la recherche de possibles fausses identités criminelles. L'algorithme avait déterminé que Gass ressemblait suffisamment à un autre conducteur du Massachusetts pour présumer d'une usurpation d'identité, d'où le courrier automatisé du RMV.

Les employés du RMV se sont montrés peu compréhensifs, affirmant qu'il revenait à l'individu accusé de prouver son identité en cas d'erreur quelconque et faisant valoir que les avantages de la protection du public l'emportaient largement sur les désagréments subis par les quelques victimes d'une accusation infondée.

John Gass est loin d'être la seule victime de ces erreurs d'algorithmes. En 2007, un bogue dans le nouveau système informatique du Département des services de santé de Californie a automatiquement mis fin aux allocations de milliers de personnes handicapées et de personnes âgées à bas revenus. Leurs frais d'assurance maladie n'étant plus payés, ces citoyens se sont alors retrouvés sans couverture médicale.

Là où le système précédent aurait notifié les personnes concernées qu'elles n'étaient plus considérées comme éligibles aux allocations en leur envoyant un courrier, le logiciel maintenant opérationnel, CalWIN, a été conçu pour les interrompre sans avertissement, à moins de se connecter soi-même et d'empêcher que cela n'arrive. Résultat : un grand nombre de ceux dont les frais n'étaient plus pris en charge ne s'en sont pas rendu compte avant de recevoir des factures médicales salées. Encore beaucoup n'avaient-ils pas les compétences nécessaires en anglais pour naviguer dans le système de santé en ligne et trouver ce qui allait de travers.

Des failles similaires sont à l'origine de la radiation de votants des listes électorales sans notification, de petites entreprises considérées à tort comme inéligibles aux contrats gouvernementaux, et d'individus identifiés par erreur comme

« parents mauvais payeurs ». Comme exemple notable de ce dernier cas, Walter Vollmer, mécanicien de 56 ans, a été ciblé à tort par le Service fédéral de localisation des parents, et s'est vu envoyer une facture de pension alimentaire à hauteur de 206 000 $. L'épouse de M. Vollmer, 32 ans, a par la suite montré des tendances suicidaires, persuadée que son mari avait eu une vie cachée pendant la majeure partie de leur mariage.

Une possibilité tout aussi alarmante : qu'un algorithme puisse ficher par erreur un individu comme terroriste. Un sort qui attend chaque semaine environ 1500 voyageurs malchanceux qui prennent l'avion. Parmi les victimes passées de ces erreurs de corrélation de données, on retrouve d'anciens généraux de l'armée, un garçon de quatre ans, ainsi qu'un pilote d'*American Airlines*, qui a été détenu 80 fois au cours d'une même année.

Beaucoup de ces problèmes sont dus aux nouveaux rôles joués par les algorithmes dans l'application de la loi. Les budgets réduits menant à des réductions de personnel, les systèmes automatisés, auparavant de simples instruments administratifs, sont maintenant des décideurs à part entière.

Dans nombre de cas, le problème est plus vaste que la simple recherche d'un bon algorithme pour une tâche donnée. Il touche à la croyance problématique selon laquelle toutes les tâches possibles et imaginables peuvent être automatisées. Prenez par exemple l'extraction de données, utilisée pour découvrir les complots terroristes : de telles attaques sont statistiquement rares et ne se conforment pas à un profil bien défini comme, par exemple, les achats sur Amazon. Les voyageurs finissent par abandonner une grande partie de leur vie privée au profit des algorithmes d'extraction de données, avec peu de résultats, si ce n'est des faux-positifs. Comme le note Bruce Schneier, le célèbre expert en sécurité informatique :

> *Chercher des complots terroristes… c'est comme chercher une aiguille dans une botte de foin, ce n'est pas en accumulant*

> *davantage de foin sur le tas qu'on va rendre le problème plus facile à résoudre. Nous ferions bien mieux de laisser les personnes chargées d'enquêtes sur de possibles complots prendre la main sur les ordinateurs, plutôt que de laisser les ordinateurs faire le travail et les laisser décider sur qui l'on doit enquêter.*

Bien qu'il soit clair qu'un sujet aussi brûlant que le terrorisme est un candidat parfait pour ce type de solutions, le problème central se résume encore une fois à cette promesse fantomatique de *l'objectivité* des algorithmes. « Nous sommes tous absolument effrayés par la subjectivité et l'inconstance du comportement humain », explique Danielle Citron, professeur de droit à l'Université du Maryland. « Et à l'inverse, nous manifestons une confiance excessive pour tout ce que peuvent accomplir les ordinateurs ».

Le professeur Citron suggère que l'erreur vient de ce que nous « faisons confiance aux algorithmes, parce que nous les percevons comme objectifs, alors qu'en réalité ce sont des humains qui les conçoivent, et peuvent ainsi leur inculquer toutes sortes de préjugés et d'opinions ». Autrement dit, un algorithme informatique a beau être impartial dans son exécution, cela ne veut pas dire qu'il n'a pas de préjugés codés à l'intérieur.

Ces erreurs de jugement, implicites ou explicites, peuvent être causées par un ou deux programmeurs, mais aussi par des difficultés d'ordre technique. Par exemple, les algorithmes utilisés dans la reconnaissance faciale avaient par le passé de meilleurs taux de réussite pour les hommes que pour les femmes, et meilleurs pour les personnes de couleur que pour les Blancs.

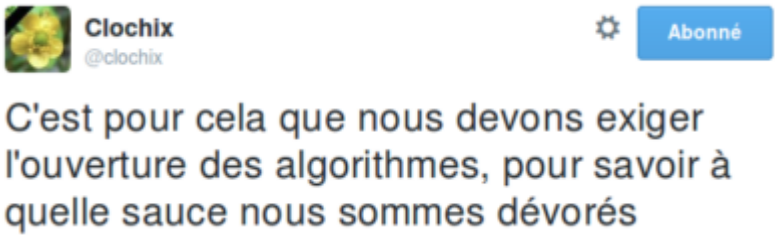
Ce n'est pas par préjugé délibéré qu'un algorithme ciblera plus d'hommes afro-américains que de femmes blanches, mais cela ne change rien au résultat. De tels biais peuvent aussi

venir de combinaisons plus abstraites, enfouies dans le chaos des corrélations de jeux de données.

Prenez par exemple l'histoire de l'afro-américaine Latanya Sweeney, docteure de l'Université d'Harvard. En effectuant des recherches sur Google, elle fut choquée de découvrir que les résultats de ses recherches étaient accompagnés de publicités demandant : « Avez-vous déjà été arrêté(e) ? ». Ces annonces n'apparaissaient pas pour ses collègues blancs. Sweeney se lança alors dans une étude, démontrant que les outils d'apprentissage automatique utilisés par Google étaient incidemment racistes, en associant plus souvent des noms donnés à des personnes noires avec des publicités ayant trait aux rapports d'arrestation.

Le système de recommandation de Google Play révèle un problème similaire : il suggère aux utilisateurs qui téléchargent *Grindr*, un outil de réseautage social basé sur la localisation pour les gays, de télécharger également une application qui assure le suivi géolocalisé des délinquants sexuels. Au vu de ces deux cas, devons-nous conclure que les algorithmes ont fait une erreur, ou plutôt qu'ils sont révélateurs des préjugés inhérents à leurs concepteurs ? Ou, ce qui semble plus probable, ne seraient-ils pas révélateurs d'associations inappropriées et à grande échelle entre – dans le premier cas – les personnes noires et le comportement criminel, et – dans le deuxième cas – l'homosexualité et les agressions sexuelles ?

Peu importe la raison, peu importe la façon répréhensible dont ces corrélations codifiées peuvent exister, elles révèlent une autre face de la culture algorithmique. Quand un seul individu fait explicitement une erreur de jugement, il ne peut jamais affecter qu'un nombre fini de personnes. Un algorithme, quant à lui, a le potentiel d'influer sur un nombre de vies exponentiellement plus grand.



Pour aller plus loin, 4 articles en français sur le même sujet :

- Surveiller les algorithmes
- Ces algorithmes qui vous nous gouvernent
- Ouvrir les modèles, pas seulement les données
- Le jaguar et le bus scolaire

Note

[1] Pour une définition plus élaborée voir Qu’est-ce qu’un algorithme