Comment détruire le capitalisme de surveillance

PAR CORY DOCTOROW

Note de l’éditeur
Le capitalisme de surveillance est partout. Mais ce n’est pas le résultat d’une malencontreuse dérive ou d’un abus de pouvoir des entreprises, c’est le système qui fonctionne comme prévu. Tel est le propos du nouvel essai de Cory Doctorow, que nous sommes ravis de publier intégralement ici sur OneZero. Voici comment détruire le capitalisme de surveillance.

La Toile aux mille mensonges

Le plus surprenant dans la renaissance au 21e siècle des partisans de la Terre plate c’est l’étendue des preuves contre leur croyance. On peut comprendre comment, il y a des siècles, des gens qui n’avaient jamais pu observer la Terre d’un point suffisamment élevé pour voir la courbure de la Terre aient pu en arriver à la croyance « pleine de bon sens » que la Terre, qui semblait plate, était effectivement plate.

Mais aujourd’hui, alors que les écoles primaires suspendent régulièrement des caméras GoPro à des ballons-sondes et les envoient assez haut pour photographier la courbure de la Terre – sans parler de la même courbure devenue banale à voir depuis le hublot d’un avion – il faut avoir une volonté de fer pour maintenir la croyance que le monde est plat.

Il en va de même pour le nationalisme blanc et l’eugénisme : à une époque où l’on peut devenir une simple donnée de la génomique computationnelle en prélevant un échantillon d’ADN dans sa joue et en l’envoyant à une entreprise de séquençage génétique avec une modeste somme d’argent, la « science des races » n’a jamais été aussi facile à réfuter.

Nous vivons un âge d’or où les faits sont à la fois aisément disponibles et faciles à nier. Des conceptions affreuses qui étaient demeurées à la marge pendant des décennies, voire des siècles, se sont répandues du jour au lendemain, semble-t-il.

Lorsqu'une idée obscure gagne du terrain, il n'y a que deux choses qui puissent expliquer son ascension : soit la personne qui exprime cette idée a bien amélioré son argumentation, soit la proposition est devenue plus difficile à nier face à des preuves de plus en plus nombreuses. En d'autres termes, si nous voulons que les gens prennent le changement climatique au sérieux, nous pouvons demander à un tas de Greta Thunberg de présenter des arguments éloquents et passionnés depuis des podiums, gagnant ainsi nos cœurs et nos esprits, ou bien nous pouvons attendre que les inondations, les incendies, le soleil brûlant et les pandémies fassent valoir leurs arguments. En pratique, nous devrons probablement faire un peu des deux : plus nous bouillirons et brûlerons, plus nous serons inondés et périrons, plus il sera facile aux Greta Thunberg du monde entier de nous convaincre.

Les arguments en faveur de croyances ridicules en des conspirations odieuses, comme ceux des partisans anti-vaccination, des climato-sceptiques, des adeptes de la Terre plate ou de l'eugénisme ne sont pas meilleurs que ceux de la génération précédente. En fait, ils sont pires parce qu'ils sont présentés à des personnes qui ont au moins une connaissance basique des faits qui les réfutent.

Les anti-vaccins existent depuis les premiers vaccins, mais les premiers anti-vaccins s'adressaient à des personnes moins bien équipées pour comprendre les principes de base de la microbiologie et qui, de plus, n'avaient pas été témoins de l'éradication de maladies meurtrières comme la polio, la variole ou la rougeole. Les anti-vaccins d'aujourd'hui ne sont pas plus éloquents que leurs prédécesseurs, et ils ont un travail bien plus difficile.

Ces théoriciens conspirationnistes farfelus peuvent-ils alors vraiment réussir grâce à des arguments supérieurs ?

Certains le pensent. Aujourd'hui, il est largement admis que l'apprentissage automatique et la surveillance commerciale peuvent transformer un théoricien du complot, même le plus maladroit, en un Svengali capable de déformer vos perceptions et de gagner votre confiance, ce grâce au repérage de personnes vulnérables, à qui il présentera des arguments qu'une I.A. aura affinés afin de contourner leurs facultés rationnelles, transformant ainsi ces gens ordinaires en platistes, en anti-vaccins ou même en nazis.
Lorsque la RAND Corporation accuse Facebook de « radicalisation » et lorsque l'algorithme de Facebook est tenu pour responsable de la diffusion de fausses informations sur les coronavirus, le message implicite est que l'apprentissage automatique et la surveillance provoquent des changements dans notre conception commune de ce qui est vrai.

Après tout, dans un monde où les théories de conspiration tentaculaires et incohérentes comme le Pizzagate et son successeur, QAnon, ont de nombreux adeptes, il doit bien se passer quelque chose.

Mais y a-t-il une autre explication possible ? Et si c'étaient les circonstances matérielles, et non les arguments, qui faisaient la différence pour ces lanceurs de théories complotistes ? Et si le traumatisme de vivre au milieu de véritables complots tout autour de nous – des complots entre des gens riches, leurs lobbyistes et les législateurs pour enterrer des faits gênants et des preuves de méfaits (ces complots sont communément appelés « corruption ») – rendait les gens vulnérables aux théories du complot ?

Si c'est ce traumatisme et non la contagion – les conditions matérielles et non l'idéologie – qui fait la différence aujourd'hui et qui permet une montée d'une désinformation détestable face à des faits facilement observables, cela ne signifie pas que nos réseaux informatiques soient irréprochables. Ils

continuent à faire le gros du travail : repérer les personnes vulnérables et les guider à travers une série d'idées et de communautés toujours plus extrémistes.

Le conspirationnisme qui fait rage a provoqué de réels dégâts et représente un réel danger pour notre planète et les espèces vivantes, des épidémies déclenchées par le déni de vaccin aux génocides déclenchés par des conspirations racistes en passant par l'effondrement de la planète causé par l'inaction climatique inspirée par le déni. Notre monde est en feu et nous devons donc l'éteindre, trouver comment aider les gens à voir la vérité du monde, au-delà des conspirations qui les ont trompés.

Mais lutter contre les incendies est une stratégie défensive. Nous devons prévenir les incendies. Nous devons nous attaquer aux conditions matérielles traumatisantes qui rendent les gens vulnérables à la contagion conspirationniste. Ici aussi, la technologie a un rôle à jouer.

Les propositions ne manquent pas pour y remédier. Du règlement de l'UE sur les contenus terroristes, qui exige des plateformes qu'elles contrôlent et suppriment les contenus « extrémistes », aux propositions américaines visant à forcer les entreprises technologiques à espionner leurs utilisateurs et à les tenir pour responsables des discours fallacieux de leurs utilisateurs, il existe beaucoup d'énergie pour forcer les entreprises technologiques à résoudre les problèmes qu'elles ont créés.

Il manque cependant une pièce essentielle au débat. Toutes ces solutions partent du principe que les entreprises de technologie détiennent la clé du problème, que leur domination sur l'Internet est un fait permanent. Les propositions visant à remplacer les géants de la tech par un Internet plus diversifié et pluraliste sont introuvables. Pire encore : les « solutions » proposées aujourd'hui exigent que les grandes entreprises technologiques restent grandes, car seules les très grandes peuvent se permettre de mettre en œuvre les systèmes exigés par ces lois.

Il est essentiel de savoir à quoi nous voulons que notre technologie ressemble si nous voulons nous sortir de ce pétrin. Aujourd'hui, nous sommes à un carrefour où nous essayons de déterminer si nous voulons réparer les géants de la tech qui dominent notre Internet, ou si nous voulons réparer Internet lui-même en le libérant de l'emprise de ces géants. Nous ne pouvons pas faire les deux, donc nous devons choisir.

Je veux que nous choisissions judicieusement. Dompter les géants de la tech est essentiel pour réparer Internet et, pour cela, nous avons besoin d'une action militante pour nos droits numériques.

Le militantisme des droits numériques après un quart de siècle

Le militantisme pour les droits numériques est plus que trentenaire à présent. L'Electronic Frontier Foundation a eu 30 ans cette année ; la Free Software Foundation a démarré en 1985. Pour la majeure partie de l'histoire du mouvement, la plus grande critique à son encontre était son inutilité : les vraies causes à défendre étaient celle du monde réel (repensez au scepticisme qu'a rencontré la Finlande en déclarant que l'accès au haut débit est un droit humain, en 2010) et le militantisme du monde réel ne pouvait exister qu'en usant ses semelles dans la rue (pensez au mépris de Malcolm Gladwell pour le « clictivisme »).

Mais à mesure de la présence croissante de la tech au cœur de nos vies quotidiennes, ces accusations d'inutilité ont d'abord laissé place aux accusations d'insincérité (« vous prêtez attention à la tech uniquement pour défendre les intérêts des entreprises de la tech », puis aux accusations de

négligence (« pourquoi n'avez-vous pas prévu que la tech pourrait être une force aussi destructrice ? »). Mais le militantisme pour des droits numériques est là où il a toujours été : prêter attention aux êtres humains dans un monde où la tech prend inexorablement le contrôle.

La dernière version de cette critique vient sous la forme du « capitalisme de surveillance », un terme inventé par la professeure d'économie Shoshana Zuboff dans son long et influent livre de 2019, The Age of Surveillance Capitalism : The Fight for a Human Future at the New Frontier of Power (à paraître en français le 15/10/2020 sous le titre *L'Âge du capitalisme de surveillance*). Zuboff avance que le « capitalisme de surveillance » est une créature unique de l'industrie de la tech et qu'au contraire de toute autre pratique commerciale abusive dans l'histoire, elle est « constituée par des mécanismes d'extraction imprévisibles et souvent illisibles, de marchandisation et de contrôle qui éloignent en réalité les personnes de leur comportement propre, tout en créant de nouveaux marchés de prédiction et de modification comportementales. Le capitalisme de surveillance défie les normes démocratiques et s'écarte de manière décisive de l'évolution du capitalisme de marché au cours des siècles ». C'est une forme nouvelle et mortelle du capitalisme, un « capitalisme scélérat », et notre manque de compréhension de ses capacités et dangers sans précédents représente une menace existentielle pour l'espèce entière. Elle a raison sur la menace que représente actuellement le capitalisme pour notre espèce, et elle a raison de dire que la tech pose des défis uniques à notre espèce et notre civilisation, mais elle se trompe vraiment sur la manière dont la tech est différente et sur la façon dont elle menace notre espèce.

De plus, je pense que son diagnostic incorrect nous mènera dans une voie qui finira par renforcer les géants de la tech, au lieu de les affaiblir. Nous devons démanteler les géants et, pour cela, nous devons commencer par identifier correctement le problème.

L'exception de la tech, hier et d'aujourd'hui

Les premiers critiques du mouvement des droits numériques, dont les meilleurs représentants sont peut-être les organisations militantes comme l'Electronic Frontier Foundation, la Free Software Foundation, Public Knowledge ou d'autres, qui mettent l'accent sur la préservation et l'amélioration des droits humains dans un environnement numérique, ont diabolisé les militants en les accusant de défendre « une exception technologique ». Au tournant du nouveau millénaire, les gens sérieux ridiculisaient toute affirmation selon laquelle les réglementations sur la tech pouvaient avoir un impact sur « le monde réel ». Les craintes exprimées sur la possibilité que les réglementations de la tech aient des conséquences sur les libertés d'expression, d'association, de vie privée, sur les fouilles et saisies, les droits fondamentaux et les inégalités, tout cela était qualifié de grotesque, comme une prétention à faire passer les inquiétudes de tristes nerds se disputant à propos de Star Trek sur des forums au-dessus des luttes pour les droits civiques, des combats de Nelson Mandela et du soulèvement du Ghetto de Varsovie.

Au cours des décennies suivantes, les accusations d'« exception technologique » n'ont fait que s'affûter alors que le rôle de la tech dans la vie quotidienne s'est affirmé : maintenant que la tech s'est infiltrée dans tous les recoins de nos vies et que notre présence en ligne a été monopolisée par une poignée de géants, les défenseurs des libertés numériques sont accusés d'apporter de l'eau au moulin des géants de la tech pour couvrir les négligences (ou pire encore, leurs manœuvres malfaisantes) qui servent leurs propres intérêts.

De mon point de vue, le mouvement pour les droits numériques est resté immobile alors que le reste du monde a progressé. Depuis sa naissance, la préoccupation principale du mouvement était les

utilisateurs, ainsi que les créateurs d'outils numériques qui fournissaient le code dont ils avaient besoin pour concrétiser les droits fondamentaux. Les militants pour les droits numériques ne se sentaient concernés par les entreprises que dans la mesure où elles agissaient pour faire respecter les droits des utilisateurs (ou, tout aussi souvent, quand les entreprises agissaient de manière tellement stupide qu'elles menaçaient d'adopter de nouvelles règles qui rendraient plus difficile pour les bons élèves d'aider les utilisateurs).

La critique du « capitalisme de surveillance » a remis en lumière les militants pour les droits numériques : non pas comme des alarmistes qui surestiment l'importance de leurs nouveaux joujoux, ni comme des complices des géants de la tech, mais plutôt comme des brasseurs d'air tranquilles dont le militantisme de longue date est un handicap qui les empêche de discerner de nouvelles menaces, alors qu'ils continuent de mener les combats technologiques du siècle dernier.

Mais l'exception de la tech est une lourde erreur, peu importe qui la commet.

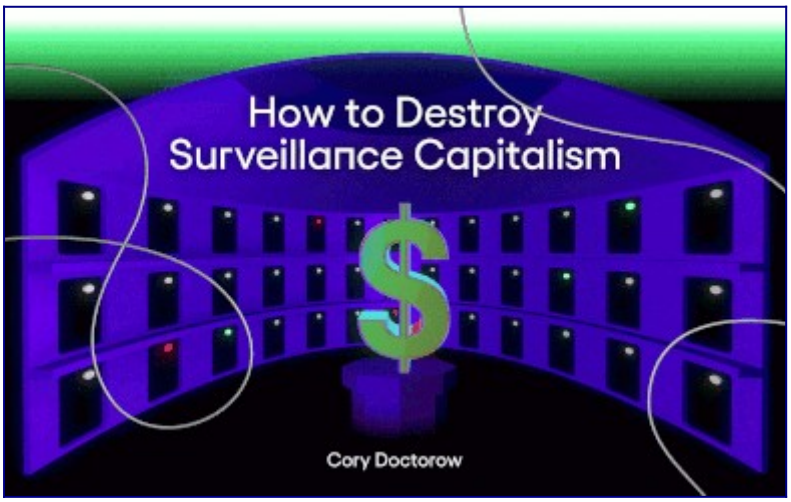


illustration de Shira Inbar

Ne vous fiez pas à ce qu’ils vous disent

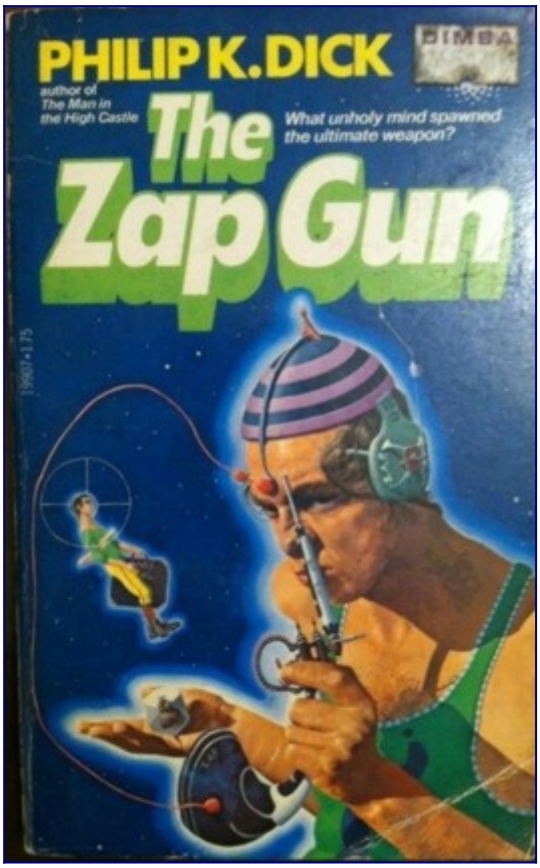
Vous avez probablement déjà entendu dire : « si c’est gratuit, c’est vous le produit ». Comme nous le verrons plus loin, c’est vrai, mais incomplet. En revanche, ce qui est absolument vrai, c’est que les annonceurs sont les clients des géants de la tech accros à la pub et que les entreprises comme Google ou Facebook vendent leurs capacités à vous convaincre d’acheter. La came des géants de la tech, c’est la persuasion. Leurs services (réseaux sociaux, moteurs de recherche, cartographie, messagerie, et tout le reste) ne sont que des moyens de fournir cette persuasion.

La peur du capitalisme de surveillance part du principe (justifié) que tout ce que les géants de la tech racontent sur eux-mêmes est sûrement un mensonge. Mais cette critique admet une exception quand il s’agit des prétentions émises par les géants de la tech dans leurs documentations marketing, plus précisément leur matraquage continu autour de l’efficacité de leurs produits dans les présentations destinées à de potentiels annonceurs numériques en ligne, ainsi que dans les séminaires de technologies publicitaires : on considère qu’ils sont aussi doués pour nous influencer qu’ils le prétendent lorsqu’ils vendent leurs systèmes de persuasion aux clients crédules. C’est une erreur, car les documents marketing ne sont pas un indicateur fiable de l’efficacité d’un produit.

Le capitalisme de surveillance considère qu’au vu de l’important volume d’achat des annonceurs auprès des géants de la tech, ces derniers doivent sûrement vendre quelque chose pour de bon. Mais ces ventes massives peuvent tout aussi bien être le résultat d’un fantasme généralisé ou de quelque chose d’encore plus pernicieux : un contrôle monopolistique sur nos communications et nos échanges commerciaux.

Être surveillé modifie notre comportement et pas pour le meilleur. La surveillance crée des risques pour notre progrès social. Le livre de Zuboff propose des explications particulièrement lumineuses de ce phénomène. Mais elle prétend aussi que la surveillance nous dérobe littéralement notre liberté : ainsi, lorsque nos données personnelles sont mélangées avec de l’apprentissage machine, cela crée un système de persuasion tellement dévastateur que nous sommes démunis face à lui. Autrement dit, Facebook utilise un algorithme qui analyse des données de votre vie quotidienne,

extraites sans consentement, afin de personnaliser votre fil d’actualité pour vous pousser à acheter des trucs. On dirait un rayon de contrôle mental sorti tout droit d’une BD des années 50, manipulé par des savants fous dont les supercalculateurs leur assurent une domination totale et perpétuelle sur le monde.



Qu’est-ce que la persuasion ?

Pour comprendre pourquoi vous ne devriez pas vous inquiéter du rayon de contrôle mental, mais bien plutôt de la surveillance et des géants de la tech, nous devons commencer par décortiquer ce que nous entendons par « persuasion ».

Google, Facebook et les autres capitalistes de la surveillance promettent à leurs clients (les annonceurs) qu'en utilisant des outils d’apprentissage machine entraînés sur des jeux de données de taille inimaginable, constitués d’informations personnelles récoltées sans consentement, ils seront capables de découvrir des moyens de contourner les capacités de rationalisation du public et de contrôler le comportement de ce dernier, provoquant ainsi des cascades d’achats, de votes ou autres effets recherchés.

L’impact de la domination excède de loin celui de la manipulation et devrait être central dans notre analyse et dans tous les remèdes que nous envisageons.

Mais il existe peu d’indices pour prouver que cela se déroule ainsi. En fait, les prédictions que le capitalisme de surveillance fournit à ses clients sont bien moins impressionnantes qu’elles ne le prétendent. Plutôt que de chercher à passer outre votre rationalité, les capitalistes de la surveillance comme Mark Zuckerberg pratiquent essentiellement une au moins des trois choses suivantes :

1. Segmentation

Si vous êtes vendeur de couches-culottes, vous aurez plus de chance d'en vendre en démarchant les personnes présentes dans les maternités. Toutes les personnes qui entrent ou sortent d'une maternité ne viennent pas d'avoir un bébé et toutes celles qui ont un bébé ne sont pas consommatrices de couches. Mais avoir un bébé est fortement corrélé avec le fait d'être un consommateur de couches et se trouver dans une maternité est hautement corrélé avec le fait d'avoir un bébé. Par conséquent, il y a des publicités pour les couches autour des maternités (et même des démarcheurs de produits pour bébés qui hantent les couloirs des maternités avec des paniers remplis de cadeaux).

Le capitalisme de surveillance, c'est de la segmentation puissance un milliard. Les vendeurs de couches peuvent aller bien au-delà des personnes présentes dans les maternités (bien qu'ils puissent aussi faire ça avec, par exemple, des publicités mobiles basées sur la géolocalisation). Ils peuvent vous cibler selon que vous lisiez des articles sur l'éducation des enfants, les couches-culottes ou une foule d'autres sujets, et l'analyse des données peut suggérer des mots-clés peu évidents à cibler. Ils peuvent vous cibler sur la base d'articles que vous avez récemment lus. Ils peuvent vous cibler sur la base de ce que vous avez récemment acheté. Ils peuvent vous cibler sur la base des e-mails ou des messages privés que vous recevez concernant ces sujets, et même si vous mentionnez ces sujets à voix haute (bien que Facebook et consorts jurent leurs grands dieux que ce n'est pas le cas, du moins pour le moment).

C'est franchement effrayant.

Mais ce n'est pas du contrôle mental.

Cela ne vous prive pas de votre libre-arbitre. Cela ne vous leurre pas.

Pensez à la manière dont le capitalisme de surveillance fonctionne en politique. Les entreprises du capitalisme de surveillance vendent aux professionnels de la politique la capacité de repérer ceux qui pourraient être réceptifs à leurs argumentaires. Les candidats qui font campagne sur la corruption du secteur financier sont à la recherche de personnes étranglées par les dettes, ceux qui utilisent la xénophobie recherchent des personnes racistes. Ces communicants ont toujours ciblé leurs messages, peu importe que leurs intentions soient honorables ou non : les syndicalistes font leurs discours aux portes des usines et les suprémacistes blancs distribuent leurs prospectus lors des réunions de l'association conservatrice John Birch Society.

Mais c'est un travail imprécis, et donc épuisant. Les syndicalistes ne peuvent pas savoir quel ouvrier approcher à la sortie de l'usine et peuvent perdre leur temps avec un membre discret de la John Birch Society ; le suprémaciste blanc ne sait pas quels membres de la Birch sont tellement délirants qu'assister à une réunion est le maximum qu'ils peuvent faire, et lesquels peuvent être convaincus de traverser le pays pour brandir une torche de jardin Tiki dans les rues de Charlottesville, en Virginie.

Comme le ciblage augmente le rendement des discours politiques, il peut bouleverser le paysage politique, en permettant à tous ceux qui espéraient secrètement le renversement d'un autocrate (ou juste d'un politicien indéboulonnable) de trouver toutes les personnes qui partagent leurs idées, et ce, à un prix dérisoire. Le ciblage est devenu essentiel à la cristallisation rapide des récents mouvements politiques tels que Black Lives Matter ou Occupy Wall Street, ainsi qu'à des acteurs moins présentables comme les mouvements des nationalistes blancs d'extrême-droite qui ont manifesté à Charlottesville.

Il est important de différencier ce type d'organisation politique des campagnes de communication. Trouver des personnes secrètement d'accord avec vous n'est en effet pas la même chose que de convaincre des gens de le devenir. L'essor de phénomènes comme les personnes non-binaires ou autres identités de genres non-conformistes est souvent décrit par les réactionnaires comme étant le résultat de campagnes en ligne de lavage de cerveaux qui ont pour but de convaincre des personnes influençables qu'elles sont secrètement *queer* depuis le début.

Mais les témoignages de ceux qui ont fait leur coming-out racontent une tout autre histoire, dans laquelle les personnes qui ont longtemps gardé secret leur genre étaient encouragées par celles qui en avaient déjà parlé. Une histoire dans laquelle les personnes qui savaient qu'elles étaient différentes (mais qui manquaient de vocabulaire pour parler de ces différences) apprenaient les termes exacts à utiliser grâce à cette manière bon marché de trouver des personnes et de connaître leurs idées.

2. Tromperie

Les mensonges et les tromperies sont des pratiques malsaines, et le capitalisme de surveillance ne fait que les renforcer avec le ciblage. Si vous voulez commercialiser un prêt sur salaire ou hypothécaire frauduleux, le capitalisme de surveillance peut vous aider à trouver des personnes à la fois désespérées et peu averties, qui seront donc réceptives à vos arguments. Cela explique la montée en puissance de nombreux phénomènes, tels que la vente multi-niveau, dans laquelle des déclarations mensongères sur des gains potentiels et l'efficacité des techniques de vente ciblent des personnes désespérées, avec de la publicité associée à leurs recherches qui indiquent, par exemple, qu'elles se débattent contre des prêts toxiques.

Le capitalisme de surveillance encourage également la tromperie en facilitant le repérage d'autres personnes qui ont été trompées de la même manière. Elles forment ainsi une communauté de personnes qui renforcent mutuellement leurs croyances. Pensez à ces forums où des personnes victimes de fraudes commerciales à plusieurs niveaux se réunissent pour échanger des conseils sur la manière d'améliorer leur chance de vendre le produit.

Parfois, la tromperie en ligne consiste à remplacer les convictions correctes d'une personne par des croyances infondées, comme c'est le cas pour le mouvement anti-vaccination, dont les victimes sont souvent des personnes qui font confiance aux vaccins au début mais qui sont convaincues par des preuves en apparence plausibles qui les conduisent à croire à tort que les vaccins sont nocifs.

Mais la fraude réussit beaucoup plus souvent lorsqu'elle ne doit pas se substituer à une véritable croyance. Lorsque ma fille a contracté des poux à la garderie, l'un des employés m'a dit que je pouvais m'en débarrasser en traitant ses cheveux et son cuir chevelu avec de l'huile d'olive. Je ne savais rien des poux et je pensais que l'employé de la crèche les connaissait, alors j'ai essayé (ça n'a pas marché, et ça ne marche pas). Il est facile de se retrouver avec de fausses croyances quand vous n'en savez pas suffisamment et quand ces croyances sont véhiculées par quelqu'un qui semble savoir ce qu'il fait.

C'est pernicieux et difficile (et c'est aussi contre ce genre de choses qu'Internet peut aider à se prémunir en rendant disponibles des informations véridiques, en particulier sous une forme qui expose les débats sous-jacents entre des points de vue très divergents, comme le fait Wikipédia) mais ce n'est pas un lavage de cerveau, c'est de l'escroquerie. Dans la majorité des cas, les personnes victimes de ces campagnes de ces arnaques comblent leur manque d'informations de la

manière habituelle, en consultant des sources apparemment fiables. Si je vérifie la longueur du pont de Brooklyn et que j'apprends qu'il mesure 1 770 mètres de long, mais qu'en réalité, il fait 1 825 mètres de long, la tromperie sous-jacente est un problème, mais c'est un problème auquel il est possible de remédier simplement. C'est un problème très différent de celui du mouvement anti-vax, où la croyance correcte d'une personne est remplacée par une fausse, par le biais d'une persuasion sophistiquée.

3. Domination

Le capitalisme de surveillance est le résultat d'un monopole. Le monopole est la cause, tandis que le capitalisme de surveillance et ses conséquences négatives en sont les effets. Je rentrerai dans les détails plus tard, mais, pour le moment, je dirai simplement que l'industrie technologique s'est développée grâce à un principe radicalement antitrust qui a permis aux entreprises de croître en fusionnant avec leurs rivaux, en rachetant les concurrents émergents et en étendant le contrôle sur des pans entiers du marché.

Prenons un exemple de la façon dont le monopole participe à la persuasion via la domination : Google prend des décisions éditoriales quant à ses algorithmes qui déterminent l'ordre des réponses à nos requêtes. Si un groupe d'escrocs décide de faire croire à la planète entière que le pont de Brooklyn mesure 1700 mètres et si Google élève le rang des informations fournies par ce groupe pour les réponses aux questions du type « Quelle est la longueur du pont de Brooklyn ? » alors les 8 ou 10 premières pages de résultats fournies par Google pourront être fausses. Sachant que la plupart des personnes ne vont pas au-delà des premiers résultats (et se contentent de la première page de résultats), le choix opéré par Google impliquera de tromper de nombreuses personnes.

La domination de Google sur la recherche (plus de 86 % des recherches effectuées sur le Web sont faites via Google) signifie que l'ordre qu'il utilise pour classer les résultats de recherche a un impact énorme sur l'opinion publique. Paradoxalement, c'est cette raison que Google invoque pour dire qu'il ne peut pas rendre son algorithme transparent : la domination de Google sur la recherche implique que les résultats de son classement sont trop importants pour se permettre de pouvoir dire au monde comment il y parvient, car si un acteur malveillant découvrait une faille dans ce système, alors il l'exploiterait pour mettre en avant son point de vue en haut des résultats. Il existe un remède évident lorsqu'une entreprise devient trop grosse pour être auditée : la diviser en fragments plus petits.

Zuboff parle du capitalisme de surveillance comme d'un « capitalisme voyou » dont les techniques de stockage de données et d'apprentissage machine nous privent de notre libre arbitre. Mais les campagnes d'influence qui cherchent à remplacer les croyances existantes et correctes par des croyances fausses ont un effet limité et temporaire, tandis que la domination monopolistique sur les systèmes d'information a des effets massifs et durables. Contrôler les résultats des recherches du monde entier signifie contrôler l'accès aux arguments et à leurs réfutations et, par conséquent, contrôler une grande partie des croyances à travers le monde. Si notre préoccupation est de savoir comment les entreprises nous empêchent de nous faire notre propre opinion et de déterminer notre propre avenir, l'impact de la domination dépasse de loin celui de la manipulation et devrait être au centre de notre analyse et de tous les remèdes que nous recherchons.

4. Contournement de nos facultés rationnelles

Mais voici le meilleur du pire : utiliser l'apprentissage machine, les techniques du dark UX, le piratage des données et d'autres techniques pour nous amener à faire des choses qui vont à l'encontre de nos principes. Ça, c'est du contrôle de l'esprit.

Certaines de ces techniques se sont révélées d'une efficacité redoutable (ne serait-ce qu'à court terme). L'utilisation de comptes à rebours sur une page de finalisation de commande peut créer un sentiment d'urgence incitant à ignorer la petite voix interne lancinante qui vous suggère d'aller faire vos courses ou de bien réfléchir avant d'agir. L'utilisation de membres de votre réseau social dans les publicités peut fournir une « justification sociale » qu'un achat vaut la peine d'être fait. Même le système d'enchères mis au point par eBay est conçu pour jouer sur nos points faibles cognitifs, nous donnant l'impression de « posséder » quelque chose parce que nous avons enchéri dessus, ce qui nous encourage à enchérir à nouveau lorsque nous sommes surenchéris pour s'assurer que « nos » biens restent à nous.

Les jeux sont très bons dans ce domaine. Les jeux « d'accès gratuit » nous manipulent par le biais de nombreuses techniques, comme la présentation aux joueurs d'une série de défis qui s'échelonnent en douceur de difficulté croissante, qui créent un sentiment de maîtrise et d'accomplissement, mais qui se transforment brusquement en un ensemble de défis impossibles à relever sans une mise à niveau payante. Ajoutez à ce mélange une certaine pression sociale – un flux de notifications sur la façon dont vos amis se débrouillent – et avant de comprendre ce qui vous arrive, vous vous retrouvez à acheter des gadgets virtuels pour pouvoir passer au niveau suivant.

Les entreprises ont prospéré et périclité avec ces techniques, et quand elles échouent cela mérite que l'on s'y attarde. En général, les êtres vivants s'adaptent aux stimuli : une chose que vous trouvez particulièrement convaincante ou remarquable, lorsque vous la rencontrez pour la première fois, le devient de moins en moins, et vous finissez par ne plus la remarquer du tout. Pensez au bourdonnement énervant que produit le réfrigérateur quand il se met en marche, qui finit par se fondre tellement bien dans le bruit ambiant que vous ne le remarquez que lorsqu'il s'arrête à nouveau.

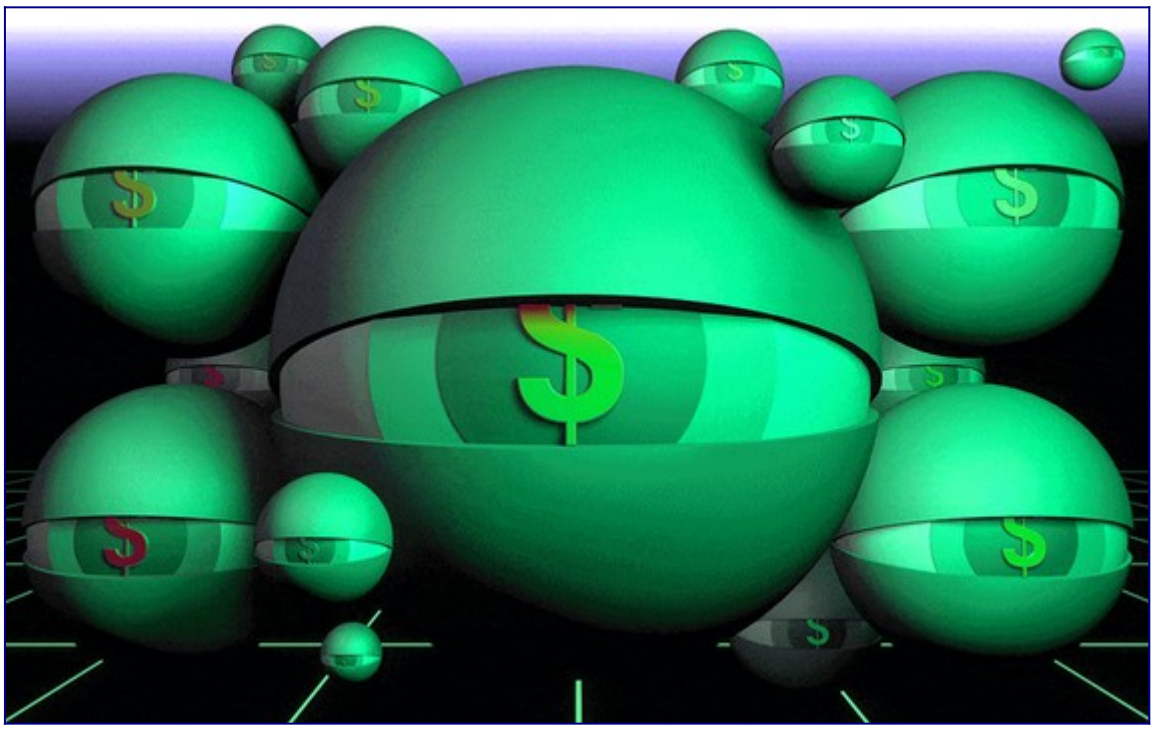
C'est pourquoi le conditionnement comportemental utilise des « programmes de renforcement intermittent ». Au lieu de vous donner des encouragements ou des embûches, les jeux et les services gamifiés éparpillent les récompenses selon un calendrier aléatoire – assez souvent pour que vous restiez intéressé, et de manière assez aléatoire pour que vous ne trouviez jamais le schéma toujours répété qui rendrait la chose ennuyeuse.

Le « renforcement intermittent » est un outil comportemental puissant, mais il représente aussi un problème d'action collective pour le capitalisme de surveillance. Les « techniques d'engagement » inventées par les comportementalistes des entreprises du capitalisme de surveillance sont rapidement copiées par l'ensemble du secteur, de sorte que ce qui commence par un mystérieux changement de conception d'un service – comme une demande d'actualisation ou des alertes lorsque quelqu'un aime vos messages ou des quêtes secondaires auxquelles vos personnages sont invités alors qu'ils sont au beau milieu de quêtes principales – tout cela devient vite péniblement envahissant. L'impossibilité où l'on est de maîtriser et faire taire les incessantes notifications de son smartphone finit par générer en un mur de bruit informationnel monotone, car chaque application et chaque site utilise ce qui semble fonctionner à ce moment-là.

Du point de vue du capitalisme de surveillance, notre capacité d'adaptation est une bactérie nocive qui la prive de sa source de nourriture – notre attention – et les nouvelles techniques pour capter cette attention sont comme de nouveaux antibiotiques qui peuvent être utilisés pour briser nos défenses immunitaires et détruire notre autodétermination. Et il existe bel et bien des techniques de ce genre. Qui peut oublier la grande épidémie de Zynga, lorsque tous nos amis ont été pris dans des boucles de dopamine sans fin et sans intérêt en jouant à FarmVille ? Mais chaque nouvelle technique qui attire l'attention est adoptée par l'ensemble de l'industrie et utilisée si aveuglément que la résistance aux antibiotiques s'installe. Après une certaine dose de répétitions, nous développons presque tous une immunité aux techniques les plus puissantes – en 2013, deux ans après le pic de Zynga, sa base d'utilisateurs avait diminué de moitié.

Pas tout le monde, bien sûr. Certaines personnes ne s'adaptent jamais aux stimuli, tout comme certaines personnes n'arrêtent jamais d'entendre le bourdonnement du réfrigérateur. C'est pourquoi la plupart des personnes qui sont exposées aux machines à sous y jouent pendant un certain temps, puis passent à autre chose, pendant qu'une petite mais tragique minorité liquide le pécule mis de côté pour la scolarité de ses enfants, achète des couches pour adultes et reste scotchée devant une machine jusqu'à s'écrouler de fatigue.

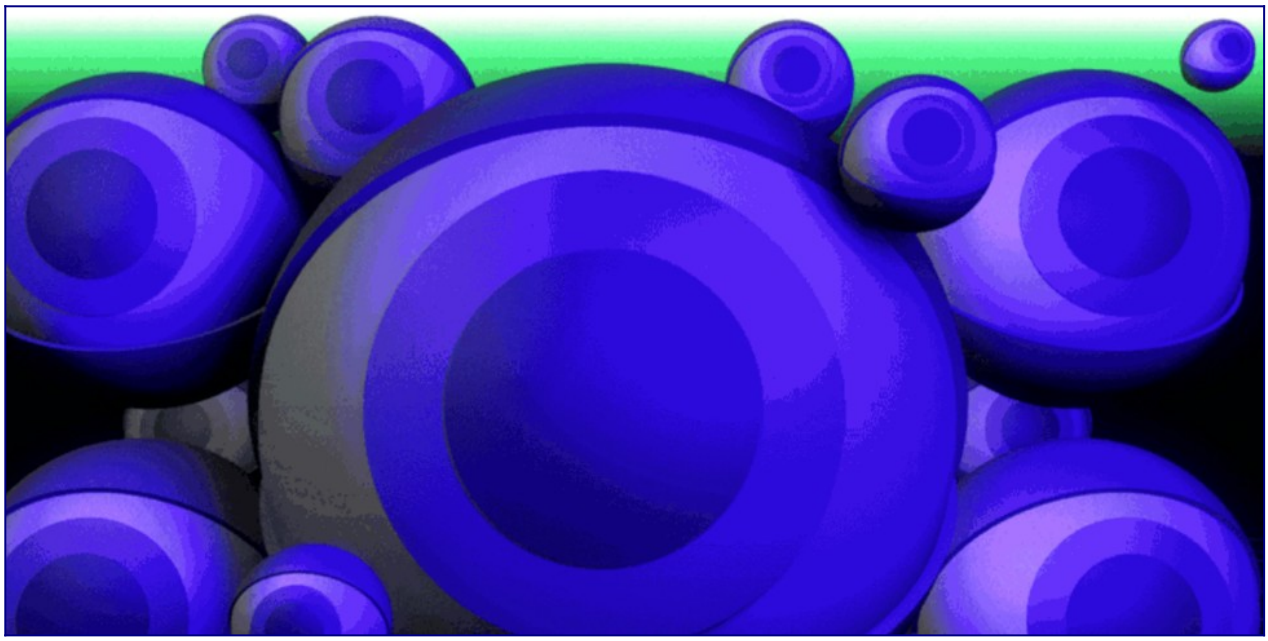
Mais les marges du capitalisme de surveillance sur la modification des comportements sont nulles. Tripler le taux de conversion en achats d'un truc semble un succès, sauf si le taux initial est bien inférieur à 1 % avec un pourcentage de progression… encore inférieur à 1 %. Alors que les machines à sous tirent des bénéfices en centimes de chaque jeu, le capitalisme de surveillance ratisse en fractions de centimes infinitésimales.



Les rendements élevés des machines à sous signifient qu'elles peuvent être rentables simplement en drainant les fortunes de la petite frange de personnes qui leur sont pathologiquement vulnérables et incapables de s'adapter à leurs astuces. Mais le capitalisme de surveillance ne peut pas survivre avec les quelques centimes qu'il tire de cette tranche vulnérable – c'est pourquoi, lorsque la Grande épidémie de Zynga s'est enfin terminée, le petit nombre de joueurs encore dépendants qui restaient n'ont pas suffi à en faire encore un phénomène mondial. Et de nouvelles armes d'attention puissantes ne sont pas faciles à trouver, comme en témoignent les longues années qui se sont écoulées depuis le dernier succès de Zynga. Malgré les centaines de millions de dollars que Zynga doit dépenser pour développer de nouveaux outils pour déjouer nos capacités d'adaptation, l'entreprise n'a jamais réussi à reproduire l'heureux accident qui lui a permis de retenir toute notre attention pendant un bref instant en 2009. Les centrales comme Supercell se sont un peu mieux comportées, mais elles sont rares et connaissent beaucoup d'échecs pour un seul succès.

La vulnérabilité de petits segments de la population à une manipulation sensible et efficace des entreprises est une préoccupation réelle qui mérite notre attention et notre énergie. Mais ce n'est pas une menace existentielle pour la société.

Si les données sont le nouvel or noir, alors les forages du capitalisme de surveillance ont des fuites



La faculté d'adaptation des internautes explique l’une des caractéristiques les plus alarmantes du capitalisme de surveillance : son insatiable appétit de données et l’expansion infinie de sa capacité à collecter des données au travers de la diffusion de capteurs, de la surveillance en ligne, et de l’acquisition de flux de données de tiers.

Zuboff étudie ce phénomène et conclut que les données doivent valoir très cher si le capitalisme de surveillance en est aussi friand (selon ses termes : « Tout comme le capitalisme industriel était motivé par l’intensification continue des moyens de production, le capitalisme de surveillance et ses acteurs sont maintenant enfermés dans l’intensification continue des moyens de modification comportementale et dans la collecte des instruments de pouvoir. »). Et si cet appétit vorace venait du fait que ces données ont une demi-vie très courte, puisque les gens s’habituent très vite aux nouvelles techniques de persuasion fondées sur les données au point que les entreprises sont engagées dans un bras de fer sans fin avec notre système limbique ? Et si c’était une course de la Reine rouge d’Alice dans laquelle il faut courir de plus en plus vite collecter de plus en plus de données, pour conserver la même place ?

Bien sûr, toutes les techniques de persuasion des géants de la tech travaillent de concert les unes avec les autres, et la collecte de données est utile au-delà de la simple tromperie comportementale.

Si une personne veut vous recruter pour acheter un réfrigérateur ou pour rejoindre un massacre participer à un pogrom, elle peut utiliser le profilage et le ciblage pour envoyer des messages à des gens avec lesquels elle estime avoir de bonnes perspectives commerciales. Ces messages eux-mêmes peuvent être mensongers et promouvoir des thèmes que vous ne connaissez pas bien (la sécurité alimentaire, l'efficacité énergétique, l'eugénisme ou des affirmations historiques sur la supériorité raciale). Elle peut recourir à l'optimisation des moteurs de recherche ou à des armées de faux critiques et commentateurs ou bien encore au placement payant pour dominer le discours afin que toute recherche d'informations complémentaires vous ramène à ses messages. Enfin, elle peut affiner les différents discours en utilisant l'apprentissage machine et d'autres techniques afin de déterminer quel type de discours convient le mieux à quelqu'un comme vous.

Chacune des phases de ce processus bénéficie de la surveillance : plus ils possèdent de données sur vous, plus leur profilage est précis et plus ils peuvent vous cibler avec des messages spécifiques. Pensez à la façon dont vous vendriez un réfrigérateur si vous saviez que la garantie de celui de votre client potentiel venait d'expirer et qu'il allait percevoir un remboursement d'impôts le mois suivant.

De plus, plus ils ont de données, mieux ils peuvent élaborer des messages trompeurs. Si je sais que vous aimez la généalogie, je n'essaierai pas de vous refourguer des thèses pseudo-scientifiques sur les différences génétiques entre les « races », et je m'en tiendrai plutôt aux conspirationnistes habituels du « grand remplacement ».

Facebook vous aide aussi à localiser les gens qui ont les mêmes opinions odieuses ou antisociales que vous. Il permet de trouver d'autres personnes avec qui porter des torches enflammées dans les rues de Charlottesville déguisé en Confédéré. Il peut vous aider à trouver d'autres personnes qui veulent rejoindre votre milice et aller à la frontière pour terroriser les migrants illégaux. Il peut vous aider à trouver d'autres personnes qui pensent aussi que les vaccins sont un poison et que la Terre est plate.

La publicité ciblée profite en réalité uniquement à ceux qui défendent des causes socialement inacceptables car elle est invisible. Le racisme est présent sur toute la planète, et il y a peu d'endroits où les racistes, et seulement eux, se réunissent. C'est une situation similaire à celle de la vente de réfrigérateurs là où les clients potentiels sont dispersés géographiquement, et où il y a peu d'endroits où vous pouvez acheter un encart publicitaire qui sera principalement vu par des acheteurs de frigo. Mais acheter un frigo est acceptable socialement, tandis qu'être un nazi ne l'est pas, donc quand vous achetez un panneau publicitaire ou quand vous faites de la pub dans la rubrique sports d'un journal pour vendre votre frigo, le seul risque c'est que votre publicité soit vue par beaucoup de gens qui ne veulent pas de frigo, et vous aurez jeté votre argent par la fenêtre.

Mais même si vous vouliez faire de la pub pour votre mouvement nazi sur un panneau publicitaire, à la télé en première partie de soirée ou dans les petites annonces de la rubrique sports, vous auriez du mal à trouver quelqu'un qui serait prêt à vous vendre de l'espace pour votre publicité, en partie parce qu'il ne serait pas d'accord avec vos idées, et aussi parce qu'il aurait peur des retombées négatives (boycott, mauvaise image, etc.) de la part de ceux qui ne partagent pas vos opinions.

Ce problème disparaît avec les publicités ciblées : sur Internet, les encarts de publicité peuvent être personnalisés, ce qui veut dire que vous pouvez acheter des publicités qui ne seront montrées qu'à ceux qui semblent être des nazis et pas à ceux qui les haïssent. Quand un slogan raciste est diffusé à quelqu'un qui hait le racisme, il en résulte certaines conséquences, et la plateforme ou la publication peut faire l'objet d'une dénonciation publique ou privée de la part de personnes outrées. Mais la

nature des risques encourus par l'acheteur de publicités en ligne est bien différente des risques encourus par un éditeur ou un propriétaire de panneaux publicitaires classiques qui pourrait vouloir publier une pub nazie.

Les publicités en ligne sont placées par des algorithmes qui servent d'intermédiaires entre un écosystème diversifié de plateformes publicitaires en libre-service où chacun peut acheter une annonce. Ainsi, les slogans nazis qui s'immiscent sur votre site web préféré ne doivent pas être vus comme une atteinte à la morale mais plutôt comme le raté d'un fournisseur de publicité lointain. Lorsqu'un éditeur reçoit une plainte pour une publicité gênante diffusée sur un de ses sites, il peut engager une procédure pour bloquer la diffusion de cette publicité. Mais les nazis pourraient acheter une publicité légèrement différente auprès d'un autre intermédiaire qui diffuse aussi sur ce site. Quoi qu'il en soit, les internautes comprennent de plus en plus que quand une publicité s'affiche sur leur écran, il est probable que l'annonceur n'a pas choisi l'éditeur du site et que l'éditeur n'a pas la moindre idée de qui sont ses annonceurs.
Ces couches d'indétermination entre les annonceurs et les éditeurs tiennent lieu de tampon moral : il y a aujourd'hui un large consensus moral selon lequel les éditeurs ne devraient pas être tenus pour responsables des publicités qui apparaissent sur leurs pages car ils ne choisissent pas directement de les y placer. C'est ainsi que les nazis peuvent surmonter d'importants obstacles pour organiser leur mouvement.

Les données entretiennent une relation complexe avec la domination. La capacité à espionner vos clients peut vous alerter sur leurs préférences pour vos concurrents directs et vous permettre par la même occasion de prendre l'ascendant sur eux.

Mais surtout, si vous pouvez dominer l'espace informationnel tout en collectant des données, alors vous renforcez d'autres stratégies trompeuses, car il devient plus difficile d'échapper à la toile de tromperie que vous tissez. Ce ne sont pas les données elles-mêmes mais la domination, c'est-à-dire le fait d'atteindre, à terme, une position de monopole, qui rend ces stratégies viables, car la domination monopolistique prive votre cible de toute alternative.

Si vous êtes un nazi qui veut s'assurer que ses cibles voient en priorité des informations trompeuses, qui vont se confirmer à mesure que les recherches se poursuivent, vous pouvez améliorer vos chances en leur suggérant des mots-clefs à travers vos communications initiales. Vous n'avez pas besoin de vous positionner sur les dix premiers résultats de la recherche *décourager électeurs de voter* si vous pouvez convaincre vos cibles de n'utiliser que les mots clefs *voter fraud* (fraude électorale), qui retourneront des résultats de recherche très différents.

Les capitalistes de la surveillance sont comme des illusionnistes qui affirment que leur extraordinaire connaissance des comportements humains leur permet de deviner le mot que vous avez noté sur un bout de papier plié et placé dans votre poche, alors qu'en réalité ils s'appuient sur des complices, des caméras cachées, des tours de passe-passe et de leur mémoire développée pour vous bluffer.

Ou peut-être sont-ils des comme des *artistes de la drague,* cette secte misogyne qui promet d'aider les hommes maladroits à coucher avec des femmes en leur apprenant quelques rudiments de programmation neurolinguistique, des techniques de communication non verbale et des stratégies de manipulation psychologique telles que le « *negging* », qui consiste à faire des commentaires dévalorisant aux femmes pour réduire leur amour-propre et susciter leur intérêt.

Certains dragueurs parviennent peut-être à convaincre des femmes de les suivre, mais ce n'est pas parce que ces hommes ont découvert comment court-circuiter l'esprit critique des femmes. Le « succès » des dragueurs vient plutôt du fait qu'ils sont tombés sur des femmes qui n'étaient pas en état d'exprimer leur consentement, des femmes contraintes, des femmes en état d'ébriété, des femmes animées d'une pulsion autodestructrice et de quelques femmes qui, bien que sobres et disposant de toutes leurs facultés, n'ont pas immédiatement compris qu'elles fréquentaient des hommes horribles mais qui ont corrigé cette erreur dès qu'elles l'ont pu.

Les dragueurs se figurent qu'ils ont découvert une formule secrète qui court-circuite les facultés critiques l'esprit critique des femmes, mais ce n'est pas le cas. La plupart des stratégies qu'ils déploient, comme le *negging*, sont devenues des sujets de plaisanteries (tout comme les gens plaisantent à propos des mauvaises campagnes publicitaires) et il est fort probable que ceux qui mettent en pratique ces stratégies avec les femmes ont de fortes chances d'être aussitôt démasqués, jetés et considérés comme de gros losers.

Les *dragueurs* sont la preuve que les gens peuvent croire qu'ils ont développé un système de contrôle de l'esprit même s'il ne marche pas. Ils s'appuient simplement sur le fait qu'une technique qui fonctionne une fois sur un million peut finir par se révéler payante si vous l'essayez un million de fois. Ils considèrent qu'ils ont juste mal appliqué la technique les autres 999 999 fois et se jurent de faire mieux la prochaine fois. Seul un groupe de personnes trouve ces histoires de *dragueurs* convaincantes, les aspirants *dragueurs*, que l'anxiété et l'insécurité rend vulnérables aux escrocs et aux cinglés qui les persuadent que, s'ils payent leur mentorat et suivent leurs instructions, ils réussiront un jour. Les *dragueurs* considèrent que, s'ils ne parviennent pas à séduire les femmes, c'est parce qu'ils ne sont pas de bons *dragueurs*, et non parce que les techniques *de drague* sont du grand n'importe quoi. Les *dragueurs* ne parviennent pas à se vendre auprès des femmes, mais ils sont bien meilleurs pour se vendre auprès des hommes qui payent pour apprendre leurs soi-disant techniques de séduction.

« Je sais que la moitié des sommes que je dépense en publicité l'est en pure perte mais je ne sais pas de quelle moitié il s'agit. » déplorait John Wanamaker, pionnier des grands magasins.

Le fait que Wanamaker considérait que la moitié seulement de ses dépenses publicitaires avait été gaspillée témoigne de la capacité de persuasion des cadres commerciaux, qui sont bien meilleurs pour convaincre de potentiels clients d'acheter leurs services que pour convaincre le grand public d'acheter les produits de leurs clients.

Qu’est-ce que Facebook ?

On considère Facebook comme l’origine de tous nos fléaux actuels, et il n’est pas difficile de comprendre pourquoi. Certaines entreprises technologiques cherchent à enfermer leurs utilisateurs mais font leur beurre en gardant le monopole sur l’accès aux applications pour leurs appareils et en abusant largement sur leurs tarifs plutôt qu’en espionnant leurs clients (c’est le cas d’Apple). D’autres ne cherchent pas à enfermer leurs utilisateurs et utilisatrices parce que ces entreprises ont bien compris comment les espionner où qu’ils soient et quoi qu’elles fassent, et elles gagnent de l’argent avec cette surveillance (Google). Seul Facebook, parmi les géants de la tech, fait reposer son business à la fois sur le verrouillage de ses utilisateurs et leur espionnage constant.

Le type de surveillance qu’exerce Facebook est véritablement sans équivalent dans le monde occidental. Bien que Facebook s’efforce de se rendre le moins visible possible sur le Web public, en masquant ce qui s’y passe aux yeux des gens qui ne sont pas connectés à Facebook, l’entreprise a disposé des pièges sur la totalité du Web avec des outils de surveillance, sous forme de boutons « J’aime » que les producteurs de contenus insèrent sur leur site pour doper leur profil Facebook. L’entreprise crée également diverses bibliothèques logicielles et autres bouts de code à l’attention des développeurs qui fonctionnent comme des mouchards sur les pages où on les utilise (journaux parcourus, sites de rencontres, forums…), transmettant à Facebook des informations sur les visiteurs du site.

Les géants de la tech peuvent surveiller, non seulement parce qu’ils font de la tech mais aussi parce que ce sont des géants.

Facebook offre des outils du même genre aux développeurs d’applications, si bien que les applications que vous utilisez, que ce soit des jeux, des applis pétomanes, des services d’évaluation des entreprises ou du suivi scolaire enverront des informations sur vos activités à Facebook même si vous n’avez pas de compte Facebook, et même si vous n’utilisez ni ne téléchargez aucune application Facebook. Et par-dessus le marché, Facebook achète des données à des tiers pour connaître les habitudes d’achat, la géolocalisation, l’utilisation de cartes de fidélité, les transactions bancaires, etc., puis croise ces données avec les dossiers constitués d’après les activités sur Facebook, avec les applications et sur le Web général.

S’il est simple d’intégrer des éléments web dans Facebook – faire un lien vers un article de presse, par exemple – les produits de Facebook ne peuvent en général pas être intégrés sur le Web. Vous pouvez inclure un tweet dans une publication Facebook, mais si vous intégrez une publication Facebook dans un tweet, tout ce que vous obtiendrez est un lien vers Facebook qui vous demande de vous authentifier avant d’y accéder. Facebook a eu recours à des contre-mesures techniques et légales radicales pour que ses concurrents ne puissent pas donner la possibilité à leurs utilisateurs d’intégrer des fragments de Facebook dans des services rivaux, ou de créer des interfaces alternatives qui fusionneraient votre messagerie Facebook avec celle des autres services que vous utilisez.

Et Facebook est incroyablement populaire, avec 2,3 milliards d’utilisateurs annoncés (même si beaucoup considèrent que ce nombre est exagéré). Facebook a été utilisé pour organiser des pogroms génocidaires, des émeutes racistes, des mouvements antivaccins, des théories de la Terre plate et la carrière politique des autocrates les plus horribles et les plus autoritaires au monde. Des choses réellement alarmantes se produisent dans le monde et Facebook est impliqué dans bon nombre d’entre elles, il est donc assez facile de conclure que ces choses sont le résultat du système de contrôle mental de Facebook, mis à disposition de toute personne prête à y dépenser quelques dollars.

Pour comprendre le rôle joué par Facebook dans l’élaboration et la mobilisation des mouvements nuisibles à la société, nous devons comprendre la double nature de Facebook.

Parce qu’il a beaucoup d’utilisateurs et beaucoup de données sur ces utilisateurs, l’outil Facebook est très efficace pour identifier des personnes avec des caractéristiques difficiles à trouver, le genre de caractéristiques qui sont suffisamment bien disséminées dans la population pour que les publicitaires aient toujours eu du mal à les atteindre de manière rentable.

Revenons aux réfrigérateurs. La plupart d’entre nous ne remplaçons notre gros électro-ménager qu’un petit nombre de fois dans nos vies. Si vous êtes un fabricant ou un vendeur de réfrigérateurs, il n’y a que ces brèves fenêtres temporelles dans la vie des consommateurs au cours desquelles ils réfléchissent à un achat, et vous devez trouver un moyen pour les atteindre. Toute personne ayant déjà enregistré un changement de titre de propriété après l’achat d’une maison a pu constater que les fabricants d’électroménager s’efforcent avec l’énergie du désespoir d’atteindre quiconque pourrait la moindre chance d’être à la recherche d’un nouveau frigo.

Facebook rend la recherche d’acheteurs de réfrigérateurs beaucoup plus facile. Il permet de cibler des publicités à destination des personnes ayant enregistré l’achat d’une nouvelle maison, des personnes qui ont cherché des conseils pour l’achat de réfrigérateurs, de personnes qui se sont plaintes du dysfonctionnement de leur frigo, ou n’importe quelle combinaison de celles-ci. Il peut même cibler des personnes qui ont récemment acheté d’autres équipements de cuisine, en faisant l’hypothèse que quelqu’un venant de remplacer son four et son lave-vaisselle pourrait être d’humeur à acheter un frigo. La grande majorité des personnes qui sont ciblées par ces publicités ne seront pas à la recherche d’un nouveau frigo mais – et c’est le point crucial – le pourcentage de personnes à la recherche de frigo que ces publicités atteignent est bien plus élevé que celui du groupe atteint par les techniques traditionnelles de ciblage marketing hors-ligne.

Facebook rend également beaucoup plus simple le fait de trouver des personnes qui ont la même maladie rare que vous, ce qui aurait été peut-être impossible avant, le plus proche compagnon d’infortune pouvant se trouver à des centaines de kilomètres. Il rend plus simple de retrouver des

personnes qui sont allées dans le même lycée que vous, bien que des décennies se soient écoulées et que vos anciens camarades se soient disséminés aux quatre coins de la planète.

Facebook rend également beaucoup plus simple de trouver des personnes ayant les mêmes opinions politiques minoritaires que vous. Si vous avez toujours eu une affinité secrète pour le socialisme, sans jamais oser la formuler à voix haute de peur de vous aliéner vos voisins, Facebook peut vous aider à découvrir d'autres personnes qui pensent la même chose que vous (et cela pourrait vous démontrer que votre affinité est plus commune que vous ne l'auriez imaginée). Il peut rendre plus facile de trouver des personnes qui ont la même identité sexuelle que vous. Et, à nouveau, il peut vous aider à comprendre que ce que vous considériez comme un secret honteux qui ne regarde que vous est en réalité un trait répandu, vous donnant ainsi le réconfort et le courage nécessaire pour en parler à vos proches.

Tout cela constitue un dilemme pour Facebook : le ciblage rend les publicités de la plateforme plus efficaces que les publicités traditionnelles, mais il permet également aux annonceurs de savoir précisément à quel point leurs publicités sont efficaces. Si les annonceurs sont satisfaits d'apprendre que les publicités de Facebook sont plus efficaces que celles de systèmes au ciblage moins perfectionné, les annonceurs peuvent aussi voir que, dans presque tous les cas, les personnes qui voient leurs publicités les ignorent. Ou alors, tout au mieux, que leurs publicités ne fonctionnent qu'à un niveau inconscient, créant des effets nébuleux impossibles à quantifier comme la « reconnaissance de marque ». Cela signifie que le prix par publicité est très réduit dans la quasi-totalité des cas.

Pour ne rien arranger, beaucoup de groupes Facebook n'hébergent que très peu de discussions. Votre équipe de football locale, les personnes qui ont la même maladie rare que vous et ceux dont vous partagez l'orientation politique peuvent échanger des rafales de messages dans les moments critiques forts mais, dans la vie de tous les jours, il n'y a pas grand-chose à raconter à vos anciens camarades de lycée et autres collectionneurs de vignettes de football.

S'il n'y avait que des discussions « saines », Facebook ne générerait pas assez de trafic pour vendre des publicités et amasser ainsi les sommes nécessaires pour continuellement se développer en rachetant ses concurrents, tout en reversant de coquettes sommes à ses investisseurs.

Facebook doit donc augmenter le trafic tout en détournant ses propres forums de discussion : chaque fois que l'algorithme de Facebook injecte de la matière à polémiques dans un groupe – brûlots politiques, théories du complot, faits-divers révoltants – il peut détourner l'objectif initial de ce groupe avec des discussions affligeantes et gonfler ainsi artificiellement ces échanges en les transformant en interminables disputes agressives et improductives. Facebook est optimisé pour l'engagement, pas pour le bonheur, et il se trouve que les systèmes automatisés sont plutôt performants pour trouver des choses qui vont mettre les gens en colère.

Facebook peut modifier notre comportement mais seulement en suivant quelques modalités ordinaires. Tout d'abord, il peut vous enfermer avec vos amis et votre famille pour que vous passiez votre temps à vérifier sans cesse sur Facebook ce qu'ils sont en train de faire. Ensuite, il peut vous mettre en colère ou vous angoisser. Il peut vous forcer à choisir entre être constamment interrompu par des mises à jour, un processus qui vous déconcentre et vous empêche de réfléchir, et rester indéfiniment en contact avec vos amis. Il s'agit donc d'une forme de contrôle mental très limitée, qui ne peut nous rendre que furieux, déprimés et angoissés.

C’est pourquoi les systèmes de ciblage de Facebook – autant ceux qu’il montre aux annonceurs que ceux qui permettent aux utilisateurs de trouver des personnes qui partagent les mêmes centres d’intérêt – sont si modernes, souples et faciles à utiliser, tandis que ses forums de discussion ont des fonctionnalités qui paraissent inchangées depuis le milieu des années 2000. Si Facebook offrait à ses utilisateurs un système de lecture de messages tout aussi souple et sophistiqué, ceux-ci pourraient se défendre contre les gros titres polémiques sur Donald Trump qui leur font saigner des yeux.

Plus vous passez de temps sur Facebook, plus il a de pubs à vous montrer. Comme les publicités sur Facebook ne marchent qu’une fois sur mille, leur solution est de tenter de multiplier par mille le temps que vous y passez. Au lieu de considérer Facebook comme une entreprise qui a trouvé un moyen de vous montrer la bonne publicité en obtenant de vous exactement ce que veulent les annonceurs publicitaires, considérez que c’est une entreprise qui sait parfaitement comment vous noyer dans un torrent permanent de controverses, même si elles vous rendent malheureux, de sorte que vous passiez tellement de temps sur le site que vous finissiez par voir au moins une pub qui va fonctionner pour vous.

Les monopoles et le droit au futur

Mme Zuboff et ceux qui la suivent sont particulièrement alarmés par l’influence de la surveillance des entreprises sur nos décisions. Cette influence nous prive de ce qu’elle appelle poétiquement « le droit au futur », c’est-à-dire le droit de décider par vous-même de ce que vous ferez à l’avenir.

Il est vrai que la publicité peut faire pencher la balance d’une manière ou d’une autre : lorsque vous envisagez d’acheter un frigo, une publicité pour un frigo qui vient juste à point peut mettre fin tout de suite à vos recherches. Mais Zuboff accorde un poids énorme et injustifié au pouvoir de persuasion des techniques d’influence basées sur la surveillance. La plupart d’entre elles ne fonctionnent pas très bien, et celles qui le font ne fonctionneront pas très longtemps. Les concepteurs de ces outils sont persuadés qu’ils les affineront un jour pour en faire des systèmes de contrôle total, mais on peut difficilement les considérer comme des observateurs sans parti-pris, et les risques que leurs rêves se réalisent sont très limités. En revanche, Zuboff est plutôt optimiste quant aux quarante années de pratiques antitrust laxistes qui ont permis à une poignée d’entreprises

de dominer le Web, inaugurant une ère de l'information avec, comme l'a fait remarquer quelqu'un sur Twitter, cinq portails web géants remplis chacun de captures d'écran des quatre autres.

Cependant, si l'on doit s'inquiéter parce qu'on risque de perdre le droit de choisir nous-mêmes de quoi sera fait notre avenir, alors les préjudices tangibles et immédiats devraient être au cœur de nos débats sur les politiques technologiques, et non les préjudices potentiels décrit par Zuboff.

Commençons avec la « gestion des droits numériques ». En 1998, Bill Clinton promulgue le Digital Millennium Copyright Act (DMCA) https://fr.wikipedia.org/wiki/Digital_Millennium_Copyright_Act. Cette loi complexe comporte de nombreuses clauses controversées, mais aucune ne l'est plus que la section 1201, la règle « anti-contournement ».

Il s'agit d'une interdiction générale de modifier les systèmes qui limitent l'accès aux œuvres protégées par le copyright. L'interdiction est si stricte qu'elle interdit de retirer le verrou de copyright même si aucune violation de copyright n'a eut lieu. C'est dans la conception même du texte : les activités, que l'article 1201 du DMCA vise à interdire, ne sont pas des violations du copyright ; il s'agit plutôt d'activités légales qui contrarient les plans commerciaux des fabricants.

Par exemple, la première application majeure de la section 1201 a visé les lecteurs de DVD comme moyen de faire respecter le codage par « région » intégré dans ces appareils https://fr.wikipedia.org/wiki/Code_de_r%C3 %A9gion_DVD. Le DVD-CCA, l'organisme qui a normalisé les DVD et les lecteurs de DVD, a divisé le monde en six régions et a précisé que les lecteurs de DVD doivent vérifier chaque disque pour déterminer dans quelles régions il est autorisé à être lu. Les lecteurs de DVD devaient avoir leur propre région correspondante (un lecteur de DVD acheté aux États-Unis serait de la région 1, tandis qu'un lecteur acheté en Inde serait de la région 5). Si le lecteur et la région du disque correspondent, le lecteur lira le disque ; sinon, il le rejettera.

Pourtant, regarder un DVD acheté légalement dans un autre pays que celui dans lequel vous vous situez n'est pas une violation de copyright – bien au contraire. Les lois du copyright n'imposent qu'une seule obligation aux consommateurs de films : vous devez aller dans un magasin, trouver un DVD autorisé, et payer le prix demandé. Si vous faites cela – et rien de plus – tout ira bien.

Le fait qu'un studio de cinéma veuille faire payer les Indiens moins cher que les Américains, ou sortir un film plus tard en Australie qu'au Royaume-Uni n'a rien à voir avec les lois sur le copyright. Une fois que vous avez légalement acquis un DVD, ce n'est pas une violation du copyright que de le regarder depuis l'endroit où vous vous trouvez.

Donc les producteurs de DVD et de lecteurs de disques ne pourraient pas employer les accusations de complicité de violations du copyright pour punir les producteurs de lecteurs lisant des disques de n'importe quelle région, ou les ateliers de réparation qui ont modifié les lecteurs pour vous laisser regarder des disques achetés hors de votre région, ou encore les développeurs de logiciels qui ont créé des programmes pour vous aider à le faire.
C'est là que la section 1201 du DCMA entre en jeu : en interdisant de toucher aux contrôles d'accès, la loi a donné aux producteurs et aux ayants droit la possibilité de poursuivre en justice leurs concurrents qui produisent des produits supérieurs avec des caractéristiques très demandées par le marché (en l'occurrence, des lecteurs de disques sans restriction de région).

C’est une arnaque ignoble contre les consommateurs, mais, avec le temps, le champ de la section 1201 s’est étendu pour inclure toute une constellation grandissante d’appareils et de services, car certains producteurs malins ont compris un certain nombre de choses :

- Tout appareil doté d’un logiciel contient une « œuvre protégée par copyright » (le logiciel en question).
- Un appareil peut être conçu pour pouvoir reconfigurer son logiciel et contourner le « moyen de contrôle d’accès à une œuvre protégée par copyright », un délit d’après la section 1201.
- Par conséquent, les entreprises peuvent contrôler le comportement de leurs consommateurs après qu’ils ont rapporté leurs achats à la maison. Elles peuvent en effet concevoir des produits pour que toutes les utilisations interdites demandent des modifications qui tombent sous le coup de la section 1201.

Cette section devient alors un moyen pour tout fabricant de contraindre ses clients à agir au profit de leurs actionnaires plutôt que dans l’intérêt des clients.
Cela se manifeste de nombreuses façons : une nouvelle génération d’imprimantes à jet d’encre utilisant des contre-mesures qui empêchent l’utilisation d’encre d’autres marques et qui ne peuvent être contournées sans risques juridiques, ou des systèmes similaires dans les tracteurs qui empêchent les réparateurs d’échanger les pièces du fabricant, car elles ne sont pas reconnues par le système du tracteur tant qu’un code de déverrouillage du fabricant n’est pas saisi.

Plus proches des particuliers, les iPhones d’Apple utilisent ces mesures pour empêcher à la fois les services de tierce partie et l’installation de logiciels tiers. Cela permet à Apple, et non à l’acheteur de l’iPhone, de décider quand celui-ci est irréparable et doit être réduit en pièces et jeté en déchetterie (l’entreprise Apple est connue pour sa politique écologiquement catastrophique qui consiste à détruire les vieux appareils électroniques plutôt que de permettre leur recyclage pour en récupérer les pièces). C’est un pouvoir très utile à exercer, surtout à la lumière de l’avertissement du PDG Tim Cook aux investisseurs en janvier 2019 : les profits de la société sont en danger si les clients choisissent de conserver leur téléphone plutôt que de le remplacer.
L’utilisation par Apple de verrous de copyright lui permet également d’établir un monopole sur la manière dont ses clients achètent des logiciels pour leurs téléphones. Les conditions commerciales de l’App Store garantissent à Apple une part de tous les revenus générés par les applications qui y sont vendues, ce qui signifie qu’Apple gagne de l’argent lorsque vous achetez une application dans son magasin et continue à gagner de l’argent chaque fois que vous achetez quelque chose en utilisant cette application. Cette situation retombe au final sur les développeurs de logiciels, qui doivent soit facturer plus cher, soit accepter des profits moindres sur leurs produits.

Il est important de comprendre que l’utilisation par Apple des verrous de copyright lui donne le pouvoir de prendre des décisions éditoriales sur les applications que vous pouvez ou ne pouvez pas installer sur votre propre appareil. Apple a utilisé ce pouvoir pour rejeter les dictionnaires qui contiennent des mots obscènes ; ou pour limiter certains discours politiques, en particulier les applications qui diffusent des propos politiques controversés, comme cette application qui vous avertit chaque fois qu’un drone américain tue quelqu’un quelque part dans le monde ; ou pour s’opposer à un jeu qui commente le conflit israélo-palestinien.

Apple justifie souvent son pouvoir monopolistique sur l’installation de logiciels au nom de la sécurité, en arguant que le contrôle des applications de sa boutique lui permet de protéger ses utilisateurs contre les applications qui contiennent du code qui surveille les utilisateurs. Mais ce

pouvoir est à double tranchant. En Chine, le gouvernement a ordonné à Apple d'interdire la vente d'outils de protection de vie privée, comme les VPN, à l'exception de ceux dans lesquels des failles de sécurité ont délibérément été introduites pour permettre à l'État chinois d'écouter les utilisateurs. Étant donné qu'Apple utilise des contre-mesures technologiques – avec des mesures de protection légales – pour empêcher les clients d'installer des applications non autorisées, les propriétaires chinois d'iPhone ne peuvent pas facilement (ou légalement) se connecter à des VPN qui les protégeraient de l'espionnage de l'État chinois.

Zuboff décrit le capitalisme de surveillance comme un « capitalisme voyou ». Les théoriciens du capitalisme prétendent que sa vertu est d'agréger des informations relatives aux décisions des consommateurs, produisant ainsi des marchés efficaces. Le prétendu pouvoir du capitalisme de surveillance, de priver ses victimes de leur libre-arbitre grâce à des campagnes d'influence surchargées de calculs, signifie que nos marchés n'agrègent plus les décisions des consommateurs parce que nous, les clients, ne décidons plus – nous sommes aux ordres des rayons de contrôle mental du capitalisme de surveillance.

Si notre problème c'est que les marchés cessent de fonctionner lorsque les consommateurs ne peuvent plus faire de choix, alors les verrous du copyright devraient nous préoccuper au moins autant que les campagnes d'influence. Une campagne d'influence peut vous pousser à acheter une certaine marque de téléphone, mais les verrous du copyright sur ce téléphone déterminent où vous pouvez l'utiliser, quelles applications peuvent fonctionner dessus et quand vous devez le jeter plutôt que le réparer.

Le classement des résultats de recherche et le droit au futur

Les marchés sont parfois présentés comme une sorte de formule magique : en découvrant des informations qui pourraient rester cachées mais sont transmises par le libre choix des consommateurs, les connaissances locales de ces derniers sont intégrées dans un système auto-correcteur qui améliore les correspondances entre les résultats – de manière plus efficace que ce qu'un ordinateur pourrait calculer. Mais les monopoles sont incompatibles avec ce processus. Lorsque vous n'avez qu'un seul magasin d'applications, c'est le propriétaire du magasin, et non le consommateur, qui décide de l'éventail des choix. Comme l'a dit un jour Boss Tweed « peu importe qui gagne les élections, du moment que c'est moi qui fais les nominations ». Un marché monopolistique est une élection dont les candidats sont choisis par le monopole.

Ce trucage des votes est rendu plus toxique par l'existence de monopoles sur le classement des résultats. La part de marché de Google dans le domaine de la recherche est d'environ 90 %. Lorsque l'algorithme de classement de Google place dans son top 10 un résultat pour un terme de recherche populaire, cela détermine le comportement de millions de personnes. Si la réponse de Google à la question « Les vaccins sont-ils dangereux ? » est une page qui réfute les théories du complot anti-vax, alors une partie non négligeable du grand public apprendra que les vaccins sont sûrs. Si, en revanche, Google envoie ces personnes sur un site qui met en avant les conspirations anti-vax, une part non-négligeable de ces millions de personnes ressortira convaincue que les vaccins sont dangereux.

L'algorithme de Google est souvent détourné pour fournir de la désinformation comme principal résultat de recherche. Mais dans ces cas-là, Google ne persuade pas les gens de changer d'avis, il ne

fait que présenter quelque chose de faux comme une vérité alors même que l'utilisateur n'a aucune raison d'en douter.

C'est vrai peu importe que la recherche porte sur « Les vaccins sont-ils dangereux ? » ou bien sur « meilleurs restaurants près de chez moi ». La plupart des utilisateurs ne regarderont jamais au-delà de la première page de résultats de recherche, et lorsque l'écrasante majorité des gens utilisent le même moteur de recherche, l'algorithme de classement utilisé par ce moteur de recherche aura déterminé une myriade de conséquences (adopter ou non un enfant, se faire opérer du cancer, où dîner, où déménager, où postuler pour un emploi) dans une proportion qui dépasse largement les résultats comportementaux dictés par les techniques de persuasion algorithmiques.

Beaucoup des questions que nous posons aux moteurs de recherche n'ont pas de réponses empiriquement correctes : « Où pourrais-je dîner ? » n'est pas une question objective. Même les questions qui ont des réponses objectives (« Les vaccins sont-ils dangereux ? ») n'ont pas de source empiriquement supérieure pour ces réponses. De nombreuses pages confirment l'innocuité des vaccins, alors laquelle afficher en premier ? Selon les règles de la concurrence, les consommateurs peuvent choisir parmi de nombreux moteurs de recherche et s'en tenir à celui dont le verdict algorithmique leur convient le mieux, mais en cas de monopole, nos réponses proviennent toutes du même endroit.

La domination de Google dans le domaine de la recherche n'est pas une simple question de mérite : pour atteindre sa position dominante, l'entreprise a utilisé de nombreuses tactiques qui auraient été interdites en vertu des normes antitrust classiques d'avant l'ère Reagan. Après tout, il s'agit d'une entreprise qui a développé deux produits majeurs : un très bon moteur de recherche et un assez bon clone de Hotmail. Tous ses autres grands succès, Android, YouTube, Google Maps, etc., ont été obtenus grâce à l'acquisition d'un concurrent naissant. De nombreuses branches clés de l'entreprise, comme la technologie publicitaire DoubleClick, violent le principe historique de séparation structurelle de la concurrence, qui interdisait aux entreprises de posséder des filiales en concurrence avec leurs clients. Les chemins de fer, par exemple, se sont vus interdire la possession de sociétés de fret qui auraient concurrencé les affréteurs dont ils transportent le fret.

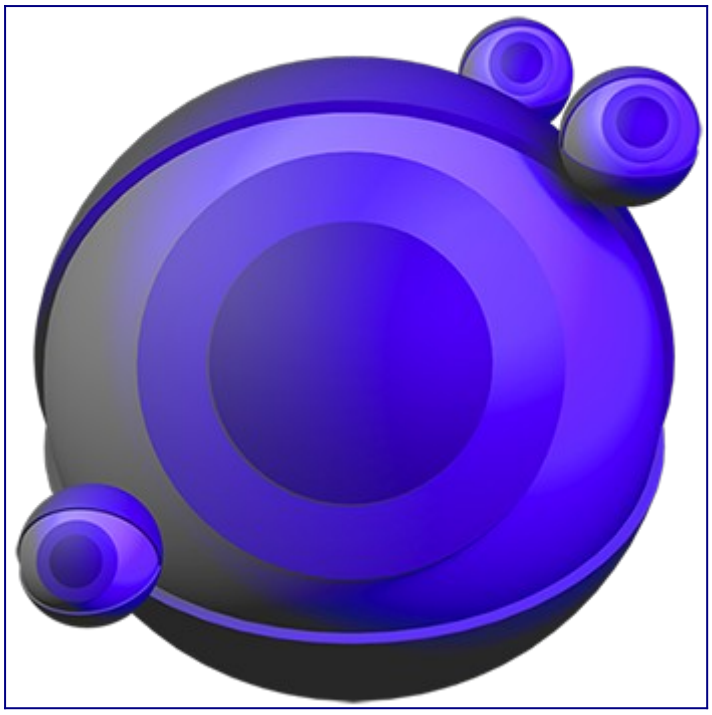
Si nous craignons que les entreprises géantes ne détournent les marchés en privant les consommateurs de leur capacité à faire librement leurs choix, alors une application rigoureuse de la législation antitrust semble être un excellent remède. Si nous avions refusé à Google le droit d'effectuer ses nombreuses fusions, nous lui aurions probablement aussi refusé sa domination totale dans le domaine de la recherche. Sans cette domination, les théories, préjugés et erreurs (et le bon jugement aussi) des ingénieurs de recherche et des chefs de produits de Google n'auraient pas eu un effet aussi disproportionné sur le choix des consommateurs..

Cela vaut pour beaucoup d'autres entreprises. Amazon, l'entreprise type du capitalisme de surveillance, est évidemment l'outil dominant pour la recherche sur Amazon, bien que de nombreuses personnes arrivent sur Amazon après des recherches sur Google ou des messages sur Facebook. Évidemment, Amazon contrôle la recherche sur Amazon. Cela signifie que les choix éditoriaux et intéressés d'Amazon, comme la promotion de ses propres marques par rapport aux produits concurrents de ses vendeurs, ainsi que ses théories, ses préjugés et ses erreurs, déterminent une grande partie de ce que nous achetons sur Amazon. Et comme Amazon est le détaillant dominant du commerce électronique en dehors de la Chine et qu'elle a atteint cette domination en rachetant à la fois de grands rivaux et des concurrents naissants au mépris des règles antitrust

historiques, nous pouvons reprocher à ce monopole de priver les consommateurs de leur droit à l'avenir et de leur capacité à façonner les marchés en faisant des choix raisonnés.

Tous les monopoles ne sont pas des capitalistes de surveillance, mais cela ne signifie pas qu'ils ne sont pas capables de façonner les choix des consommateurs de multiples façons. Zuboff fait l'éloge d'Apple pour son App Store et son iTunes Store, en insistant sur le fait qu'afficher le prix des fonctionnalités de ses plateformes était une recette secrète pour résister à la surveillance et ainsi créer de nouveaux marchés. Mais Apple est le seul détaillant autorisé à vendre sur ses plateformes, et c'est le deuxième plus grand vendeur d'appareils mobiles au monde. Les éditeurs de logiciels indépendants qui vendent sur le marché d'Apple accusent l'entreprise des mêmes vices de surveillance qu'Amazon et autres grands détaillants : espionner ses clients pour trouver de nouveaux produits lucratifs à lancer, utiliser efficacement les éditeurs de logiciels indépendants comme des prospecteurs de marché libre, puis les forcer à quitter tous les marchés qu'ils découvrent.

Avec l'utilisation des verrous de copyright, les clients qui possèdent un iPhone ne sont pas légalement autorisés à changer de distributeurs d'applications. Apple, évidemment, est la seule entité qui peut décider de la manière dont elle classe les résultats de recherche sur son store. Ces décisions garantissent que certaines applications sont souvent installées (parce qu'elles apparaissent dès la première page) et d'autres ne le sont jamais (parce qu'elles apparaissent sur la millionième page). Les décisions d'Apple en matière de classement des résultats de recherche ont un impact bien plus important sur les comportements des consommateurs que les campagnes d'influence des robots publicitaires du capitalisme de surveillance.



Les monopoles ont les moyens d’endormir les chiens de garde

Les idéologues du marché les plus fanatiques sont les seuls à penser que les marchés peuvent s’autoréguler sans contrôle de l’État. Pour rester honnêtes, les marchés ont besoin de chiens de garde : régulateurs, législateurs et autres représentants du contrôle démocratique. Lorsque ces

chiens de garde s'endorment sur la tâche, les marchés cessent d'agréger les choix des consommateurs parce que ces choix sont limités par des activités illégitimes et trompeuses dont les entreprises peuvent se servir sans risques parce que personne ne leur demande des comptes.

Mais ce type de tutelle réglementaire a un coût élevé. Dans les secteurs concurrentiels, où la concurrence passe son temps à grappiller les marges des autres, les entreprises individuelles n'ont pas les excédents de capitaux nécessaires pour faire pression efficacement en faveur de lois et de réglementations qui serviraient leurs objectifs.

Beaucoup des préjudices causés par le capitalisme de surveillance sont le résultat d'une réglementation trop faible ou même inexistante. Ces vides réglementaires viennent du pouvoir des monopoles qui peuvent s'opposer à une réglementation plus stricte et adapter la réglementation existante pour continuer à exercer leurs activités telles quelles.

Voici un exemple : quand les entreprises collectent trop de données et les conservent trop longtemps, elles courent un risque accru de subir une fuite de données. En effet, vous ne pouvez pas divulguer des données que vous n'avez jamais collectées, et une fois que vous avez supprimé toutes les copies de ces données, vous ne pouvez plus risquer de les fuiter. Depuis plus d'une décennie, nous assistons à un festival ininterrompu de fuites de données de plus en plus graves, plus effrayantes les unes que les autres de par l'ampleur des violations et la sensibilité des données concernées.

Mais les entreprises persistent malgré tout à moissonner et conserver en trop grand nombre nos données pour trois raisons :

1. Elles sont enfermées dans cette course aux armements émotionnels (évoquée plus haut) avec notre capacité à renforcer nos systèmes de défense attentionnelle pour résister à leurs nouvelles techniques de persuasion. Elles sont également enfermées dans une course à l'armement avec leurs concurrents pour trouver de nouvelles façons de cibler les gens. Dès qu'elles découvrent un point faible dans nos défenses attentionnelles (une façon contre-intuitive et non évidente de cibler les acheteurs potentiels de réfrigérateurs), le public commence à prendre conscience de la tactique, et leurs concurrents s'y mettent également, hâtant le jour où tous les acheteurs potentiels de réfrigérateurs auront été initiés à cette tactique.

2. Elles souscrivent à cette belle croyance qu'est le capitalisme de surveillance. Les données sont peu coûteuses à agréger et à stocker, et les partisans, tout comme les opposants, du capitalisme de surveillance ont assuré aux managers et concepteurs de produits que si vous collectez suffisamment de données, vous pourrez pratiquer la sorcellerie du marketing pour contrôler les esprits ce qui fera grimper vos ventes. Même si vous ne savez pas comment tirer profit de ces données, quelqu'un d'autre finira par vous proposer de vous les acheter pour essayer. C'est la marque de toutes les bulles économiques : acquérir un bien en supposant que quelqu'un d'autre vous l'achètera à un prix plus élevé que celui que vous avez payé, souvent pour le vendre à quelqu'un d'autre à un prix encore plus élevé.

3. Les sanctions pour fuite de données sont négligeables. La plupart des pays limitent ces pénalités aux dommages réels, ce qui signifie que les consommateurs dont les données ont fuité doivent prouver qu'ils ont subi un préjudice financier réel pour obtenir réparation. En 2014, Home Depot a révélé qu'ils avaient perdu les données des cartes de crédit de 53 millions de ses clients, mais a réglé l'affaire en payant ces clients environ 0,34 $ chacun – et un tiers de ces 0,34 $ n'a même pas

été payé en espèces. Cette réparation s'est matérialisée sous la forme d'un crédit pour se procurer un service de contrôle de crédit largement inefficace.

Mais les dégâts causés par les fuites sont beaucoup plus importants que ce que peuvent traiter ces règles sur les dommages réels. Les voleurs d'identité et les fraudeurs sont rusés et infiniment inventifs. Toutes les grandes fuites de données de notre époque sont continuellement recombinées, les ensembles de données sont fusionnés et exploités pour trouver de nouvelles façons de s'en prendre aux propriétaires de ces données. Toute politique raisonnable, fondée sur des preuves, de la dissuasion et de l'indemnisation des violations ne se limiterait pas aux dommages réels, mais permettrait plutôt aux utilisateurs de réclamer compensation pour ces préjudices à venir.

Quoi qu'il en soit, même les réglementations les plus ambitieuses sur la protection de la vie privée, telles que le règlement général de l'UE sur la protection des données, sont loin de prendre en compte les conséquences négatives de la collecte et de la conservation excessives et désinvoltes des données par les plateformes, et les sanctions qu'elles prévoient ne sont pas appliquées de façon assez agressive par ceux qui doivent les appliquer.

Cette tolérance, ou indifférence, à l'égard de la collecte et de la conservation excessives des données peut être attribuée en partie à la puissance de lobbying des plateformes. Ces plateformes sont si rentables qu'elles peuvent facilement se permettre de détourner des sommes gigantesques pour lutter contre tout changement réel – c'est-à-dire un changement qui les obligerait à internaliser les coûts de leurs activités de surveillance.
Et puis il y a la surveillance d'État, que l'histoire du capitalisme de surveillance rejette comme une relique d'une autre époque où la grande inquiétude était d'être emprisonné pour un discours subversif, et non de voir son libre-arbitre dépouillé par l'apprentissage machine.

Mais la surveillance d'État et la surveillance privée sont intimement liées. Comme nous l'avons vu lorsque Apple a été enrôlé par le gouvernement chinois comme collaborateur majeur de la surveillance d'État. La seule manière abordable et efficace de mener une surveillance de masse à l'échelle pratiquée par les États modernes, qu'ils soient « libres » ou autocratiques, est de mettre sous leur coupe les services commerciaux.

Toute limitation stricte du capitalisme de surveillance paralyserait la capacité de surveillance d'État, qu'il s'agisse de l'utilisation de Google comme outil de localisation par les forces de l'ordre locales aux États-Unis ou du suivi des médias sociaux par le Département de la sécurité intérieure pour constituer des dossiers sur les participants aux manifestations contre la politique de séparation des familles des services de l'immigration et des douanes (ICE).

Sans Palantir, Amazon, Google et autres grands entrepreneurs technologiques, les flics états-uniens ne pourraient pas espionner la population noire comme ils le font, l'ICE ne pourrait pas gérer la mise en cage des enfants à la frontière américaine et les systèmes d'aides sociales des États ne pourraient pas purger leurs listes en déguisant la cruauté en empirisme et en prétendant que les personnes pauvres et vulnérables n'ont pas droit à une aide. On peut attribuer à cette relation symbiotique une partie de la réticence des États à prendre des mesures significatives pour réduire la surveillance. Il n'y a pas de surveillance d'État de masse sans surveillance commerciale de masse.

Le monopole est la clé du projet de surveillance massive d'État. Il est vrai que les petites entreprises technologiques sont susceptibles d'être moins bien défendues que les grandes, dont les experts en sécurité font partie des meilleurs dans leur domaine, elles disposent également d'énormes ressources pour sécuriser et surveiller leurs systèmes contre les intrusions. Mais les petites

entreprises ont également moins à protéger : moins d'utilisateurs, des données plus fragmentées sur un plus grand nombre de systèmes et qui doivent être demandées une par une par les acteurs étatiques.

Un secteur technologique centralisé qui travaille avec les autorités est un allié beaucoup plus puissant dans le projet de surveillance massive d'État qu'un secteur fragmenté composé d'acteurs plus petits. Le secteur technologique états-unien est suffisamment petit pour que tous ses cadres supérieurs se retrouvent autour d'une seule table de conférence dans la Trump Tower en 2017, peu après l'inauguration de l'immeuble. La plupart de ses plus gros acteurs candidatent pour remporter le JEDI, le contrat à 10 milliards de dollars du Pentagone pour mettre en place une infrastructure de défense commune dans le cloud. Comme d'autres industries fortement concentrées, les géants de la tech font pantoufler leurs employés clés dans le service public. Ils les envoient servir au Ministère de la Défense et à la Maison Blanche, puis engagent des cadres et des officiers supérieurs de l'ex-Pentagone et de l'ex-DOD pour travailler dans leurs propres services de relations avec les gouvernements.

Ils ont même de bons arguments pour ça : après tout, quand il n'existe que quatre ou cinq grandes entreprises dans un secteur industriel, toute personne qualifiée pour contrôler la réglementation de ces entreprises a occupé un poste de direction dans au moins deux d'entre elles. De même, lorsqu'il n'y a que cinq entreprises dans un secteur, toute personne qualifiée pour occuper un poste de direction dans l'une d'entre elles travaille par définition dans l'une des autres.

Les monopoles n’engendrent pas la surveillance, mais ils l’encouragent certainement

par Cory Doctorow

 Les industries compétitives sont fragmentées dans le sens où elles sont composées d’entreprises qui s’entre-déchirent en permanence et qui rognent sur leurs marges respectives lorsqu’elles proposent des offres à leurs meilleurs clients. Ce qui leur laisse moins d’investissement afin d’obtenir des règles plus favorables. Cette situation rend aussi plus difficile la mutualisation des ressources de chaque entreprise au profit de l’industrie toute entière.

La rencontre entre la surveillance et l’apprentissage machine est censé être l’aboutissement d’une crise existentielle, un moment particulier pour l’espèce humaine où notre libre arbitre serait très proche de l’extinction pure et simple. Même si je reste sceptique quant à cette hypothèse, je pense tout de même que la technologie pose de réelles menaces existentielles à notre société (et aussi plus généralement pour notre espèce entière).
Et ces menaces viennent des monopoles.

L’une des conséquences de l’emprise de la technologie sur la réglementation est qu’elle peut rejeter la responsabilité de mauvaises décisions en matière de sécurité sur ses clients et sur la société en général. Il est tout à fait banal dans le domaine de la technologie que les entreprises dissimulent les mécanismes de leurs produits, qu’elles en rendent le fonctionnement difficile à comprendre et qu’elles menacent les chercheurs en sécurité indépendants qui auditent ces objets.

L’informatique est le seul domaine dans lequel ces pratiques existent : personne ne construit un pont ou un hôpital en gardant secret la composition de l’acier ou les équations utilisées pour calculer les contraintes de charge. C’est une pratique assez bizarre qui conduit, encore et toujours, à des défauts de sécurité grotesques à une échelle tout aussi grotesque, des pans entiers de dispositifs étant révélés comme vulnérables bien après qu’ils ont été déployées et placés dans des endroits sensibles.

Le pouvoir monopolistique qui tient à distance toute conséquence significative de ces violations, signifie que les entreprises technologiques continuent à créer des produits exécrables, mal conçus et qui finissent par être intégrés à nos vies, par posséder nos données, et être connectés à notre monde physique. Pendant des années, Boeing s’est battu contre les conséquences d’une série de mauvaises décisions technologiques qui ont fait de sa flotte de 737 un paria mondial, c’est l’un des rares cas où des décisions technologiques de piètre qualité ont été sérieusement sanctionnées par le marché.

Ces mauvaises décisions en matière de sécurité sont encore aggravées par l’utilisation de verrous de copyright pour faire appliquer des décisions commerciales à l’encontre des consommateurs.

Souvenez-vous que ces verrous sont devenus un moyen incontournable de façonner le comportement des consommateurs, qui rend techniquement impossible l'utilisation de cartouches d »encre compatibles, d'insuline, d'applications mobiles ou de dépôts de services tiers en relation avec vos biens acquis légalement.

Rappelez-vous également que ces verrous sont soutenus par une législation (telle que la section 1201 du DMCA ou l'article 6 de la directive européenne sur le droit d'auteur de 2001) qui interdit de les altérer (de les « contourner »), et que ces lois ont été utilisées pour menacer les chercheurs en sécurité qui divulguent des vulnérabilités sans la permission des fabricants.

Cela revient à un véritable *veto* des fabricants sur les alertes de sécurité et les critiques. Bien que cela soit loin de l'intention législative du DMCA (et de son équivalent dans d'autres juridictions dans le monde), le Congrès n'est pas intervenu pour clarifier la loi et ne le fera jamais, car cela irait à l'encontre des intérêts des puissantes entreprises dont le lobbying est imparable.

Les verrous de copyright sont une arme à double tranchant. D'abord parce qu'ils provoquent de mauvaises décisions en matière de sécurité qui ne pourront pas être librement étudiées ni discutées. Si les marchés sont censés être des machines à agréger l'information (et si les rayons de contrôle mental fictif du capitalisme de surveillance en font un « capitalisme voyou » parce qu'il refuse aux consommateurs le pouvoir de prendre des décisions), alors un programme qui impose légalement l'ignorance sur les risques des produits rend le monopole encore plus « voyou » que les campagnes d'influence du capitalisme de surveillance.

Et contrairement aux rayons de contrôle mental, ce silence imposé sur la sécurité est un problème brûlant et documenté qui constitue une menace existentielle pour notre civilisation et peut-être même pour notre espèce. La prolifération des dispositifs non sécurisés – en particulier ceux qui nous espionnent et surtout lorsque ces dispositifs peuvent également manipuler le monde physique, par exemple, qui tourne le volant de votre voiture ou en actionnant un disjoncteur dans une centrale électrique – est une forme de dette technique.
En conception logicielle, la « dette technique » fait référence à des décisions anciennes et bien calculées qui, avec le recul, s'avèrent être mauvaises. Par exemple, un développeur de longue date a peut-être décidé d'intégrer un protocole réseau exigé par un fournisseur, qui a depuis cessé de le prendre en charge.

Mais tout dans le produit repose toujours sur ce protocole dépassé. Donc, à chaque révision, des équipes doivent travailler autour de ce noyau obsolète, en y ajoutant des couches de compatibilité, en l'entourant de contrôles de sécurité qui tentent de renforcer ses défenses, etc. Ces mesures de fortune aggravent la dette technique, car chaque révision ultérieure doit en tenir compte, tout comme les intérêts d'un crédit revolving. Et comme dans le cas d'un prêt à risque, les intérêts augmentent plus vite que vous ne pouvez espérer les rembourser : l'équipe en charge du produit doit consacrer tellement d'énergie au maintien de ce système complexe et fragile qu'il ne lui reste plus de temps pour remanier le produit de fond en comble et « rembourser la dette » une fois pour toutes.

En général, la dette technique entraîne une faillite technologique : le produit devient si fragile et instable qu'il finit par échouer de manière catastrophique. Pensez aux systèmes bancaires et comptables désuets basés sur du COBOL qui se sont effondrés au début de la pandémie lorsque les demandes d'allocations chômage se sont multipliées. Parfois, cela met fin au produit, parfois, cela entraîne l'entreprise dans sa chute. Être pris en défaut de paiement d'une dette technique est effrayant et traumatisant, tout comme lorsque l'on perd sa maison pour cause de faillite.

Mais la dette technique créée par les verrous de copyright n'est pas individuelle, elle est systémique. Chacun dans le monde est exposé à ce surendettement, comme ce fut le cas lors de la crise financière de 2008. Lorsque cette dette arrivera à échéance – lorsque nous serons confrontés à des violations de sécurité en cascade qui menacent le transport et la logistique mondiales, l'approvisionnement alimentaire, les processus de production pharmaceutique, les communications d'urgence et autres systèmes essentiels qui accumulent de la dette technique en partie due à la présence de verrous de copyright délibérément non sécurisés et délibérément non vérifiables – elle constituera en effet un risque existentiel.

Vie privée et monopole

De nombreuses entreprises technologiques sont prisonnières d'une orthodoxie : si elles recueillent assez de données sur suffisamment de nos activités, tout devient possible – le contrôle total des esprits et des profits infinis. C'est une hypothèse invérifiable : en effet, si des données permettent à une entreprise technologique d'améliorer ne serait-ce que légèrement ses prévisions de comportements, alors elle déclarera avoir fait le premier pas vers la domination mondiale sans retour en arrière possible. Si une entreprise ne parvient pas à améliorer la collecte et l'analyse des données, alors elle déclarera que le succès est juste au coin de la rue et qu'il sera possible de l'atteindre une fois qu'elle disposera de nouvelles données.

La technologie de surveillance est loin d'être la première industrie à adopter une croyance absurde et égoïste qui nuit au reste du monde, et elle n'est pas la première industrie à profiter largement d'une telle illusion. Bien avant que les gestionnaires de fonds spéculatifs ne prétendent (à tort) pouvoir battre le S&P 500 (l'équivalent du CAC40 américain), de nombreuses autres industries « respectables » se sont révélées être de véritables charlatans. Des fabricants de suppositoires au radium (si, si, ça existe !) aux cruels sociopathes qui prétendaient pouvoir « guérir » les homosexuels, l'histoire est jonchée de titans industriels autrefois respectables qui ont mal fini.

Cela ne veut pas dire que l'on ne peut rien reprocher aux Géants de la tech et à leurs addictions idéologiques aux données. Si les avantages de la surveillance sont généralement surestimés, ses inconvénients sont, à tout le moins, *sous-estimés*.

Cette situation est très ironique. La croyance que le capitalisme de surveillance est un « capitalisme voyou » s'appuie sur l'hypothèse que les marchés ne toléreraient pas des entreprises engluées dans de fausses croyances. Une compagnie pétrolière qui se trompe souvent sur l'endroit où se trouve le pétrole finira par faire faillite en creusant tout le temps des puits déjà secs.

Mais les monopoles peuvent faire des choses graves pendant longtemps avant d'en payer le prix. Imaginez comment la concentration dans le secteur financier a permis à la crise des subprimes de s'envenimer alors que les agences de notation, les régulateurs, les investisseurs et les critiques sont tous tombés sous l'emprise d'une fausse croyance selon laquelle les mathématiques complexes pourraient construire des instruments de dette « entièrement couverts », qui ne pourraient pas faire défaut. Une petite banque qui se livrerait à ce genre de méfaits ferait tout simplement faillite au lieu d'échapper à une crise inévitable, à moins qu'elle ait pris une telle ampleur qu'elle l'aurait évitée. Mais les grandes banques ont pu continuer à attirer les investisseurs, et lorsqu'elles ont finalement réussi à s'en sortir, les gouvernements du monde entier les ont renflouées. Les pires auteurs de la crise des subprimes sont plus importants qu'ils ne l'étaient en 2008, rapportant plus de profits et payant leurs dirigeants des sommes encore plus importantes.

Les grandes entreprises technologiques sont en mesure de surveiller non seulement parce qu'elles sont technologiques, mais aussi parce qu'elles sont énormes. La raison pour laquelle tous les éditeurs de sites web intègrent le bouton « J'aime » de Facebook, est que Facebook domine les recommandations des médias sociaux sur Internet – et chacun de ces boutons « J'aime » espionne tous les utilisateurs qui visitent sur une page qui les contient (voir aussi : intégration de Google Analytics, boutons Twitter, etc.).

Si les gouvernements du monde entier ont tardé à mettre en place des sanctions significatives pour atteintes à la vie privée, c'est parce que la concentration des grandes entreprises technologiques génère d'énormes profits qui peuvent être utilisés pour faire pression contre ces sanctions.
La raison pour laquelle les ingénieurs les plus intelligents du monde veulent travailler pour les Géants de la tech est que ces derniers se taillent la part du lion des emplois dans l'industrie technologique.

Si les gens se sont horrifiés des pratiques de traitement des données de Facebook, Google et Amazon mais qu'ils continuent malgré tout d'utiliser ces services, c'est parce que tous leurs amis sont sur Facebook, que Google domine la recherche et qu'Amazon a mis tous les commerçants locaux en faillite.

Des marchés concurrentiels affaibliraient le pouvoir de lobbying des entreprises en réduisant leurs profits et en les opposant les unes aux autres à l'intérieur d'une réglementation commune. Cela donnerait aux clients d'autres endroits où aller pour obtenir leurs services en ligne. Les entreprises seraient alors suffisamment petites pour réglementer et ouvrir la voie à des sanctions significatives en cas d'infraction. Cela permettrait aux ingénieurs, dont les idées remettent en cause l'orthodoxie de la surveillance, de lever des capitaux pour concurrencer les opérateurs historiques. Cela donnerait aux éditeurs de sites web de multiples moyens d'atteindre leur public et de faire valoir leurs arguments contre l'intégration de Facebook, Google et Twitter.

En d'autres termes, si la surveillance ne provoque pas de monopoles, les monopoles encouragent certainement la surveillance…

Ronald Reagan, pionnier du monopole technologique

L'exceptionnalisme technologique est un péché, qu'il soit pratiqué par les partisans aveugles de la technologie ou par ses détracteurs. Ces deux camps sont enclins à expliquer la concentration monopolistique en invoquant certaines caractéristiques particulières de l'industrie technologique, comme les effets de réseau ou l'avantage du premier arrivé. La seule différence réelle entre ces deux groupes est que les apologistes de la technologie disent que le monopole est inévitable et que nous devrions donc laisser la technologie s'en tirer avec ses abus tandis que les régulateurs de la concurrence aux États-Unis et dans l'UE disent que le monopole est inévitable et que nous devrions donc punir la technologie pour ses abus mais sans essayer de briser les monopoles.

Pour comprendre comment la technologie est devenue aussi monopolistique, il est utile de se pencher sur l'aube de l'industrie technologique grand public : 1979, l'année où l'Apple II Plus a été lancé et est devenu le premier ordinateur domestique à succès. C'est également l'année où Ronald Reagan a fait campagne pour la présidentielle de 1980, qu'il a remportée, ce qui a entraîné un changement radical dans la manière dont les problèmes de concurrence sont traités en Amérique. Toute une cohorte d'hommes politiques de Reagan – dont Margaret Thatcher au Royaume-Uni, Brian Mulroney au Canada, Helmut Kohl en Allemagne et Augusto Pinochet au Chili – a ensuite procédé à des réformes similaires qui se sont finalement répandues dans le monde entier.

L'histoire de la lutte antitrust a commencé près d'un siècle avant tout cela avec des lois comme la loi Sherman, qui ciblait les monopoles au motif qu'ils étaient mauvais en soi – écrasant les concurrents, créant des « *déséconomies d'échelle* » (lorsqu'une entreprise est si grande que ses parties constitutives vont mal et qu'elle semble impuissante à résoudre les problèmes), et assujettissant leurs régulateurs à un point tel qu'ils ne peuvent s'en tirer sans une foule de difficultés.

Puis vint un affabulateur du nom de Robert Bork, un ancien avocat général que Reagan avait nommé à la puissante Cour d'appel américaine pour le district de Columbia et qui avait inventé de toutes pièces une histoire législative alternative de la loi Sherman et des lois suivantes. Bork a soutenu que ces lois n'ont jamais visé les monopoles (malgré de nombreuses preuves du contraire, y compris les discours retranscrits des auteurs des de ces lois) mais qu'elles visaient plutôt à prévenir les « préjudices aux consommateurs » – sous la forme de prix plus élevés.
Bork était un hurluberlu, certes, mais les riches aimaient vraiment ses idées. Les monopoles sont un excellent moyen de rendre les riches plus riches en leur permettant de recevoir des « rentes de monopole » (c'est-à-dire des profits plus importants) et d'assujettir les régulateurs, ce qui conduit à un cadre réglementaire plus faible et plus favorable, avec moins de protections pour les clients, les fournisseurs, l'environnement et les travailleurs.

Les théories de Bork étaient particulièrement satisfaisantes pour les mêmes personnalités influentes qui soutenaient Reagan. Le ministère de la Justice et d'autres agences gouvernementales de l'administration Reagan ont commencé à intégrer la doctrine antitrust de Bork dans leurs décisions d'application (Reagan a même proposé à Bork de siéger à la Cour suprême, mais Bork a été tellement mauvais à l'audience de confirmation du Sénat que, 40 ans plus tard, les experts de Washington utilisent le terme « borked » pour qualifier toute performance politique catastrophique).

Peu à peu, les théories de Bork se sont répandues, et leurs partisans ont commencé à infiltrer l'enseignement du droit, allant même jusqu'à organiser des séjours tous frais payés, où des membres de la magistrature étaient invités à de copieux repas, à participer à des activités de plein

air et à assister à des séminaires où ils étaient endoctrinés contre la théorie antitrust et les dommages qu'elle cause aux consommateurs. Plus les théories de Bork s'imposaient, plus les monopolistes gagnaient de l'argent – et plus ils disposaient d'un capital excédentaire pour faire pression en faveur de campagnes d'influence antitrust à la Bork.

L'histoire des théories antitrust de Bork est un très bon exemple du type de retournements d'opinion publique obtenus secrètement et contre lesquels Zuboff nous met en garde, où les idées marginales deviennent peu à peu l'orthodoxie dominante. Mais Bork n'a pas changé le monde du jour au lendemain. Il a été très endurant, pendant plus d'une génération, et il a bénéficié d'un climat favorable parce que les forces qui ont soutenu les théories antitrust oligarchiques ont également soutenu de nombreux autres changements oligarchiques dans l'opinion publique. Par exemple, l'idée que la fiscalité est un vol, que la richesse est un signe de vertu, etc. – toutes ces théories se sont imbriquées pour former une idéologie cohérente qui a élevé l'inégalité au rang de vertu.

Aujourd'hui, beaucoup craignent que l'apprentissage machine permette au capitalisme de surveillance de vendre « Bork-as-a-Service », à la vitesse de l'Internet, afin qu'on puisse demander à une société d'apprentissage machine de provoquer des retournements *rapides* de l'opinion publique sans avoir besoin de capitaux pour soutenir un projet multiforme et multigénérationnel mené aux niveaux local, étatique, national et mondial, dans les domaines des affaires, du droit et de la philosophie. Je ne crois pas qu'un tel projet soit réalisable, bien que je sois d'accord avec le fait que c'est essentiellement ce que les plateformes prétendent vendre. Elles mentent tout simplement à ce sujet. Les (entreprises de la) Big Tech mentent tout le temps, *y compris* dans leur documentation commerciale.

L'idée que la technologie forme des « monopoles naturels » (des monopoles qui sont le résultat inévitable des réalités d'une industrie, comme les monopoles qui reviennent à la première entreprise à exploiter des lignes téléphoniques longue distance ou des lignes ferroviaires) est démentie par la propre histoire de la technologie : en l'absence de tactiques anticoncurrentielles, Google a réussi à détrôner AltaVista et Yahoo, et Facebook a réussi à se débarrasser de Myspace. La collecte de montagnes de données présente certains avantages, mais ces montagnes de données ont également des inconvénients : responsabilité (en raison de fuites), rendements décroissants (en raison d'anciennes données) et inertie institutionnelle (les grandes entreprises, comme la science, progressent en liquidant les autres à mesure).

En effet, la naissance du Web a vu l'extinction en masse des technologies propriétaires géantes et très rentables qui disposaient de capitaux, d'effets de réseau, de murs et de douves autour de leurs entreprises. Le Web a montré que lorsqu'une nouvelle industrie est construite autour d'un protocole, plutôt que d'un produit, la puissance combinée de tous ceux qui utilisent le protocole pour atteindre leurs clients, utilisateurs ou communautés, dépasse même les produits les plus massivement diffusés. CompuServe, AOL, MSN et une foule d'autres jardins clos propriétaires ont appris cette leçon à la dure : chacun croyait pouvoir rester séparé du Web, offrant une « curation » et une garantie de cohérence et de qualité au lieu du chaos d'un système ouvert. Chacun a eu tort et a fini par être absorbé dans le Web public.

Oui, la technologie est fortement monopolisée et elle est maintenant étroitement associée à la concentration de l'industrie, mais c'est davantage lié à une question de temps qu'à des tendances intrinsèquement monopolistiques. La technologie est née au moment où l'application de la législation antitrust était démantelée, et la technologie est tombée exactement dans les mêmes

travers contre lesquels l'antitrust était censé se prémunir. En première approximation, il est raisonnable de supposer que les monopoles de Tech sont le résultat d'un manque d'action anti-monopole et non des caractéristiques uniques tant vantées de Tech, telles que les effets de réseau, l'avantage du premier arrivé, etc.

À l'appui de cette théorie, je propose de considérer la concentration que tous les *autres* secteurs ont connue au cours de la même période. De la lutte professionnelle aux biens de consommation emballés, en passant par le crédit-bail immobilier commercial, les banques, le fret maritime, le pétrole, les labels discographiques, la presse écrite et les parcs d'attractions, *tous* les secteurs ont connu un mouvement de concentration massif. Il n'y a pas d'effets de réseau évidents ni d'avantage de premier arrivé dans ces secteurs. Cependant, dans tous les cas, ils ont atteint leur statut de concentration grâce à des tactiques qui étaient interdites avant le triomphe de Bork : fusion avec des concurrents majeurs, rachat de nouveaux venus innovants sur le marché, intégration horizontale et verticale, et une série de tactiques anticoncurrentielles qui étaient autrefois illégales mais ne le sont plus.

Encore une fois : lorsque vous modifiez les lois destinées à empêcher les monopoles, puis que les monopoles se forment exactement comme la loi était censée les empêcher, il est raisonnable de supposer que ces faits sont liés. La concentration de Tech peut être facilement expliquée sans avoir recours aux théories radicales des effets de réseau – mais seulement si vous êtes prêt à accuser les marchés non réglementés de tendre vers le monopole. Tout comme un fumeur de longue date peut vous fournir une foule de raisons selon lesquelles ce n'est pas son tabagisme qui a provoqué son cancer (« Ce sont les toxines environnementales »), les vrais partisans des marchés non réglementés ont toute une série d'explications peu convaincantes pour prétendre que le monopole de la technologie ne modifie pas le capitalisme.

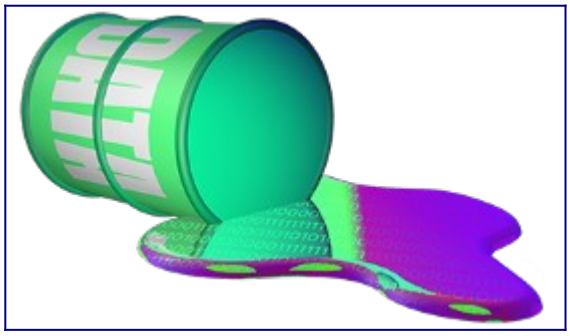
Conduire avec les essuie-glaces

Cela fait quarante ans que le projet de Bork pour réhabiliter les monopoles s'est réalisé, soit une génération et demie, c'est à dire suffisamment de temps pour qu'une idée commune puisse devenir farfelue ou l'inverse. Avant les années 40, les Américains aisés habillaient leurs petits garçons en rose alors que les filles portaient du bleu (une couleur « fragile et délicate »). Bien que les couleurs genrées soient totalement arbitraires, beaucoup découvriront cette information avec étonnement et trouveront difficile d'imaginer un temps où le rose suggérait la virilité.

Après quarante ans à ignorer scrupuleusement les mesures antitrust et leur mise en application, il n'est pas surprenant que nous ayons presque tous oublié que les lois antitrust existent, que la croissance à travers les fusions et les acquisitions était largement interdite par la loi, et que les stratégies d'isolation d'un marché, comme par l'intégration verticale, pouvait conduire une entreprise au tribunal.

L'antitrust, c'est le volant de cette voiture qu'est la société de marché, l'outil principal qui permet de contrôler la trajectoire de ces prétendants au titre de maîtres de l'univers. Mais Bork et ses amis nous ont arraché ce volant des mains il y a quarante ans. Puisque la voiture continue d'avancer, nous appuyons aussi fort que possible sur toutes les autres commandes de la voiture, de même que nous ouvrons et fermons les portes, montons et descendons les vitres dans l'espoir qu'une de ces commandes puisse nous permettre de choisir notre direction et de reprendre le contrôle avant de foncer dans le décor.

Ça ressemble à un scénario de science-fiction des années 60 qui deviendrait réalité : voyageant à travers les étoiles, des humains sont coincés dans un « vaisseau générationnel » autrefois piloté par leurs ancêtres, et maintenant, après une grande catastrophe, l'équipage a complètement oublié qu'il est dans un vaisseau et ne se souvient pas où est la salle de contrôle. À la dérive, le vaisseau court à sa perte, et, à moins que nous puissions reprendre le contrôle et corriger le cap en urgence, nous allons tout fonçons droit vers une mort ardente dans le cœur d'un soleil.



La surveillance a toujours son importance

Rien de tout cela ne doit minimiser les problèmes liés à la surveillance. La surveillance est importante, et les Géants de la tech qui l'utilisent font peser un véritable risque existentiel sur notre espèce, mais ce n'est pas parce que la surveillance et l'apprentissage machine nous subtilisent notre libre arbitre.

La surveillance est devenue bien plus efficace avec les Géants de la tech. En 1989, la Stasi — la police secrète est-allemande — avait l'intégralité du pays sous surveillance, un projet titanesque qui recrutait une personne sur 60 en tant qu'informateur ou comme agent de renseignement.

Aujourd'hui, nous savons que la NSA espionne une partie significative de la population mondiale, et le ratio entre agents de renseignement et population surveillée est plutôt de l'ordre de 1 pour 10 000 (ce chiffre est probablement sous-estimé puisqu'il suppose que tous les Américains détenant un niveau de confidentialité top secret travaillent pour la NSA — en fait on ne sait pas combien de personnes sont autorisées à espionner pour le compte de la NSA, mais ce n'est certainement pas toutes les personnes classées top secret).

Comment ce ratio de citoyens surveillés a-t-il pu exploser de 1/60 à 1/10 000 en moins de trente ans ? C'est bien grâce aux Géants de la tech. Nos appareils et leurs services collectent plus de données que ce que la NSA collecte pour ses propres projets de surveillance. Nous achetons ces appareils, nous nous connectons à leurs services, puis nous accomplissons laborieusement les tâches nécessaires pour insérer des données sur nous, notre vie, nos opinions et nos préférences. Cette surveillance de masse s'est révélée complètement inutile dans la lutte contre le terrorisme : la NSA évoque un seul et unique cas, dans lequel elle a utilisé un programme de collection de données pour faire échouer une tentative de transfert de fond de quelques milliers de dollars d'un citoyen américain vers un groupe terroriste basé à l'étranger. Les raisons de cette inefficacité déconcertante sont les mêmes que pour l'échec du ciblage publicitaire par les entreprises de surveillance commerciale : les personnes qui commettent des actes terroristes, tout comme celles qui achètent un frigo, se font très rares. Si vous voulez détecter un phénomène dont la probabilité de base est d'un sur un million avec un outil dont la précision n'est que de 99 %, chaque résultat juste apparaîtra au prix de 9 999 faux positifs.

Essayons de le formuler autrement : si une personne sur un million est terroriste, alors nous aurons seulement un terroriste dans un échantillon d'un million de personnes. Si votre test de détecteur à terroristes est précis à 99 %, il identifiera 10 000 terroristes dans votre échantillon d'un million de personnes (1 % d'un million = 10 000). Pour un résultat juste, vous vous retrouvez avec 9 999 faux positifs.

En réalité, la précision algorithmique de la détection de terroriste est bien inférieure à 99 %, tout comme pour les publicités de frigo. La différence, c'est qu'être accusé à tort d'être un potentiel acheteur de frigo est une nuisance somme toute assez faible, alors qu'être accusé à tort de planifier un attentat terroriste peut détruire votre vie et celle de toutes les personnes que vous aimez.

L'État ne peut surveiller massivement que parce que le capitalisme de surveillance et son très faible rendement existent, ce qui demande un flux constant de données personnelles pour pouvoir rester viable. L'échec majeur du capitalisme de surveillance vient des publicités mal ciblées, tandis que celui de la surveillance étatique vient des violations éhontées des Droits de l'humain, qui ont tendance à dériver vers du totalitarisme.

La surveillance de l'État n'est pas un simple parasite des Géants de la tech, qui pomperait les données sans rien accorder en retour. En réalité, ils sont plutôt en symbiose : les Géants pompent nos données pour le compte des agences de renseignement, et ces dernières s'assurent que le pouvoir politique ne restreint pas trop sévèrement les activités des Géants de la tech jusqu'à devenir inutile aux besoins du renseignement. Il n'y a aucune distinction claire entre la surveillance d'État et le capitalisme de surveillance, ils sont tous deux co-dépendants.

Pour comprendre comment tout cela fonctionne aujourd'hui, pas besoin de regarder plus loin que l'outil de surveillance d'Amazon, la sonnette Ring et son application associée Neighbors. Ring — un produit acheté et non développé par Amazon — est une sonnette munie d'une caméra qui diffuse les images de l'entrée devant votre porte sur votre téléphone. L'application Neighbors vous permet de mettre en place un réseau de surveillance à l'échelle de votre quartier avec les autres détenteurs de sonnette Ring autour de chez vous, avec lesquels vous pouvez partager des vidéos de « personnes suspectes ». Si vous pensez que ce système est le meilleur moyen pour permettre aux commères racistes de suspecter toute personne de couleur qui se balade dans le quartier, vous avez raison. Ring est devenu de facto, le bras officieux de la police sans s'embêter avec ces satanées lois et règlements.

À l'été 2019, une série de demande de documents publics a révélé qu'Amazon a passé des accords confidentiels avec plus de 400 services de police locaux au travers desquelles ces agences font la promotion de Ring and Neighbors en échange de l'accès à des vidéos filmées par les visiophones Ring. En théorie, la police devrait réclamer ces vidéos par l'intermédiaire d'Amazon (et des documents internes ont révélé qu'Amazon consacre des ressources non-négligeables pour former les policiers à formuler des histoires convaincantes dans ce but), mais dans la pratique, quand un client Ring refuse de transmettre ses vidéos à la police, Amazon n'exige de la police qu'une simple requête formelle à adresser à l'entreprise, ce qu'elle lui remet alors.

Ring et les forces de police ont trouvé de nombreuses façons de mêler leurs activités . Ring passe des accords secrets pour avoir un accès en temps réel aux appels d'urgence (le 911) pour ensuite diffuser à ses utilisateurs les procès-verbaux de certaines infractions, qui servent aussi à convaincre n'importe quelle personne qui envisage d'installer un portier de surveillance mais qui ne sait pas vraiment si son quartier est suffisamment dangereux pour que ça en vaille le coup.

Plus les flics vantent les mérites du réseau de surveillance capitaliste Ring, plus l'État dispose de capacités de surveillance. Les flics qui s'appuient sur des entités privées pour faire respecter la loi s'opposent ensuite à toute régulation du déploiement de cette technologie, tandis que les entreprises leur rendent la pareille en faisant pression contre les règles qui réclament une surveillance publique de la technologie de surveillance policière. Plus les flics s'appuient sur *Ring and Neighbors*, plus il sera difficile d'adopter des lois pour les freiner. Moins il y aura de lois contre eux, plus les flics se reposeront sur ces technologies.

Dignité et sanctuaire

Quand bien même nous exercerions un contrôle démocratique sur nos États et les forcerions à arrêter de piller les silos de données comportementales du capitalisme de surveillance, ce dernier continuera à nous maltraiter. Nous vivons une époque parfaitement éclairée par Zuboff. Son chapitre sur le sanctuaire – ce sentiment de ne pas être observé – est une magnifique ode à l'introspection, au calme, à la pleine conscience et à la tranquillité.

Quand nous sommes observé·e·s, quelque chose change. N'importe quel parent sait ce que cela signifie. Vous pouvez lever la tête de votre bouquin (ou plus vraisemblablement de votre téléphone) et observer votre enfant dans un état profond de réalisation de soi et d'épanouissement, un instant où il est en train d'apprendre quelque chose à la limite de ses capacités, qui demande une concentration intense. Pendant un court laps de temps, vous êtes sidéré·e, et vous observez ce moment rare et beau de concentration qui se déroule devant vos yeux, et puis votre enfant lève la tête, vous voit le regarder, et ce moment s'évanouit. Pour grandir, vous devez être vous-même et donner à voir votre moi authentique, c'est à ce moment que vous devenez vulnérable, tel un bernard-l'hermite entre deux coquilles.

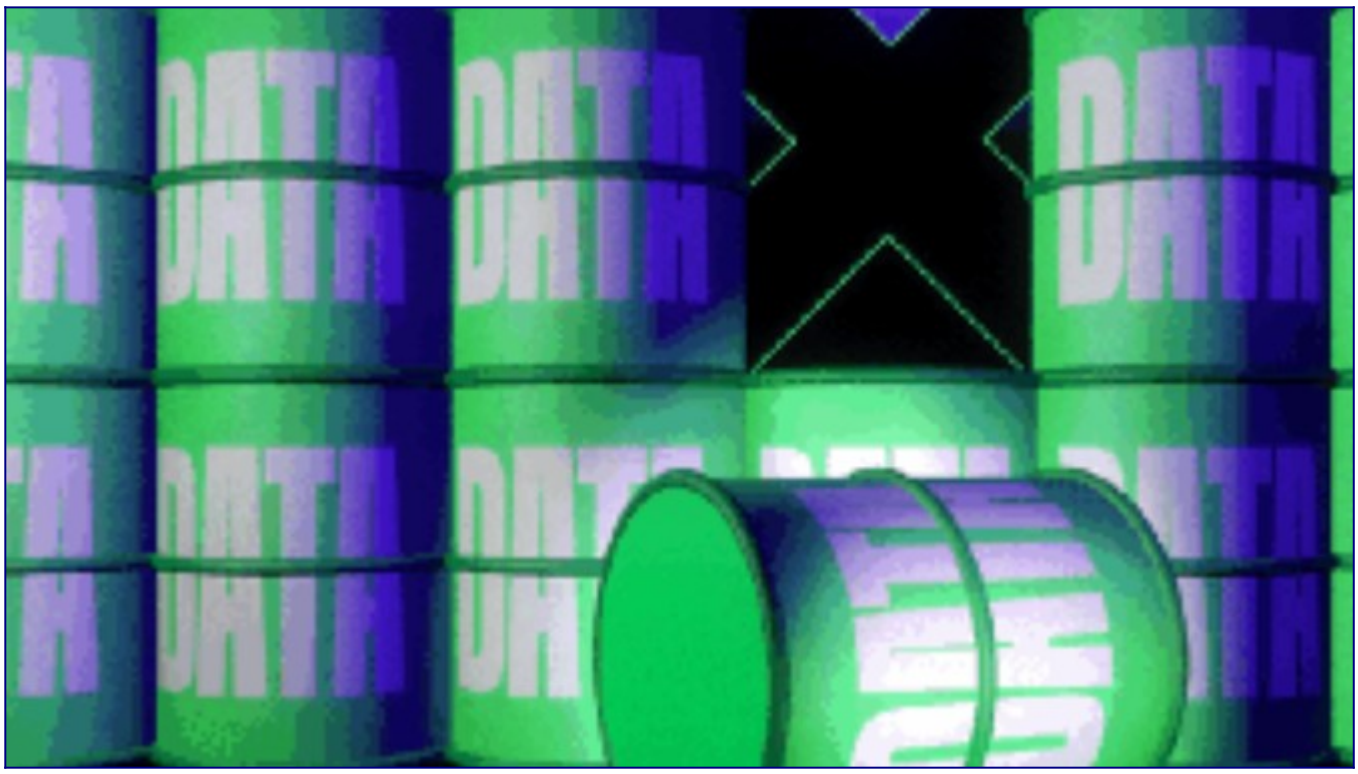
Cette partie de vous, tendre et fragile, que vous exposez au monde dans ces moments-là, est bien trop délicate pour être révélée à autrui, pas même à une personne à laquelle vous faites autant confiance qu'un enfant à ses parents.

À l'ère numérique, notre moi authentique est inextricablement mêlé à de notre vie en ligne. Votre historique de recherche est un enregistrement en continu des questions que vous vous posez. Votre historique de géolocalisation est un registre des endroits que vous cherchiez et des expériences que vous avez vécues en ces lieux. Votre réseau social révèle les différentes facettes de votre personnalité ainsi que les gens avec qui vous êtes en contact.

Être observé pendant ces activités, c'est perdre le sanctuaire de votre moi authentique. Mais il y a une autre manière pour le capitalisme de surveillance de nous dérober notre capacité d'être véritablement nous-même : nous rendre anxieux. Ce capitalisme de surveillance n'est pas vraiment un rayon de contrôle mental, pas besoin de ça pour rendre quelqu'un anxieux. Après tout, l'anxiété est le synonyme d'agitation, et pour qu'une personne se sente agitée, il n'y a pas vraiment besoin de la secouer. Il suffit d'aiguillonner et de piquer et de notifier et de bourdonner autour et de bombarder de manière intermittente et juste assez aléatoire pour que notre système limbique ne puisse jamais vraiment s'y habituer.

Nos appareils et nos services sont polyvalents dans le sens où ils peuvent connecter n'importe quoi ou n'importe qui à n'importe quoi ou à n'importe qui d'autre, et peuvent aussi exécuter n'importe quel programme. Cela signifie que ces rectangles de distractions dans nos poches détiennent nos plus précieux moments avec nos proches, tout comme les communications les plus urgentes et les plus sensibles (de « je suis en retard, peux-tu aller chercher les gamins ? » jusqu'à « mauvaise nouvelle du docteur, il faut qu'on parle TOUT DE SUITE »), mais aussi les pubs pour les frigos et les messages de recrutement nazis.

À toute heure du jour ou de la nuit, nos poches sonnent, font voler en éclat notre concentration, détruisent le fragile maillage de nos réflexions quand nous avons besoin de penser des situations difficiles. Si vous enfermiez quelqu'un dans une cellule et que vous l'agitiez de la sorte, on appellerait ça de la torture par privation de sommeil, et ce serait considéré comme un crime de guerre par la Convention de Genève.



Affliger les affligés

Les effets de la surveillance sur notre capacité à être nous-mêmes ne sont pas les mêmes pour tout le monde. Certain·e·s d'entre nous ont la chance de vivre à une époque et dans un lieu où tous les faits les plus importants de leur vie sont socialement acceptés et peuvent être exposés au grand jour sans en craindre les conséquences sociales.

Mais pour beaucoup d'entre nous, ce n'est pas le cas. Rappelez-vous que, d'aussi loin qu'on s'en souvienne, de nombreuses façons d'être, considérées aujourd'hui comme socialement acceptables, ont donné lieu à de terribles condamnations sociales, voire à des peines d'emprisonnement. Si vous avez 65 ans, vous avez connu une époque où les personnes vivant dans des « sociétés libres » pouvaient être emprisonnées ou punies pour s'être livrées à des pratiques homosexuelles, pour être tombées amoureuses d'une personne dont la peau était d'une couleur différente de la leur, ou pour avoir fumé de l'herbe.

Aujourd'hui, non seulement ces pratiques sont dépénalisées dans une grande partie du monde, mais en plus, elles sont considérées comme normales, et les anciennes prohibitions sont alors vues comme des vestiges d'un passé honteux et regrettable.

Comment sommes-nous passés de la prohibition à la normalisation ? Par une activité privée et personnelle : les personnes dont l'homosexualité était secrète ou qui fumaient de l'herbe en secret, ou qui aimaient quelqu'un d'une couleur de peau différente de la leur en secret, étaient susceptibles de représailles si elles dévoilaient leur moi authentique. On les empêchait de défendre leur droit à exister dans le monde et à être en accord avec elles-mêmes. Mais grâce à la sphère privée, ces personnes pouvaient former des liens forts avec leurs amis et leurs proches qui ne partageaient pas leurs manières de vivre mal vues par la société. Elles avaient des conversations privées dans lesquelles elles se dévoilaient, elles révélaient leur moi authentique à leurs proches, puis les ralliaient à leur cause au fil des conversations.

Le droit de choisir le moment et la manière d'aborder ces conversations a joué un rôle fondamental dans le renversement des normes. C'est une chose de faire son *coming out* à son père au cours d'une sortie de pêche à l'écart du monde, c'en est une autre de tout déballer pendant le repas de Noël, en présence de son oncle raciste sur Facebook prêt à faire une scène.

Sans sphère privée, il est possible qu'aucun de ces changements n'aurait eu lieu et que les personnes qui en ont bénéficié auraient subi une condamnation sociale pour avoir fait leur *coming out* face à un monde hostile ou alors elles n'auraient jamais pu révéler leur moi authentique aux personnes qu'elles aiment.

Et donc, à moins que vous ne pensiez que notre société ait atteint la perfection sociale – et que vos petits-enfants vous demanderont dans 50 ans de leur raconter comment, en 2020, toutes les injustices ont été réparées et qu'il n'y avait plus eu de changement à apporter –, vous devez vous attendre à ce qu'en ce moment même figurent parmi vos proches des personnes, dont le bonheur est indissociable du vôtre, et dont le cœur abrite un secret qui les empêche toujours de dévoiler leur moi authentique en votre présence. Ces personnes souffrent et emporteront leur chagrin secret dans leur tombe, et la source de ce chagrin, ce sera les relations faussées qu'elles entretenaient avec vous.

Une sphère privée est nécessaire au progrès humain.

Toute donnée collectée et conservée finit par fuiter

L'absence de vie privée peut empêcher les personnes vulnérables d'exprimer leur moi authentique et limiter nos actions en nous privant d'un sanctuaire. Mais il existe un autre risque, encouru par tous et pas seulement par les personnes détenant un secret : la criminalité.

Les informations d'identification personnelle présentent un intérêt très limité pour contrôler l'esprit des gens, mais le vol d'identité – terme fourre-tout pour désigner toute une série de pratiques délictueuses graves, susceptibles de détruire vos finances, de compromettre votre intégrité personnelle, de ruiner votre réputation, voire de vous exposer à un danger physique – est en pleine expansion.

Les attaquants ne se limitent pas à utiliser des données issues de l'intrusion dans une seule et même source.

De nombreux services ont subi des violations qui ont révélé des noms, des adresses, des numéros de téléphone, des mots de passe, des préférences sexuelles, des résultats scolaires, des réalisations professionnelles, des démêlés avec la justice, des informations familiales, des données génétiques, des empreintes digitales et autres données biométriques, des habitudes de lecture, des historiques de recherche, des goûts littéraires, des pseudonymes et autres données sensibles. Les attaquants peuvent fusionner les données provenant de ces violations pour constituer des dossiers très détaillés sur des sujets choisis au hasard, puis utiliser certaines parties des données pour commettre divers délits.

Les attaquants peuvent, par exemple, utiliser des combinaisons de noms d'utilisateur et de mots de passe dérobés pour détourner des flottes entières de véhicules commerciaux équipés de systèmes de repérage GPS et d'immobilisation antivol, ou pour détourner des *babyphones* afin de terroriser les tout-petits en diffusant du contenu audio pornographique. Les attaquants utilisent les données divulguées pour tromper les opérateurs téléphoniques afin qu'ils leur communiquent votre numéro

de téléphone, puis ils interceptent des codes d'authentification à deux facteurs par SMS pour pirater votre courrier électronique, votre compte bancaire ou vos portefeuilles de crypto-monnaie.

Les attaquants rivalisent de créativité pour trouver des moyens de transformer les données divulguées en armes. Ces données sont généralement utilisées pour pénétrer dans les entreprises afin d'accéder à davantage de données.

Tout comme les espions, les fraudeurs en ligne dépendent entièrement des entreprises qui collectent et conservent nos données à outrance. Les agences d'espionnage paient voire intimident parfois des entreprises pour avoir accès à leurs données, elles peuvent aussi se comporter comme des délinquants et dérober du contenu de bases de données d'entreprises.

La collecte excessive de données entraîne de graves conséquences sociales, depuis la destruction de notre moi authentique jusqu'au recul du progrès social, de la surveillance de l'État à une épidémie de cybercriminalité. La surveillance commerciale est également une aubaine pour les personnes qui organisent des campagnes d'influence, mais c'est le cadet de nos soucis.

L'exceptionnalisme technologique critique reste un exceptionnalisme technologique

Les géants de la tech ont longtemps pratiqué un exceptionnalisme technologique : cette idée selon laquelle ils ne devraient pas être soumis aux lois et aux normes du commun des mortels. Des devises comme celle de Facebook « Move fast and break things » [avancer vite et casser des choses, NdT] ont provoqué un mépris compréhensible envers ces entreprises à la rhétorique égoïste.

L'exceptionnalisme technologique nous a tous mis dans le pétrin. Il est donc assez ironique et affligeant de voir les critiques des géants de la tech commettre le même péché.

Les géants de la tech ne forment pas un « capitalisme voyou » qui ne peut être guéri par les remèdes traditionnels anti-monopole que sont le démantèlement des trusts (forcer les entreprises à se défaire des concurrents qu'elles ont acquis) et l'interdiction des fusions monopolistiques et autres tactiques anticoncurrentielles. Les géants de la tech n'ont pas le pouvoir d'utiliser l'apprentissage machine pour influencer notre comportement de manière si approfondie que les marchés perdent la capacité de punir les mauvais acteurs et de récompenser les concurrents vertueux. Les géants de la tech n'ont pas de rayon de contrôle mental qui réécrit les règles, si c'était le cas, nous devrions nous débarrasser de notre vieille boîte à outils.

Cela fait des siècles que des gens prétendent avoir mis au point ce rayon de contrôle mental et cela s'est toujours avéré être une arnaque, même si parfois les escrocs se sont également arnaqués entre eux.

Depuis des générations, le secteur de la publicité améliore constamment sa capacité à vendre des services publicitaires aux entreprises, tout en ne réalisant que des gains marginaux sur la vente des produits de ces entreprises. La complainte de John Wanamaker selon laquelle « La moitié de l'argent que je dépense en publicité est gaspillée, mais je ne sais pas quelle moitié » témoigne du triomphe des directeurs de la publicité qui ont réussi à convaincre Wanamaker que la moitié seulement de ce qu'il dépense était gaspillée.

L'industrie technologique a fait d'énormes progrès dans la capacité à convaincre les entreprises qu'elles sont douées pour la publicité, alors que leurs améliorations réelles en matière de publicité, par opposition au ciblage, ont été plutôt modestes. La vogue de l'apprentissage machine – et

l'invocation mystique de l'« intelligence artificielle » comme synonyme de techniques d'inférence statistique directe – a considérablement renforcé l'efficacité du discours commercial des géants de la tech, car les spécialistes du marketing ont exploité le manque de connaissance technique des clients potentiels pour s'en tirer avec énormément de promesses et peu de résultats.

Il est tentant de penser que si les entreprises sont prêtes à déverser des milliards dans un projet, celui-ci doit être bon. Pourtant, il arrive souvent que cette règle empirique nous fasse faire fausse route. Par exemple, on n'a pratiquement jamais entendu dire que les fonds d'investissement surpassent les simples fonds indiciels, et les investisseurs qui confient leur argent à des gestionnaires de fonds experts s'en sortent généralement moins bien que ceux qui confient leur épargne à des fonds indiciels. Mais les fonds gérés représentent toujours la majorité de l'argent investi sur les marchés, et ils sont soutenus par certains des investisseurs les plus riches et les plus pointus du monde. Leur vote de confiance dans un secteur aussi peu performant est une belle leçon sur le rôle de la chance dans l'accumulation de richesses, et non un signe que les fonds de placement sont une bonne affaire.

Les affirmations du système de contrôle mental des géants de la tech laissent à penser que cette pratique est une arnaque. Par exemple, avec le recours aux traits de personnalité des « cinq grands » comme principal moyen d'influencer les gens, même si cette théorie des cinq grands n'est étayée par aucune étude à grande échelle évaluée par des pairs, et qu'elle est surtout l'apanage des baratineurs en marketing et des psychologues pop.

Le matériel promotionnel des géants de la tech prétend aussi que leurs algorithmes peuvent effectuer avec précision une « analyse des sentiments » ou détecter l'humeur des gens à partir de leurs « micro-expressions », mais il s'agit là d'affirmations marketing et non scientifiques. Ces méthodes n'ont pas été testées par des scientifiques indépendants, et lorsqu'elles l'ont été, elles se sont révélées très insuffisantes. Les micro-expressions sont particulièrement suspectes car il a été démontré que les entreprises spécialisées dans la formation de personnes pour les détecter sont moins performantes que si on laissait faire le hasard.

Les géants de la tech ont été si efficaces pour commercialiser leurs soi-disant super-pouvoirs qu'il est facile de croire qu'elles peuvent commercialiser tout le reste avec la même habileté, mais c'est une erreur de croire au baratin du marketing. Aucune déclaration d'une entreprise sur la qualité de ses produits n'est évidemment impartiale. Le fait que nous nous méfions de tout ce que disent les géants de la tech sur le traitement des données, le respect des lois sur la protection de la vie privée, etc. est tout à fait légitime, car pourquoi goberions-nous la littérature marketing comme s'il s'agissait d'une vérité d'évangile ? Les géants de la tech mentent sur à peu près tout, y compris sur le fonctionnement de leurs systèmes de persuasion alimentés par l'apprentissage automatique.

Ce scepticisme devrait imprégner toutes nos évaluations des géants de la tech et de leurs capacités supposées, y compris à la lecture attentive de leurs brevets. Zuboff confère à ces brevets une importance énorme, en soulignant que Google a revendiqué de nouvelles capacités de persuasion dans ses dépôts de brevets. Ces affirmations sont doublement suspectes : d'abord parce qu'elles sont très intéressées, et ensuite parce que le brevet lui-même est notoirement une invitation à l'exagération.

Les demandes de brevet prennent la forme d'une série de revendications et vont des plus étendues aux plus étroites. Un brevet typique commence par affirmer que ses auteurs ont inventé une méthode ou un système permettant de faire absolument tout ce qu'il est possible d'imaginer avec un

outil ou un dispositif. Ensuite, il réduit cette revendication par étapes successives jusqu'à ce que nous arrivions à l'« invention » réelle qui est le véritable objet du brevet. L'espoir est que la personne qui passe en revue les demandes de brevets – qui est presque certainement surchargée de travail et sous-informée – ne verra pas que certaines (ou toutes) ces revendications sont ridicules, ou du moins suspectes, et qu'elle accordera des prétentions plus larges du brevet. Les brevets portant sur des choses non brevetables sont tout de même très utiles, car ils peuvent être utilisés contre des concurrents qui pourraient accorder une licence sur ce brevet ou se tenir à l'écart de ses revendications, plutôt que de subir le long et coûteux processus de contestation.

De plus, les brevets logiciels sont couramment accordés même si le déposant n'a aucune preuve qu'il peut faire ce que le brevet prétend. C'est-à-dire que vous pouvez breveter une « invention » que vous n'avez pas réellement faite et que vous ne savez pas comment faire.

Avec ces considérations en tête, il devient évident que le fait qu'un Géant de la tech ait breveté ce qu'il qualifie de rayon efficace de contrôle mental ne permet nullement de savoir si cette entreprise peut effectivement contrôler nos esprits.

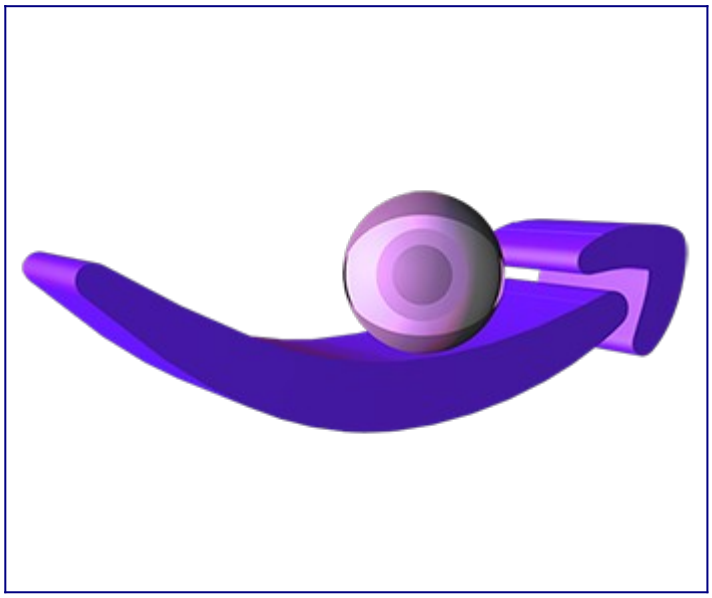
Les géants de la tech collectent nos données pour de nombreuses raisons, y compris la diminution du rendement des stocks de données existants. Mais de nombreuses entreprises technologiques collectent également des données en raison d'une croyance exceptionnaliste erronée aux effets de réseau des données. Les effets de réseau se produisent lorsque chaque nouvel utilisateur d'un système augmente sa valeur. L'exemple classique est celui des télécopieurs [des fax NdT] : un seul télécopieur ne sert à rien, deux télécopieurs sont d'une utilité limitée, mais chaque nouveau télécopieur mis en service après le premier double le nombre de liaisons possibles de télécopie à télécopie.

Les données exploitées pour les systèmes prédictifs ne produisent pas nécessairement ces bénéfices. Pensez à Netflix : la valeur prédictive des données extraites d'un million d'utilisateurs anglophones de Netflix n'est guère est à peine améliorée par l'ajout des données de visualisation d'un utilisateur supplémentaire. La plupart des données que Netflix acquiert après ce premier échantillon minimum viable font double emploi avec des données existantes et ne produisent que des gains minimes. En attendant, le recyclage des modèles avec de nouvelles données devient plus cher à mesure que le nombre de points de données augmente, et les tâches manuelles comme l'étiquetage et la validation des données ne deviennent pas moins chères lorsqu'on augmente l'ordre de grandeur.

Les entreprises font tout le temps la course aux modes au détriment de leurs propres profits, surtout lorsque ces entreprises et leurs investisseurs ne sont pas motivés par la perspective de devenir rentables mais plutôt par celle d'être rachetés par un Géant de la tech ou d'être introduits en Bourse. Pour ces entreprises, cocher des cases à la mode comme « collecte autant de données que possible » pourrait permettre d'obtenir un meilleur retour sur investissement que « collecte une quantité de données adaptée à l'entreprise ».

C'est un autre dommage causé par l'exceptionnalisme technologique : la croyance selon laquelle davantage de données produit toujours plus de profits sous la forme de plus d'informations qui peuvent être traduites en de meilleurs rayons de contrôle mental. Cela pousse les entreprises à collecter et à conserver des données de manière excessive, au-delà de toute rationalité. Et comme les entreprises se comportent de manière irrationnelle, bon nombre d'entre elles vont faire faillite et devenir des navires fantômes dont les cales sont remplies de données qui peuvent nuire aux gens de multiples façons, mais dont personne n'est plus responsable. Même si les entreprises ne font pas

faillite, les données qu'elles collectent sont maintenues en-deça de la sécurité minimale viable – juste assez de sécurité pour maintenir la viabilité de l'entreprise en attendant d'être rachetées par un Géant de la tech, un montant calculé pour ne pas dépenser un centime de trop pour la protection des données.



Comment les monopoles, et non le contrôle de la pensée, conduisent à la surveillance capitaliste : le cas de Snapchat

Pendant la première décennie de son existence, Facebook est entré en concurrence avec les réseaux sociaux de l'époque (Myspace, Orkut, etc) en se présentant comme l'alternative respectant de la vie privée. De fait, Facebook a justifié son jardin clos, qui permet aux utilisateurs d'y amener des données du Web, mais empêche les services tels que Google Search d'indexer et de mémoriser les pages Facebook, en tant que mesure de respect de la vie privée qui protège les utilisateurs des heureux gagnants de la bataille des réseaux sociaux comme Myspace.

En dépit des fréquentes promesses disant qu'il ne collecterait ou n'analyserait jamais les données de ses utilisateurs, Facebook a lancé à intervalles réguliers des initiatives exactement dans ce but, comme le sinistre Beacon tool, qui vous espionne lorsque vous surfez sur le Web puis ajoute vos activités sur le web à votre timeline publique, permettant à vos amis de surveiller vos habitudes de navigation. Beacon a suscité une révolte des utilisateurs. À chaque fois, Facebook a renoncé à ses actions de surveillance, mais jamais complètement ; inévitablement, le nouveau Facebook vous surveillera plus que l'ancien Facebook, mais moins que le Facebook intermédiaire qui suit le lancement d'un nouveau produit ou service.

Le rythme auquel Facebook a augmenté ses efforts de surveillance semble lié au climat compétitif autour de Facebook. Plus Facebook avait de concurrents, mieux il se comportait. À chaque fois qu'un concurrent majeur s'est effondré, le comportement de Facebook s'est notablement dégradé.

Dans le même temps, Facebook a racheté un nombre prodigieux d'entreprises, y compris une société du nom de Onavo. À l'origine, Onavo a créé une application mobile pour suivre l'évolution de la batterie. Mais les permissions que demandaient Onavo étaient telles que l'appli était capable de recueillir de façon très précise l'intégralité de ce que les utilisateurs font avec leurs téléphones, y compris quelles applis ils utilisent et comment.

Avec l’exemple d’Onavo, Facebook a découvert qu’il était en train de perdre des parts de marché au profit de Snapchat, une appli qui, comme Facebook une décennie plus tôt, se vend comme l’alternative qui respecte la vie privée par rapport au statu quo . À travers Onavo, Facebook a pu extraire des données des appareils des utilisateurs de Snapchat, que ce soient des utilisateurs actuels ou passés. Cela a poussé Facebook à racheter Instagram, dont certaines fonctionnalités sont concurrentes de Snapchat, et a permis à Facebook d’ajuster les fonctionnalités d’Instagram ainsi que son discours marketing dans le but d’éroder les gains de Snapchat et s’assurer que Facebook n’aurait pas à faire face aux pressions de la concurrence comme celles subies par le passé par Myspace et Orkut.

La manière dont Facebook a écrasé Snapchat révèle le lien entre le monopole et le capitalisme de surveillance. Facebook a combiné la surveillance avec une application laxiste des lois antitrust pour repérer de loin la menace de la concurrence par Snapchat et pour prendre des mesures décisives à son encontre. Le capitalisme de surveillance de Facebook lui a permis d’éviter la pression de la concurrence avec des tactiques anti-compétitives. Les utilisateurs de Facebook veulent toujours de la confidentialité, Facebook n’a pas utilisé la surveillance pour les convaincre du contraire, mais ils ne peuvent pas l’obtenir car la surveillance de Facebook lui permet de détruire tout espoir d’émergence d’un rival qui lui fait concurrence sur les fonctionnalités de confidentialité.

Un monopole sur vos amis

Un mouvement de décentralisation a essayé d’éroder la domination de Facebook et autres entreprises des géants de la tech en proposant des alternatives sur le Web indépendant (indieweb) : Mastodon en alternative à Twitter, Diaspora en alternative à Facebook, etc, mais ces efforts ont échoué à décoller.

Fondamentalement, chacun de ces services est paralysé par le même problème : tout utilisateur potentiel d’une alternative de Facebook ou Twitter doit convaincre tous ses amis de le suivre sur une alternative décentralisée pour pouvoir continuer à avoir les bénéfices d’un média social. Pour beaucoup d’entre nous, la seule raison pour laquelle nous avons un compte Facebook est parce que nos amis ont des comptes Facebook, et la raison pour laquelle ils ont des comptes Facebook est que nous avons des comptes Facebook.

Tout cela a contribué à faire de Facebook, et autres plateformes dominantes, des « zones de tir à vue » dans lesquelles aucun investisseur ne financera un nouveau venu.

Et pourtant, tous les géants d’aujourd’hui sont apparus malgré l’avantage bien ancré des entreprises qui existaient avant eux. Pour comprendre comment cela a été possible, il nous faut comprendre l’interopérabilité et l’interopérabilité antagoniste.

Le gros problème de nos espèces est la coordination.

L’« interopérabilité » est la capacité qu’ont deux technologies à fonctionner l’une avec l’autre : n’importe qui peut fabriquer un disque qui jouera sur tous les lecteurs de disques, n’importe qui peut fabriquer un filtre que vous pourrez installer sur la ventilation de votre cuisinière, n’importe qui peut fabriquer l’essence pour votre voiture, n’importe qui peut fabriquer un chargeur USB pour téléphone qui fonctionnera dans votre allume-cigare, n’importe qui peut fabriquer une ampoule qui marchera dans le culot de votre lampe, n’importe qui peut fabriquer un pain qui grillera dans votre grille-pain.

L’interopérabilité est souvent une source d’innovation au bénéfice du consommateur : Apple a fabriqué le premier ordinateur personnel viable commercialement, mais des millions de vendeurs de logiciels indépendants ont fait des programmes interopérables qui fonctionnaient sur l’Apple II Plus. La simple antenne pour les entrées analogiques à l’arrière des téléviseurs a d’abord permis aux opérateurs de câbles de se connecter directement aux télévisions, puis ont permis aux entreprises de consoles de jeux et ensuite aux ordinateurs personnels d’utiliser une télévision standard comme écran. Les prises téléphoniques RJ11 standardisées ont permis la production de téléphones par divers vendeurs avec divers formes, depuis le téléphone en forme de ballon de foot reçu en cadeau d’abonnement de *Sports Illustrated*, aux téléphones d’affaires avec haut-parleurs, mise en attente, et autres, jusqu’aux répondeurs et enfin les modems, ouvrant la voie à la révolution d’Internet.

On utilise souvent indifféremment « interopérabilité » et « standardisation », qui est le processus pendant lequel les fabricants et autres concernés négocient une liste de règles pour l’implémentation d’une technologie, comme les prises électriques de vos murs, le bus de données CAN utilisé par le système de votre voiture, ou les instructions HTML que votre navigateur internet interprète.

Mais l’interopérabilité ne nécessite pas la standardisation, en effet la standardisation émerge souvent du chaos de mesures d’interopérabilité ad hoc. L’inventeur du chargeur USB dans l’allume-cigare n’a pas eu besoin d’avoir la permission des fabricants de voitures ou même des fabricants des pièces du tableau de bord. Les fabricants automobiles n’ont pas mis en place des contre-mesures pour empêcher l’utilisation de ces accessoires d’après-vente par leurs consommateurs, mais ils n’ont pas non plus fait en sorte de faciliter la vie des fabricants de chargeurs. Il s’agit d’une forme d’« interopérabilité neutre ».

Au-delà de l’interopérabilité neutre, il existe l’« interopérabilité antagoniste ». C’est quand un fabricant crée un produit qui interagit avec le produit d’un autre fabricant en dépit des objections du deuxième fabricant, et cela même si ça nécessite de contourner un système de sécurité conçu pour empêcher l’interopérabilité.

Le type d’interopérabilité antagoniste le plus usuel est sans doute les cartouches d’encre d’imprimantes par des fournisseurs tiers. Les fabricants d’imprimantes affirment qu’ils vendent les imprimantes en dessous de leur coût et que leur seul moyen de récupérer les pertes est de se constituer une marge élevée sur les encres. Pour empêcher les propriétaires d’imprimantes d’acheter leurs cartouches ailleurs, les entreprises d’imprimantes appliquent une série de systèmes de sécurité anti-consommateurs qui détectent et rejettent les cartouches re-remplies ou par des tiers.

Les propriétaires d’imprimantes quant à eux défendent le point de vue que HP et Epson et Brother ne sont pas des œuvres caritatives et que les consommateurs de leurs produits n’ont aucune obligation à les aider à survivre, et donc que si ces entreprises choisissent de vendre leurs produits à perte, il s’agit de leur choix stupide et à eux d’assumer les conséquences. De même, les compétiteurs qui fabriquent des cartouches ou les re-remplissent font remarquer qu’ils ne doivent rien aux entreprises d’imprimantes, et que le fait qu’ils érodent les marges de ces entreprises est le problème de celles-ci et non celui de leurs compétiteurs. Après tout, les entreprises d’imprimantes n’ont aucun scrupule à pousser un re-remplisseur à fermer boutique, donc pourquoi est-ce que les re-remplisseurs devraient se soucier de la bonne santé économique des entreprises d’imprimantes ?

L’interopérabilité antagoniste a joué un rôle hors normes dans l’histoire de l’industrie tech : depuis la création du « alt.* » dans les catégories de Usenet (qui a commencé à l’encontre des souhaits des responsables de Usenet et qui s’est développé au point d’être plus important que tout le Usenet

combiné) à la guerre des navigateurs (lorsque Netscape et Microsoft ont dépensé d'énormes ressources en ingénierie pour faire en sorte que leur navigateur soit incompatible avec les fonctionnalités spéciales et autres peccadilles de l'autre) à Facebook (dont le succès a entre autres été dû au fait qu'il a aidé ses nouveaux utilisateurs en leur permettant de rester en contact avec les amis qu'ils ont laissés sur Myspace parce que Facebook leur a fourni un outil pour s'emparer des messages en attente sur Myspace et les importer sur Facebook, créant en pratique un lecteur Myspace basé sur Facebook).

Aujourd'hui, la validation par le nombre est considérée comme un avantage inattaquable. Facebook est là où tous vos amis sont, donc personne ne peut fonder un concurrent à Facebook. Mais la compatibilité antagoniste retourne l'avantage concurrentiel : si vous êtes autorisés à concurrencer Facebook en proposant un outil qui importe les messages en attente sur Facebook de tous vos utilisateurs dans un environnement qui est compétitif sur des terrains que Facebook ne pourra jamais atteindre, comme l'élimination de la surveillance et des pubs, alors Facebook serait en désavantage majeur. Vous aurez rassemblé tous les potentiels ex-utilisateurs de Facebook sur un unique service facile à trouver. Vous les auriez éduqués sur la façon dont un service Facebook-like fonctionne et quels sont ses potentiels avantages, et vous aurez fourni un moyen simple aux utilisateurs mécontents de Facebook pour dire à leurs amis où ils peuvent trouver un meilleur traitement.

L'interopérabilité antagoniste a été la norme pendant un temps et une contribution clef à une scène tech dynamique et vibrante, mais à présent elle est coincée derrière une épaisse forêt de lois et règlements qui ajoutent un risque légal aux tactiques éprouvées de l'interopérabilité antagoniste. Ces nouvelles règles et les nouvelles interprétations des règles existantes signifient qu'un potentiel « interopérateur » antagoniste aura besoin d'échapper aux réclamations de droits d'auteurs, conditions de service, secret commercial, ingérence et brevets.

En l'absence d'un marché concurrentiel, les faiseurs de lois ont délégué des tâches lourdes et gouvernementales aux sociétés de Big Tech, telles que le filtrage automatique des contributions des utilisateurs pour la violation des droits d'auteur ou pour des contenus terroristes et extrémistes ou pour détecter et empêcher le harcèlement en temps réel ou encore pour contrôler l'accès au contenu sexuel.

Ces mesures ont fixé une taille minimale à partir de laquelle on peut faire du Big Tech, car seules les très grandes entreprises peuvent se permettre les filtres humains et automatiques nécessaires pour se charger de ces tâches.

Mais ce n'est pas la seule raison pour laquelle rendre les plateformes responsables du maintien de l'ordre parmi leurs utilisateurs mine la compétition. Une plateforme qui est chargée de contrôler le comportement de ses utilisateurs doit empêcher de nombreuses techniques vitales à l'interopérabilité antagoniste de peur qu'elles ne contreviennent à ses mesures de contrôle. Par exemple si quelqu'un utilisant un remplaçant de Twitter tel que Mastodon est capable de poster des messages sur Twitter et de lire des messages hors de Twitter, il pourrait éviter les systèmes automatiques qui détectent et empêchent le harcèlement (tels que les systèmes qui utilisent le timing des messages ou des règles basées sur les IP pour estimer si quelqu'un est un harceleur).

Au point que nous sommes prêts à laisser les géants de la tech s'autocontrôler, plutôt que de faire en sorte que leur industrie soit suffisamment limitée pour que les utilisateurs puissent quitter les mauvaises plateformes pour des meilleures et suffisamment petites pour qu'une réglementation qui

ferait fermer une plateforme ne détruirait pas l'accès aux communautés et données de milliards d'utilisateurs, nous avons fait en sorte que les géants de la tech soient en mesure de bloquer leurs concurrents et qu'il leur soit plus facile de demander un encadrement légal des outils pour bannir et punir les tentatives à l'interopérabilité antagoniste.

En définitive, nous pouvons essayer de réparer les géants de la tech en les rendant responsables pour les actes malfaisants de ses utilisateurs, ou bien nous pouvons essayer de réparer Internet en réduisant la taille de géants. Mais nous ne pouvons pas faire les deux. Pour pouvoir remplacer les produits des géants d'aujourd'hui, nous avons besoin d'éclaircir la forêt légale qui empêche l'interopérabilité antagoniste de façon à ce que les produits de demain, agiles, personnels, de petite échelle, puissent se fédérer sur les géants tels que Facebook, permettant aux utilisateurs qui sont partis à continuer à communiquer avec les utilisateurs qui ne sont pas encore partis, envoyant des vignes au-dessus du mur du jardin de Facebook afin que les utilisateurs piégés de Facebook puissent s'en servir afin de grimper aux murs et de s'enfuir, accédant au Web ouvert et global.