Détruire le capitalisme de surveillance – 5

Voici la cinquième partie de l'essai que consacre Cory Doctorow au capitalisme de surveillance (parcourir sur le blog les épisodes précédents – parcourir les cinq premiers épisodes en un seul PDF de 50 pages).

Billet original sur le Medium de OneZero : How To Destroy Surveillance Capitalism

Traduction Framalang : Claire, Fabrice, goofy, Jums, Susyl, anonymes

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, 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.

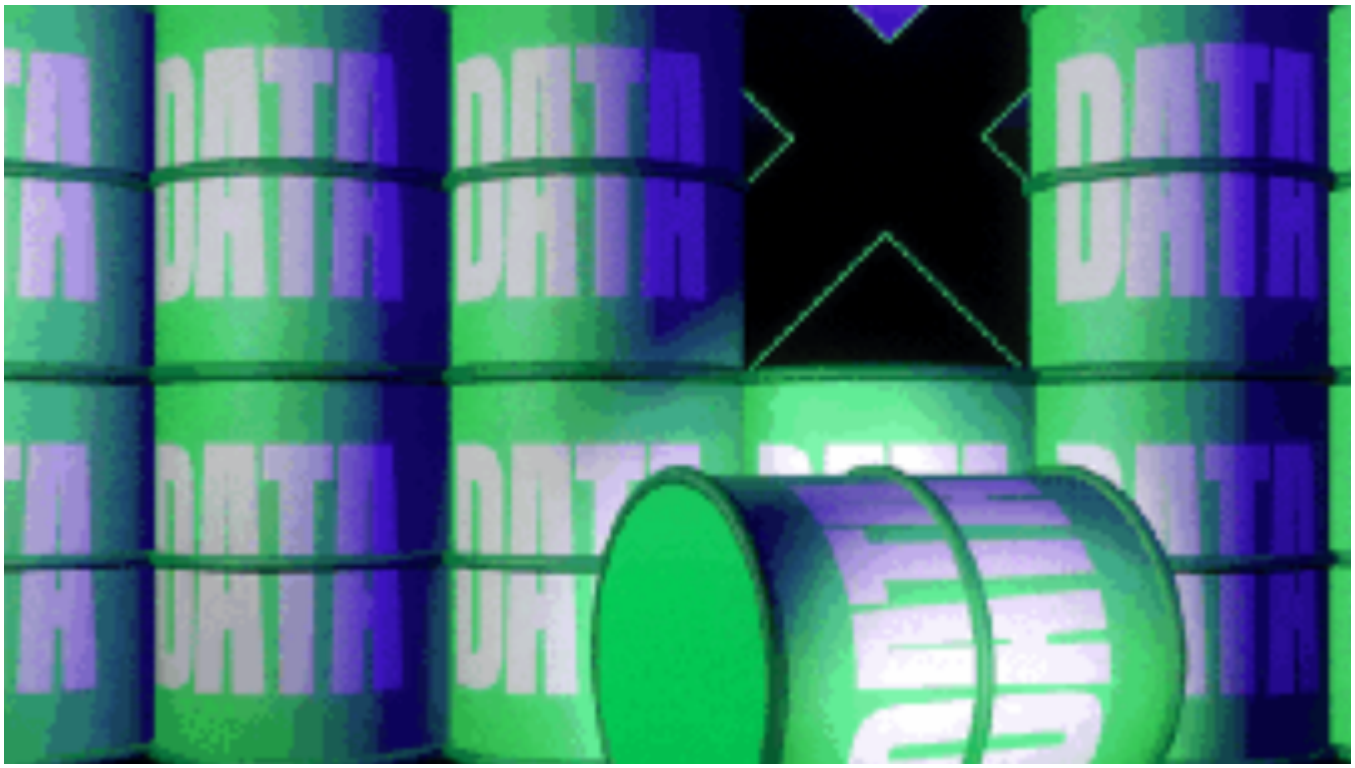
Cette partie de vous, tendre et fragile, que vous exposez au monde dans ces moments-là, est bien trop délicate pour être révélée à autrui, pas même à une personne à laquelle vous faites autant confiance qu'un enfant à ses parents.

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 étaient 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.

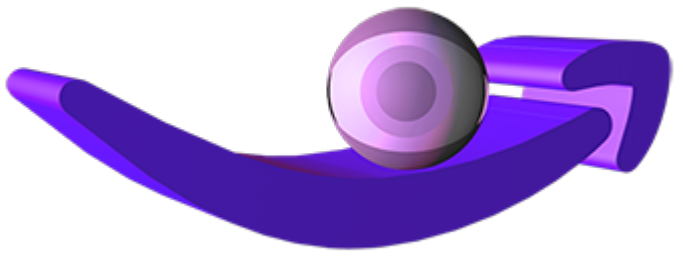
Les géants de la tech collectent nos données pour de nombreuses raisons, y compris la diminution du rendement des stocks de données existants. Mais de nombreuses entreprises technologiques collectent également des données en raison d'une croyance exceptionnaliste erronée aux effets de réseau des données. 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 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 l’architecture 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.

(à suivre)