Détruire le capitalisme de surveillance – 4

Voici la quatrième partie de l'essai que consacre Cory Doctorow au capitalisme de surveillance (parcourir sur le blog les épisodes précédents – parcourir les trois premiers épisodes en PDF : doctorow-1-2-3).

Traduction Framalang : Claire, Fabrice, goofy, jums, mo, ngfchristian, retrodev, tykayn

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

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

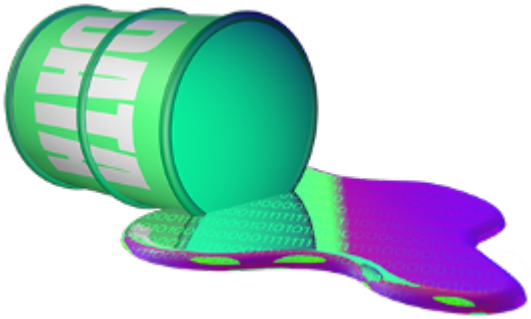
Cela fait quarante ans que le projet de Bork pour réhabiliter les monopoles s'est réalisé, soit une génération et demie, c'est à dire suffisamment de temps pour qu'une idée commune puisse devenir farfelue ou l'inverse. Avant les années 40, les Américains aisés habillaient leurs petits garçons en rose 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.