Détruire le capitalisme de surveillance (3)

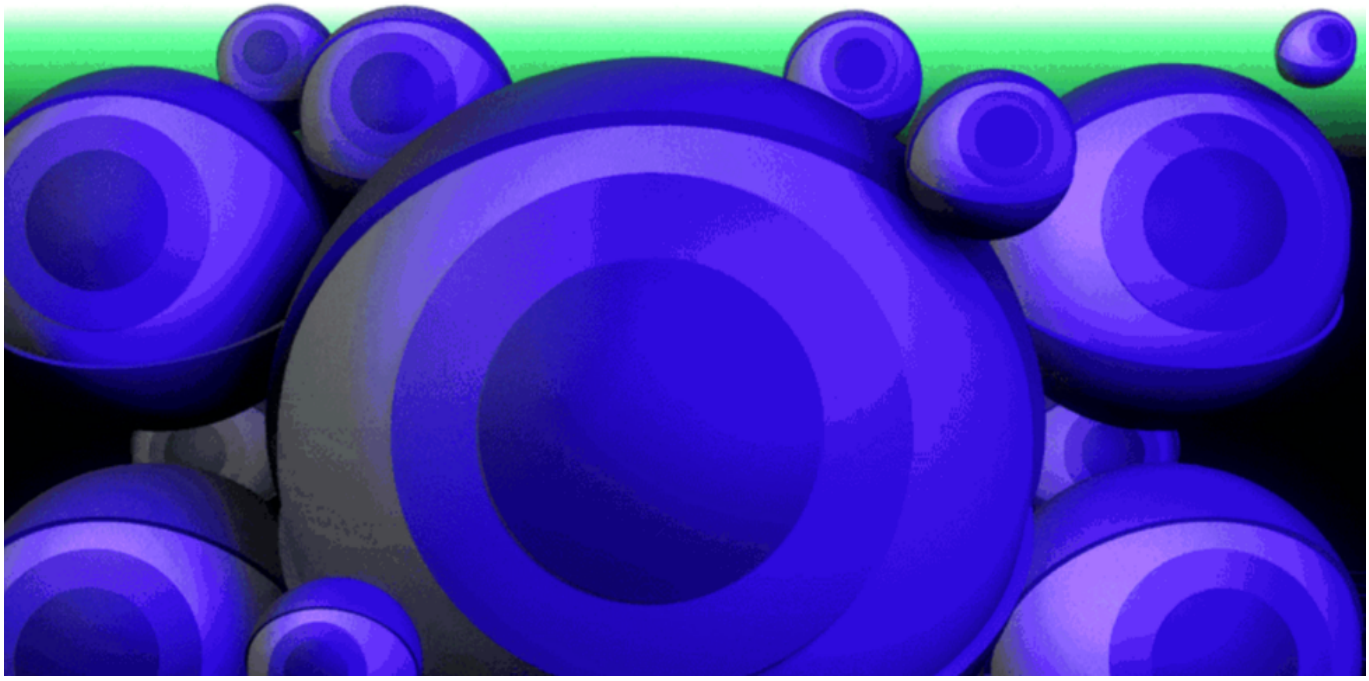
Voici une troisième partie de l'essai que consacre Cory Doctorow au capitalisme de surveillance (parcourir sur le blog les épisodes précédents – parcourir les trois premiers épisodes en PDF : doctorow-1-2-3). Il s'attache ici à démonter les mécanismes utilisés par les Gafam pour lutter contre nos facultés à échapper aux messages publicitaires, mais aussi pour faire croire aux publicitaires que leurs techniques sont magiquement efficaces. Il insiste également sur la quasi-impunité dont bénéficient jusqu'à présent les géants de la Tech…

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

Traduction Framalang : Claire, Fabrice, Gangsoleil, Goofy, Jums, Laure, Retrodev

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

par Cory Doctorow



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 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 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 prétendues 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). 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. 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

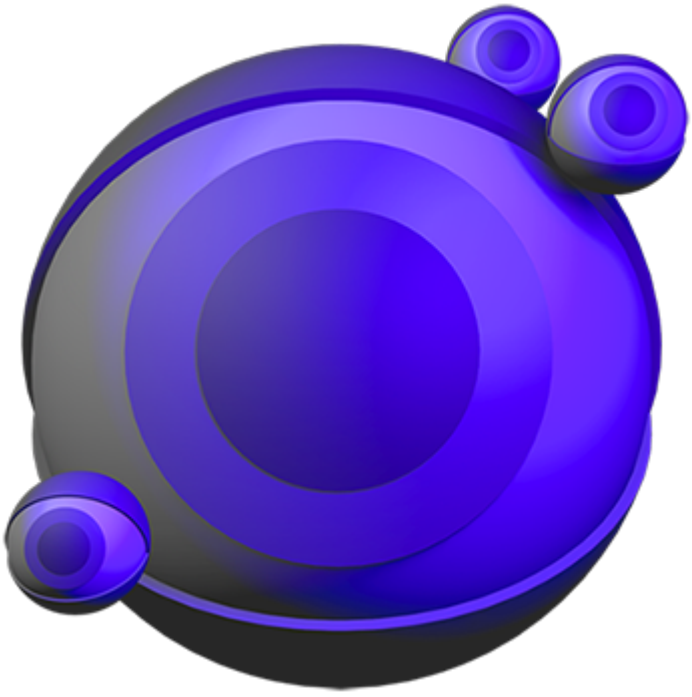
faire librement leurs choix, alors une application rigoureuse de la législation antitrust semble être un excellent remède. Si nous avions refusé à Google le droit d'effectuer ses nombreuses fusions, nous lui aurions probablement aussi refusé sa domination totale dans le domaine de la recherche. Sans 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.

(à suivre…)