Un professeur de Harvard expose Google et Facebook

[Source : cogiito.com]

10 Decembre 2022, par le Dr Mercola

https://articles.mercola.com/sites/articles/archive/2022/12/10/surveillance-capitalism.aspx?ui=bf44c67dbbe698b8fcdd71f20d71cfa1d832c892640d87fefbbbdcc255ad581d&sd=20221129&cid_source=dnl&cid_medium=email&cid_content=art3HL&cid=20221210&cid=DM1303633&bid=1665765878

L'HISTOIRE EN UN COUP D'ŒIL

> Dans son livre intitulé « The Age of Surveillance Capitalism », Shoshana Zuboff, psychologue sociale et professeur à Harvard, révèle comment les plus grandes entreprises technologiques du monde ont détourné nos données personnelles – ce que l'on appelle les « flux de données comportementales excédentaires » – à notre insu et sans notre consentement, et les utilisent contre vous pour générer des profits.
>
> Des entreprises comme Facebook, Google et des tiers de toutes sortes ont le pouvoir – et l'utilisent – de cibler vos démons intérieurs, de vous déclencher et de profiter de vous au moment où vous êtes le plus vulnérable pour vous inciter à agir de manière à les servir, commercialement ou politiquement.
>
> Votre existence entière – même vos humeurs changeantes, déchiffrées par un logiciel de reconnaissance faciale – est devenue une source de revenus pour les entreprises, car vous êtes habilement manœuvré pour faire (et généralement acheter) ou penser quelque chose que vous n'auriez peut-être pas fait, acheté ou pensé autrement.
>
> Les expériences massives de Facebook, dans lesquelles l'entreprise a utilisé des signaux subliminaux pour voir si elle pouvait rendre les

gens plus heureux ou plus tristes et affecter le comportement réel hors ligne, ont prouvé qu'en manipulant le langage et en insérant des signaux subliminaux dans le contexte en ligne, elle pouvait modifier le comportement et les émotions du monde réel, et que ces méthodes et pouvoirs pouvaient être exercés "sans que l'utilisateur en ait conscience".

Le système de sécurité Nest de Google intègre un microphone caché qui ne figure dans aucun des schémas de l'appareil. Les données vocales, et toutes les informations fournies par vos conversations quotidiennes, sont extrêmement précieuses pour le Big Data, et viennent s'ajouter à ses capacités de modélisation prédictive en constante expansion.

> "Dans une pièce où les gens entretiennent unanimement une conspiration du silence, un mot de vérité résonne comme un coup de pistolet."
>
> ~ Czesław Miłosz1

Ces dernières années, un certain nombre d'individus courageux nous ont alertés sur le fait que nous sommes tous surveillés et manipulés par des collecteurs de big data tels que Google et Facebook, et ont fait la lumière sur la profondeur et l'ampleur de cette surveillance permanente. Parmi eux, Shoshana Zuboff, psychologue sociale et professeur à Harvard.

Son livre, *"The Age of Surveillance Capitalism"*, est l'un des meilleurs ouvrages que j'ai lus ces dernières années. Il est absolument indispensable si vous vous intéressez à ce sujet et si vous voulez comprendre comment Google et Facebook ont obtenu un contrôle aussi massif de votre vie.

Son livre révèle comment les plus grandes entreprises technologiques du monde ont détourné nos données personnelles – ce que l'on appelle les *"flux de données sur les surplus comportementaux"* – à notre insu et sans notre consentement et les utilisent contre nous pour générer des profits pour eux-mêmes.

> NOUS sommes devenus le produit.
>
> NOUS sommes le véritable flux de revenus dans cette économie numérique.

"Le terme "capitalisme de surveillance" n'est pas un terme arbitraire", déclare Zuboff dans le documentaire vedette de VPRO Backlight. "Pourquoi 'surveillance' ? Parce qu'il doit s'agir d'opérations conçues pour être indétectables, indéchiffrables, enveloppées dans une rhétorique qui vise à nous tromper, à nous obscurcir et à nous embobiner tous, tout le

> temps.”

La naissance du capitalisme de surveillance

Dans la vidéo présentée, Zuboff “révèle une forme impitoyable de capitalisme dans laquelle aucune ressource naturelle, mais le citoyen lui-même, sert de matière première”.2 Elle explique également comment ce capitalisme de surveillance est né.

Comme pour la plupart des inventions révolutionnaires, le hasard a joué un rôle. Après la crise des dot.com de 2000 qui a fait éclater la bulle Internet, une jeune entreprise nommée Google a lutté pour survivre. Les fondateurs Larry Page et Sergey Brin semblaient voir le début de la fin pour leur entreprise.

Par hasard, ils ont découvert que les “données résiduelles” laissées par les utilisateurs lors de leurs recherches sur Internet avaient une valeur considérable. Ils pouvaient échanger ces données ; ils pouvaient les vendre. En compilant ces données résiduelles, ils pouvaient prédire le comportement d’un internaute donné et garantir ainsi aux annonceurs une audience plus ciblée. C’est ainsi qu’est né le capitalisme de surveillance.

La collecte de données que vous connaissez est celle qui a le moins de valeur

Des commentaires tels que “Je n’ai rien à cacher, donc je me fiche qu’ils me pistent” ou “J’aime les publicités ciblées parce qu’elles facilitent mes achats” révèlent notre ignorance de ce qui se passe réellement.

Nous croyons comprendre quel type d’informations est collecté à notre sujet. Par exemple, vous ne vous souciez peut-être pas que Google sache que vous avez acheté un certain type de chaussures ou un certain livre.

Toutefois, les informations que nous communiquons librement sont les moins importantes des informations personnelles qui sont effectivement recueillies à notre sujet, note M. Zuboff. Les entreprises technologiques nous disent que les données collectées sont utilisées pour améliorer les services, et c’est effectivement le cas pour certaines d’entre elles.

Mais elles sont également utilisées pour modéliser le comportement humain en analysant les modèles de comportement de centaines de millions de personnes. Une fois que vous disposez d’un modèle d’entraînement suffisamment important, vous pouvez commencer à prédire avec précision le comportement de différents types d’individus au fil du temps.

Les données recueillies sont également utilisées pour prédire toute une série d'attributs individuels vous concernant, tels que des traits de personnalité, l'orientation sexuelle, l'orientation politique – "toute une série de choses que nous n'avons jamais eu l'intention de divulguer", explique M. Zuboff.

Comment les données prédictives sont-elles utilisées ?

Toutes sortes de données prédictives sont transmises avec chaque photo que vous téléchargez sur les médias sociaux. Par exemple, il n'y a pas que les entreprises technologiques qui peuvent voir vos photos. Votre visage est utilisé à votre insu et sans votre consentement pour former un logiciel de reconnaissance faciale, et personne ne sait comment ce logiciel est censé être utilisé.

À titre d'exemple, le gouvernement chinois utilise un logiciel de reconnaissance faciale pour suivre et surveiller les groupes minoritaires et les défenseurs de la démocratie, et cela pourrait se produire ailleurs aussi, à tout moment.

La photo que vous avez téléchargée de vous-même lors d'une fête fournit donc toute une série d'informations précieuses, qu'il s'agisse du type de personnes avec lesquelles vous êtes le plus susceptible de passer du temps, des endroits où vous êtes susceptible d'aller pour vous amuser ou des informations sur la façon dont les muscles de votre visage bougent et modifient la forme de vos traits lorsque vous êtes de bonne humeur.

En rassemblant une quantité stupéfiante de points de données sur chaque personne, minute par minute, le Big Data peut faire des prédictions très précises sur le comportement humain, et ces prédictions sont ensuite "vendues aux entreprises clientes qui veulent maximiser notre valeur pour leur entreprise", explique M. Zuboff.

Votre existence entière – même vos humeurs changeantes, déchiffrées par un logiciel de reconnaissance faciale – est devenue une source de revenus pour de nombreuses entreprises technologiques. Vous pouvez penser que vous avez votre libre arbitre mais, en réalité, vous êtes habilement manœuvré et amené à faire (et généralement à acheter) ou à penser quelque chose que vous n'auriez peut-être pas fait, acheté ou pensé autrement…

Les expériences de contagion de Facebook

Dans le documentaire, Zuboff met en lumière les "expériences de contagion" massives de Facebook[3,4,] dans lesquelles l'entreprise a utilisé des signaux subliminaux et des manipulations du langage pour voir si elle pouvait rendre les gens plus heureux ou plus tristes et affecter le comportement réel hors ligne. Il s'avère que c'est possible. Ces expériences ont permis de tirer deux conclusions essentielles :

> En manipulant le langage et en insérant des indices subliminaux dans le contexte en ligne, ils peuvent modifier le comportement et les émotions dans le monde réel.

Ces méthodes et pouvoirs peuvent être exercés “en contournant la conscience de l’utilisateur”.

Dans la vidéo, Zuboff explique également comment le jeu en ligne Pokemon Go – qui a en fait été créé par Google – a été conçu pour manipuler le comportement et l’activité du monde réel à des fins lucratives. Elle décrit également le stratagème dans son article du New York Times, en disant :

“Les joueurs du jeu ne savaient pas qu’ils étaient des pions dans un véritable jeu de modification du comportement à des fins lucratives, car les récompenses et les punitions liées à la chasse à des créatures imaginaires étaient utilisées pour attirer les gens vers les McDonald’s, les Starbucks et les pizzerias locales qui payaient l’entreprise pour les “passages”, exactement de la même manière que les annonceurs en ligne payent pour les “clics” vers leurs sites web.”

Vous êtes manipulé tous les jours d’innombrables façons.

Zuboff passe également en revue ce que nous avons appris du scandale de Cambridge Analytica. Cambridge Analytica est une entreprise de marketing politique qui, en 2018, a utilisé les données Facebook de 80 millions d’Américains pour déterminer les meilleures stratégies de manipulation des électeurs américains.

Christopher Wylie, désormais ancien directeur de la recherche de Cambridge Analytica, a dénoncé les méthodes de l’entreprise. Selon Wylie, ils avaient tellement de données sur les gens qu’ils savaient exactement comment déclencher la peur, la rage et la paranoïa chez un individu donné. Et, en déclenchant ces émotions, ils pouvaient les manipuler pour qu’ils consultent un certain site web, rejoignent un certain groupe et votent pour un certain candidat.

La réalité est donc que des entreprises comme Facebook, Google et des tiers de toutes sortes ont le pouvoir – et utilisent ce pouvoir – de cibler vos démons intérieurs personnels, de vous déclencher et de profiter de vous lorsque vous êtes le plus faible ou le plus vulnérable pour vous inciter à agir de manière à les servir, commercialement ou politiquement. C’est certainement quelque chose à garder à l’esprit lorsque vous surfez sur le web et les sites de médias sociaux.

“Il y a seulement une minute, nous n’avions pas beaucoup de ces outils, et nous étions bien”, dit Zuboff dans le film. “Nous vivions des vies riches et

bien remplies. Nous avions des liens étroits avec nos amis et notre famille.

Cela dit, je tiens à reconnaître que le monde numérique apporte beaucoup à nos vies, et nous méritons d'avoir tout cela. Mais nous méritons de l'avoir sans payer le prix du capitalisme de surveillance.

> Les citoyens du 21e siècle ne devraient pas avoir à choisir entre passer à l'analogique ou vivre dans un monde où notre autodétermination et notre vie privée sont détruites au nom de cette logique de marché. C'est inacceptable.

Ne soyons pas non plus naïfs. Vous mettez les mauvaises personnes au sein de notre gouvernement, à n'importe quel moment, et elles regardent par-dessus leurs épaules les riches possibilités de contrôle offertes par ces nouveaux systèmes.

> Il viendra un moment où, même en Occident, même dans nos sociétés démocratiques, notre gouvernement sera tenté d'annexer ces capacités et de les utiliser sur nous et contre nous. Ne soyons pas naïfs à ce sujet.

Lorsque nous décidons de résister au capitalisme de surveillance – à l'heure actuelle, lorsqu'il est dans la dynamique du marché – nous préservons également notre avenir démocratique, ainsi que le type de contrepoids dont nous aurons besoin à l'avenir dans une civilisation de l'information si nous voulons préserver la liberté et la démocratie pour une autre génération."

La surveillance devient de plus en plus effrayante

Mais la surveillance et la collecte de données ne s'arrêtent pas à ce que vous faites en ligne. Le Big Data veut aussi avoir accès à vos moments les plus intimes – ce que vous faites et comment vous vous comportez dans l'intimité de votre maison, par exemple, ou dans votre voiture. M. Zuboff raconte comment on a découvert que le système de sécurité Nest de Google était équipé d'un microphone caché qui ne figurait sur aucun des schémas de l'appareil.

> "Les voix sont ce que tout le monde recherche, tout comme les visages", explique M. Zuboff.

Les données vocales, et toutes les informations fournies par vos conversations quotidiennes, sont extrêmement précieuses pour le Big Data, et viennent enrichir ses capacités de modélisation prédictive en constante expansion.

Mme Zuboff explique également comment ces types de dispositifs de collecte de données et forcent les utilisateurs à donner leur consentement en prenant en “otage” la fonctionnalité de l’appareil si vous ne voulez pas que vos données soient collectées et partagées.

Par exemple, les thermostats Nest de Google collecteront des données sur votre utilisation et les partageront avec des tiers, qui les partageront avec des tiers et ainsi de suite à l’infini – et Google n’assume aucune responsabilité pour ce que ces tiers pourraient faire de vos données.

> Vous pouvez refuser cette collecte de données et ce partage avec des tiers, mais si vous le faites, Google ne prendra plus en charge la fonctionnalité du thermostat ; il ne mettra plus à jour votre logiciel et pourra affecter la fonctionnalité d’autres appareils liés, comme les détecteurs de fumée.

Deux universitaires qui ont analysé le contrat du thermostat Nest de Google ont conclu qu’un consommateur un tant soit peu vigilant quant à l’utilisation de ses données de consommation devrait examiner 1 000 contrats de confidentialité avant d’installer un seul thermostat dans sa maison.

Les voitures modernes sont également équipées de multiples caméras qui alimentent le Big Data. Comme indiqué dans le film, la nouvelle voiture moyenne est équipée de 15 caméras, et si vous avez accès aux données d’à peine 1 % de toutes les voitures, vous avez “connaissance de tout ce qui se passe dans le monde”.

> Bien sûr, ces caméras vous sont vendues comme faisant partie intégrante de nouveaux dispositifs de sécurité, mais vous payez cette sécurité supplémentaire avec votre vie privée et celle de tous ceux qui vous entourent.

Les mesures pandémiques érodent rapidement la vie privée

La pandémie actuelle de coronavirus utilise également la “sécurité” comme moyen de démanteler la vie privée. Comme le rapporte le New York Times, le 23 mars 2020 :5

> “En Corée du Sud, les agences gouvernementales exploitent les images des caméras de surveillance, les données de localisation des smartphones et les relevés d’achats par carte de crédit pour aider à retracer les mouvements récents des patients atteints de coronavirus et établir les chaînes de transmission du virus.

En Lombardie, en Italie, les autorités analysent les données de localisation transmises par les téléphones portables des citoyens pour déterminer combien de personnes obéissent à un ordre de confinement gouvernemental et les distances types qu'elles parcourent chaque jour. Environ 40 % d'entre eux se déplacent "trop", a récemment déclaré un responsable.

En Israël, l'agence de sécurité intérieure du pays est sur le point de commencer à utiliser une base de données de localisation des téléphones portables – initialement destinée aux opérations de lutte contre le terrorisme – pour tenter de localiser les citoyens qui ont pu être exposés au virus.

Alors que les pays du monde entier s'efforcent d'endiguer la pandémie, nombre d'entre eux déploient des outils de surveillance numérique pour exercer un contrôle social, allant jusqu'à utiliser les technologies des agences de sécurité sur leurs propres civils…

Pourtant, renforcer la surveillance pour combattre la pandémie maintenant pourrait ouvrir définitivement les portes à des formes plus invasives d'espionnage plus tard. C'est une leçon que les Américains ont apprise après les attaques terroristes du 11 septembre 2001, selon les experts en libertés civiles.

Près de vingt ans plus tard, les forces de l'ordre ont accès à des systèmes de surveillance plus puissants, tels que la géolocalisation et la reconnaissance faciale – des technologies qui peuvent être utilisées à des fins politiques …

Nous pourrions très facilement nous retrouver dans une situation où nous donnons au gouvernement local, étatique ou fédéral le pouvoir de prendre des mesures en réponse à cette pandémie qui modifient fondamentalement la portée des droits civils américains", a déclaré Albert Fox Cahn, directeur exécutif du Surveillance Technology Oversight Project, une organisation à but non lucratif de Manhattan."

L'humanité à la croisée des chemins

Zuboff évoque également son travail dans une tribune libre publiée le 24 janvier 2020 dans le New York Times.6,7 "Vous êtes désormais contrôlés à distance. Les capitalistes de la surveillance contrôlent la science et les scientifiques, les secrets et la vérité ", écrit-elle, poursuivant :

> "Nous pensions que nous recherchions Google, mais nous comprenons maintenant que Google nous recherche.
>
> Nous supposions que nous utilisions les médias sociaux pour nous connecter, mais nous avons appris que la connexion est la façon dont les médias sociaux nous utilisent.

Nous nous demandions à peine pourquoi notre nouveau téléviseur ou matelas avait une politique de confidentialité, mais nous avons commencé à comprendre que les politiques de ‘confidentialité’ sont en fait des politiques de surveillance…

> La vie privée n’est pas privée, car l’efficacité des systèmes de surveillance et de contrôle dépend des parties de nous-mêmes que nous abandonnons – ou qui nous sont secrètement volées.

Notre siècle numérique aurait dû être l’âge d’or de la démocratie.

> Au lieu de cela, nous entrons dans sa troisième décennie, marquée par une nouvelle forme d’inégalité sociale que l’on peut qualifier d’”inégalité épistémique” … des asymétries extrêmes de la connaissance et du pouvoir qui en découle, alors que les géants de la technologie prennent le contrôle de l’information et de l’apprentissage lui-même …

Les capitalistes de la surveillance exploitent l’inégalité croissante de la connaissance au nom du profit. Ils manipulent l’économie, notre société et même nos vies en toute impunité, mettant en danger non seulement la vie privée des individus mais aussi la démocratie elle-même …

Pourtant, les vents semblent avoir finalement tourné. Une nouvelle prise de conscience fragile est en train de naître … Les capitalistes de la surveillance sont rapides parce qu’ils ne recherchent ni le consentement authentique ni le consensus. Ils s’appuient sur l’engourdissement psychique et les messages d’inévitabilité pour susciter l’impuissance, la résignation et la confusion qui paralysent leurs proies.

La démocratie est lente, et c’est une bonne chose. Son rythme reflète les dizaines de millions de conversations qui ont lieu… et qui réveillent progressivement le géant endormi de la démocratie.

Ces conversations ont lieu maintenant, et de nombreux signes indiquent que les législateurs sont prêts à se joindre à eux et à diriger. Cette troisième décennie sera probablement déterminante pour notre avenir. Améliorerons-nous l’avenir numérique ou le rendra-t-il pire ? “8,9

Inégalité épistémique

L’inégalité épistémique fait référence à l’inégalité dans ce que vous êtes en mesure d’apprendre.

>

> “Elle se définit comme l’inégalité d’accès à l’apprentissage imposée par les mécanismes commerciaux privés de capture, de production, d’analyse et de vente de l’information. Elle est parfaitement illustrée par l’abîme qui se creuse rapidement entre ce que nous savons et ce que l’on sait de nous”, écrit Mme Zuboff dans sa tribune publiée dans le New York Times.[10]

Google, Facebook, Amazon et Microsoft ont été le fer de lance de la transformation du marché de la surveillance, se plaçant au sommet de la hiérarchie épistémique. Ils savent tout de vous et vous ne savez rien d’eux. Vous ne savez même pas ce qu’ils savent de vous.

> “Ils ont opéré dans l’ombre pour amasser d’énormes monopoles de connaissances en prenant sans demander, une manœuvre que tout enfant reconnaît comme un vol”, écrit Zuboff.

“Le capitalisme de surveillance commence par revendiquer unilatéralement l’expérience humaine privée en tant que matière première gratuite à traduire en données comportementales. Nos vies sont transformées en flux de données.”

Ces flux de données vous concernent, mais ne sont pas pour vous. Tout cela est utilisé contre vous – pour vous séparer de votre argent, ou pour vous faire agir d’une manière qui soit d’une certaine façon profitable à une entreprise ou à un programme politique. Alors, demandez-vous, où est votre liberté dans tout cela ?

Ils vous font danser à leur rythme

> Si une entreprise peut vous inciter à acheter des produits dont vous n’avez pas besoin en diffusant une publicité personnalisée et séduisante pour un produit dont elle sait qu’il vous donnera confiance au moment précis où vous vous sentez peu sûr de vous ou sans valeur (une tactique qui a été testée et perfectionnée[11]), agissez-vous vraiment par votre libre arbitre ?

Si une intelligence artificielle utilisant la modélisation prédictive détecte que vous avez faim (sur la base d’une variété d’indices tels que votre localisation, vos expressions faciales et verbales) et vous envoie une publicité d’un restaurant local au moment même où vous décidez d’aller manger, faites-vous vraiment des choix de vie conscients, autodéterminés et basés sur des valeurs ? Comme le note Zuboff dans son article :[12]

> “L’inégalité des connaissances sur nous produit une inégalité de pouvoir sur nous, et donc l’inégalité épistémique s’élargit pour inclure la distance entre ce que nous pouvons faire et ce qui peut nous être fait.

> Les scientifiques des données décrivent cela comme le passage de la surveillance à l'actionnement, dans lequel une masse critique de connaissances sur un système de machine permet le contrôle à distance de ce système.

Désormais, les gens sont devenus des cibles pour le contrôle à distance, car les capitalistes de la surveillance ont découvert que les données les plus prédictives proviennent de l'intervention dans le comportement pour régler, rassembler et modifier l'action dans le sens des objectifs commerciaux.

Ce troisième impératif, les "économies d'action", est devenu un terrain d'expérimentation intense. Nous apprenons à écrire la musique", a déclaré un scientifique, "et ensuite nous laissons la musique nous faire danser"…

Le fait est qu'en l'absence de transparence des entreprises et de contrôle démocratique, l'inégalité épistémique règne. Ils savent. Ils décident de qui sait. Ils décident de qui décide. L'intolérable désavantage du public en matière de connaissances est aggravé par la perfection des communications de masse des capitalistes de la surveillance, qui en font un éclairage par le gaz….

Le 30 avril 2019, Mark Zuckerberg a fait une annonce spectaculaire lors de la conférence annuelle des développeurs de l'entreprise, déclarant :

> " L'avenir est privé. Quelques semaines plus tard, un avocat plaidant de Facebook s'est présenté devant un juge fédéral de district en Californie pour contrecarrer une action en justice d'un utilisateur pour atteinte à la vie privée, arguant que l'acte même d'utiliser Facebook annule toute attente raisonnable en matière de vie privée 'en droit'."

Nous avons besoin d'un tout nouveau cadre réglementaire

Dans la vidéo, M. Zuboff souligne qu'il n'existe aucune loi pour mettre un frein à ce tout nouveau type de capitalisme de surveillance, et que la seule raison pour laquelle il a pu prospérer au cours des 20 dernières années est l'absence de lois à son encontre, principalement parce qu'il n'a jamais existé auparavant.

> C'est le problème de l'inégalité épistémique. Google et Facebook étaient les seuls à savoir ce qu'ils faisaient. Le réseau de surveillance s'est développé dans l'ombre, à l'insu du public ou des législateurs.

Si nous nous étions battus contre lui pendant deux décennies, nous aurions

peut-être dû nous résigner à la défaite, mais en l'état actuel des choses, nous n'avons même pas essayé de le réglementer.

Selon M. Zuboff, cela devrait nous donner de l'espoir. Nous pouvons renverser la situation et récupérer notre vie privée, mais nous avons besoin d'une législation qui réponde à la réalité de l'ampleur et de la profondeur du système de collecte de données. Il ne suffit pas de s'attaquer aux données que nous savons que nous donnons lorsque nous sommes en ligne. Zuboff écrit :[13]

> "Ces contestations du XXIe siècle exigent un cadre de droits épistémiques inscrits dans la loi et soumis à une gouvernance démocratique.
>
> De tels droits interrompraient les chaînes d'approvisionnement en données en sauvegardant les limites de l'expérience humaine avant qu'elles ne soient attaquées par les forces de la datafication.

Le choix de transformer n'importe quel aspect de la vie d'une personne en données doit appartenir aux individus en vertu de leurs droits dans une société démocratique.

Cela signifie, par exemple, que les entreprises ne peuvent pas revendiquer le droit à votre visage, ni utiliser votre visage comme matière première gratuite pour l'analyse, ni posséder et vendre des produits informatiques dérivés de votre visage…

> Tout ce qui est fait par les humains peut être défait par les humains. Le capitalisme de surveillance est jeune, il a à peine 20 ans, mais la démocratie est ancienne, enracinée dans des générations d'espoir et de contestation.

Les capitalistes de la surveillance sont riches et puissants, mais ils ne sont pas invulnérables. Ils ont un talon d'Achille : la peur.

Ils craignent les législateurs qui ne les craignent pas. Ils craignent les citoyens qui exigent une nouvelle voie à suivre, tout en insistant sur les nouvelles réponses aux anciennes questions : Qui saura ? Qui décidera qui sait ? Qui décidera qui décide ? Qui écrira la musique, et qui dansera ?"

Comment protéger votre vie privée en ligne

S'il ne fait aucun doute que nous avons besoin d'un tout nouveau cadre

législatif pour mettre un frein au capitalisme de surveillance, en attendant, il existe des moyens de protéger votre vie privée en ligne et de limiter les "surplus de données comportementales" recueillies à votre sujet.

Robert Epstein, psychologue chercheur principal à l'American Institute of Behavioral Research and Technology, recommande de prendre les mesures suivantes pour protéger votre vie privée :[14]

Utilisez un réseau privé virtuel (VPN) tel que NordVPN, qui ne coûte qu'environ 3 dollars par mois et peut être utilisé sur un maximum de six appareils. À mon avis, c'est une nécessité si vous cherchez à préserver votre vie privée. Epstein explique :

> "Lorsque vous utilisez votre téléphone portable, votre ordinateur portable ou votre ordinateur de bureau de manière habituelle, votre identité est très facile à voir pour Google et d'autres entreprises. Ils peuvent la voir via votre adresse IP, mais il existe de plus en plus de moyens beaucoup plus sophistiqués de savoir que c'est vous. L'un d'entre eux s'appelle l'empreinte digitale du navigateur.

C'est quelque chose de très inquiétant. En fait, le type de navigateur que vous possédez et la façon dont vous l'utilisez sont comme une empreinte digitale. Vous utilisez votre navigateur d'une manière unique, et juste par la façon dont vous tapez, ces entreprises peuvent maintenant vous identifier instantanément.

Brave offre une certaine protection contre l'empreinte digitale du navigateur, mais vous devez vraiment utiliser un VPN. Ce que fait un VPN, c'est que tout ce que vous faites passe par un autre ordinateur, ailleurs. Cela peut être n'importe où dans le monde, et il existe des centaines de sociétés proposant des services VPN. Celle que je préfère actuellement s'appelle Nord VPN.

> Vous téléchargez le logiciel, l'installez, comme vous installez n'importe quel logiciel. C'est incroyablement facile à utiliser. Vous n'avez pas besoin d'être un technicien pour utiliser Nord, et il vous montre une carte du monde et vous cliquez simplement sur un pays.

Le VPN donne l'impression que votre ordinateur n'est pas votre ordinateur. Il crée une sorte de fausse identité pour vous, et c'est une bonne chose. Maintenant, très souvent, je vais passer par les ordinateurs de Nord aux États-Unis. Il faut parfois le faire, sinon on ne peut pas faire certaines choses. PayPal n'aime pas que vous soyez dans un pays étranger par exemple."

Nord, lorsqu'il est utilisé sur votre téléphone portable, masquera également votre identité lorsque vous utiliserez des applications comme Google Maps.

N'utilisez pas Gmail, car chaque courriel que vous écrivez est stocké de façon permanente. Il devient une partie de votre profil et est utilisé pour construire des modèles numériques de vous, ce qui leur permet de faire des prédictions sur votre ligne de pensée et chaque envie et désir.

De nombreux autres systèmes de messagerie électronique plus anciens, comme AOL et Yahoo, sont également utilisés comme plateformes de surveillance, de la même manière que Gmail.

> ProtonMail.com, qui utilise un cryptage de bout en bout, est une excellente alternative et le compte de base est gratuit.

N'utilisez pas le navigateur Chrome de Google, car tout ce que vous y faites est surveillé, y compris les frappes au clavier et toutes les pages Web que vous avez visitées. Brave est une excellente alternative qui prend la confidentialité au sérieux.

> Brave est également plus rapide que Chrome et supprime les publicités. Il est basé sur Chromium, la même infrastructure logicielle que Chrome, de sorte que vous pouvez facilement transférer vos extensions, vos favoris et vos signets.

N'utilisez pas Google comme moteur de recherche, ni aucune extension de Google, comme Bing ou Yahoo, qui tirent tous deux leurs résultats de recherche de Google.

Il en va de même pour l'assistant personnel Siri de l'iPhone, qui tire toutes ses réponses de Google.

Les moteurs de recherche alternatifs suggérés par Epstein incluent SwissCows et Qwant.

Il recommande d'éviter StartPage, car il a été récemment racheté par une société de marketing en ligne agressive, qui, comme Google, dépend de la surveillance.

N'utilisez pas de téléphone portable Android, pour toutes les raisons évoquées précédemment. Epstein utilise un BlackBerry, qui est plus sûr que les téléphones Android ou l'iPhone. Selon lui, le prochain modèle de BlackBerry, le Key3, sera l'un des téléphones portables les plus sécurisés au monde.

> N’utilisez pas les appareils Google Home dans votre maison ou votre appartement – Ces appareils enregistrent tout ce qui se passe chez vous, qu’il s’agisse de paroles ou de sons tels que se brosser les dents ou faire bouillir de l’eau, même lorsqu’ils semblent inactifs, et renvoient ces informations à Google.

Les téléphones Android écoutent et enregistrent également en permanence, tout comme Nest, le thermostat domestique de Google, et Alexa d’Amazon.

Effacez votre cache et vos cookies – Comme l’explique Epstein dans son article :15

“Les entreprises et les pirates de toutes sortes installent constamment du code informatique invasif sur vos ordinateurs et vos appareils mobiles, principalement pour vous surveiller mais parfois à des fins plus infâmes.

Sur un appareil mobile, vous pouvez effacer la plupart de ces déchets en allant dans le menu des paramètres de votre navigateur, en sélectionnant l’option “confidentialité et sécurité”, puis en cliquant sur l’icône qui efface votre cache et vos cookies.

Avec la plupart des navigateurs d’ordinateurs portables et de bureau, le fait de maintenir trois touches enfoncées simultanément – CTRL, MAJ et DEL – vous permet d’accéder directement au menu correspondant ; j’utilise cette technique plusieurs fois par jour sans même y penser.

Vous pouvez également configurer les navigateurs Brave et Firefox pour qu’ils effacent automatiquement votre cache et vos cookies à chaque fois que vous fermez votre navigateur.”

N’utilisez pas Fitbit, car il a été récemment acheté par Google et leur fournira toutes vos informations physiologiques et vos niveaux d’activité, en plus de tout ce que Google possède déjà sur vous.

Sources et References

- [1] Goodreads.com Czesław Miłosz Quotable Quotes
- [2] Youtube.com, Shoshana Zuboff on Surveillance Capitalism
- [3] Nature September 13, 2012; 489: 295-298 (Archived)
- [4] PNAS June 17, 2014; 111(24): 8788-8790 (Archived)
- [5] New York Times March 23, 2020 (Archived)
- [6, 8] New York Times January 24, 2020
- [7, 9, 10, 12, 13] New York Times January 24, 2020 (Archived)
- [11] The Guardian May 1, 2017 (Archived)
- [14, 15] Medium March 17, 2017