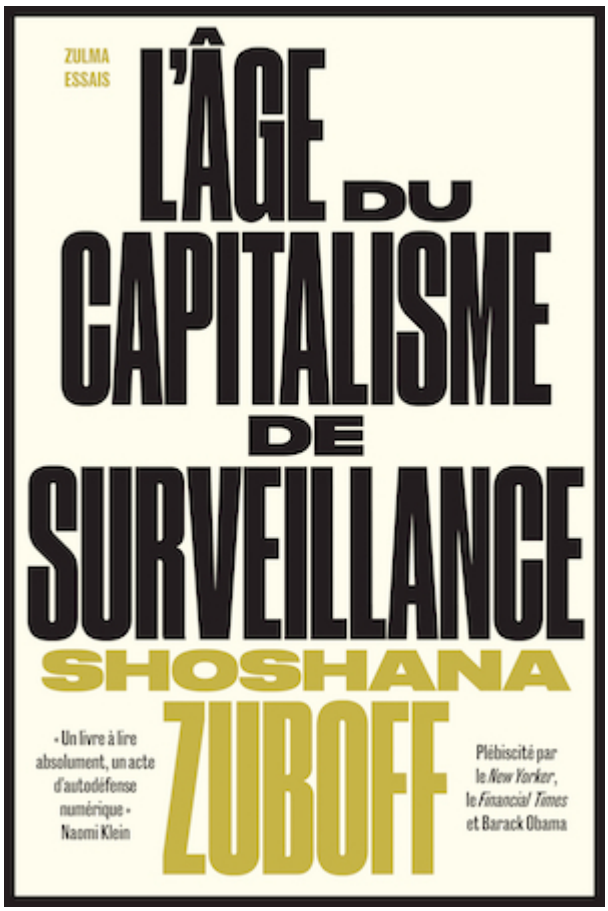
L’Âge du capitalisme de surveillance, par Shoshana Zuboff

mercredi 3 mars 2021, par Jean-Marie NICOLLE



Rien n’est gratuit en ce monde. On devrait s’étonner de la naïveté des internautes qui croient encore en la gratuité des services rendus sur le réseau, comme s’il n’y avait rien à payer pour écouter de la musique, voir des films, obtenir des renseignements médicaux, trouver des conseils de jardinage, etc. Qu’y a-t-il derrière cette apparente gratuité ?

Peu de gens connaissent l’organisation économique des sites web car les grandes sociétés du numérique se gardent bien de fournir des informations sur leurs véritables activités. Derrière l’écran lumineux qui verse généreusement des flots d’informations, il y a la face cachée et même assez sombre du marché numérique. Les véritables clients de l’internet ne sont pas les utilisateurs ordinaires du réseau, mais les usagers qui achètent d’autres services.

Lesquels ? Ce sont les produits transformés d’une matière première fournie gratuitement et à leur insu par les utilisateurs, à savoir leurs données personnelles. Google, Facebook, Amazon et Cie se sont spécialisées dans l’extraction des « data » et ont fait fortune grâce à leur exploitation. La communication des données personnelles est la nouvelle dîme par laquelle les internautes financent sans le savoir la pseudo-gratuité des services.

Shoshana Zuboff, spécialiste de psychologie sociale, analyse dans *L’Âge du capitalisme de surveillance* la jeune histoire de cette nouvelle industrie florissante et révèle les coups fourrés, les transgressions de la loi, tous les crimes contre la démocratie qui ont permis ce capitalisme de surveillance. Si son style est un peu lourd, encombré par le jargon des sciences sociales, si ses explications sont un peu longues et

répétitives (l'ouvrage fait 850 pages !), si ses analyses politiques et philosophiques manquent d'ampleur, il n'en demeure pas moins que son enquête, qui suit pas à pas l'évolution des grandes sociétés de l'Internet, nous livre une documentation considérable (les notes occupent 100 pages). Son mérite est d'avoir obtenu des renseignements essentiels sur des pratiques soigneusement occultées par le bien commode secret industriel.

L'ouvrage est divisé en trois parties correspondant aux trois étapes de cette nouvelle industrie : 1. L'extraction des données personnelles ; 2. Leur exploitation pour concevoir des prédictions de comportements ; 3. La construction d'un pouvoir instrumentalisant.

1. L'extraction des données personnelles

Commençons par le projet de l'Aware Home qui visait à créer un réseau de capteurs sur tous les objets d'une maison et ses habitants, en circuit fermé, pour améliorer le confort d'un chez-soi. En 2018, Google acquiert les différentes sociétés du projet et télécharge toutes les données sur ses serveurs, rompant ainsi le contrat de confidentialité passé avec les utilisateurs. Les données personnelles font alors l'objet d'un nouveau marché car elles vont permettre d'élaborer des données comportementales prédictives. L'extraction des données personnelles a commencé avec le lancement des moteurs de recherche dont le plus important est Google. Au lieu d'effacer au fur et à mesure les requêtes et les historiques de navigation, Google les conserve pour les analyser et les transformer en de nouvelles données. Déjà, en 2004, Gmail, lancé par Google, explorait la correspondance privée de ses utilisateurs pour leur envoyer de la publicité ciblée. En 2007, Facebook permettait à ses annonceurs de suivre les utilisateurs sur Internet et de divulguer leurs achats à leur réseau personnel sans autorisation. Devant de tels viols de la vie privée, des utilisateurs ont déposé plainte. La cour de justice de l'Union Européenne a alors promulgué un droit à l'oubli en 2014, mais cela n'empêcha pas Google de poursuivre son pillage des données personnelles par d'autres voies.

Ses ingénieurs ont bien vu que les résidus des interactions avec les utilisateurs (nombre de recherches, tournure de la requête, orthographe des mots, ponctuation, temps passé, localisation de l'utilisateur, etc.) valaient de l'or si on savait bien les exploiter. Cette énergie dépensée par les utilisateurs est un travail récupéré par Google, mais un travail non rémunéré, car il n'y a aucun contrat. Les utilisateurs sont des sources gratuites d'approvisionnement de matière première.

Par l'analyse des données, on a d'abord pu affiner le ciblage de la publicité qui n'est plus liée aux mots-clés d'une requête ; elle devient plus « personnelle », liée au savoir que l'on a pu reconstituer sur chaque utilisateur. Google a pu ainsi augmenter le prix de ses publicités en garantissant à l'annonceur une plus grande précision dans le ciblage. Le service rendu aux utilisateurs du moteur de recherche devient secondaire ; ce qui compte, c'est de déchiffrer le profil de chacun pour faire correspondre les publicités à ses centres d'intérêt, lesquels sont déduits des traces de son comportement face à son écran. La visée obtenue est moins aléatoire, plus sûre, et donc, vaut plus cher.

Comme lors de l'impérialisme colonialiste, le capitalisme a su profiter d'un vide juridique sur un nouvel espace transfrontalier. Profitant de l'effet de surprise, le capitalisme numérique prend de court les États qui réagissent tard et maladroitement ; il invoque la liberté d'innover contre les réglementations contraignantes, et gagne ainsi de considérables marges de manœuvre pour exploiter ses affaires. Constituées en groupe de pression (*lobby*), les sociétés numériques font passer des lois en leur faveur. Ainsi, en 1996, une loi est adoptée au Congrès américain qui protège les sites de toute responsabilité (section 230 du *Communications Decency Act*) : « Aucun fournisseur, aucun utilisateur d'un service informatique interactif ne sera traité comme l'éditeur ou l'émetteur d'une information livrée par un autre fournisseur de contenu informatif. » On ne pourra poursuivre en justice une plate-forme en ligne pour le contenu des informations qu'elle affiche.

Pour obtenir encore plus de données, Google n'a pas hésité à favoriser des fabricants de téléphones mobiles, comme les appareils Android, afin d'y introduire des applications à son service. La fonction de

téléphone recouvre en fait une fonction d'approvisionnement des données personnelles. Malgré le système d'autorisations présenté à l'utilisateur pour sélectionner la communication de ses données sur son téléphone, en réalité, Android donne tout à Google. Des applications apparemment innocentes comme la météo, les lampes de poche, le covoiturage, etc., contiennent des programmes de traçage. Par exemple, le téléphone émet un son imperceptible à l'oreille humaine qui permet de détecter sa présence dans tel ou tel immeuble doté de capteurs. Même si le téléphone est éteint, la géolocalisation est maintenue : « Les téléphones Android recueillent depuis le début 2017 des informations en triangulant l'antenne la plus proche, et ceci même si la géolocalisation est éteinte, que les applis sont toutes éteintes et qu'il n'y a pas de carte SIM dans le téléphone. »

Une autre technique d'extraction de données personnelles consiste à introduire un « assistant numérique » dans un logiciel, comme Microsoft l'a fait avec Cortana : sous prétexte d'aider l'utilisateur dans ses difficultés techniques, on insère un programme espion qui permet de compléter son profil. Cependant, comment faire lorsque l'utilisateur change d'appareil ? Comment continuer à le suivre lorsqu'on a perdu l'identifiant de sa machine et que les cookies envoyés ne répondent plus ? Une société américaine, Verizon, a mis au point un numéro de suivi dissimulé et ineffaçable pour chaque utilisateur, un identifiant incontournable par la navigation privée ou d'autres outils de confidentialité. Le nœud une fois fermé, l'utilisateur ne peut plus s'en défaire. Plus aucune procédure de retrait ne fonctionne.

La pratique du *selfie* est aussi une source extraordinaire. En explorant tous les visages photographiés et mis en ligne sur Facebook (350 millions de photos par jour !), cette entreprise a mis au point un logiciel de reconnaissance faciale qui approche les 100% de réussite. En analysant les poses, le regard, l'habillement, la coiffure, les postures, etc., on peut profiler les individus et prédire leurs comportements. Après le visage, la voix : les répondeurs vocaux complexes, qui proposent une sorte de « conversation » avec le client, enregistrent des paroles facilement analysables par la suite. « Il fut un temps où vous exploriez grâce à Google. Maintenant, c'est vous que Google explore. »

Le poste de télévision peut aussi nous surveiller, comme la Smart TV de Samsung qui enregistre tout ce qui se dit à proximité du poste. Les jouets comme les poupées interactives ou les robots glanent des informations auprès des enfants en leur demandant leur adresse par exemple. Amazon a obtenu de certaines entreprises de BTP l'installation dans les plafonds des immeubles en construction d'enceintes connectées, des serrures, des thermostats, des interrupteurs qui transmettent des données personnelles. La même technique est utilisée dans les entreprises pour espionner le personnel.

Lorsque de telles pratiques sont révélées, la stratégie réactive des sociétés numériques est toujours déclinée en quatre étapes : incursion, accoutumance, adaptation, redirection.

— 1. L'incursion consiste à s'introduire partout où c'est possible pour extraire des données nouvelles. Par exemple, l'opération *Street View* de *Google Maps* a permis, en envoyant circuler des voitures équipées de capteurs, de collecter secrètement des données personnelles depuis les réseaux privés Wifi. Ainsi, des mots de passe, des noms, des numéros de téléphone, des informations bancaires, des e-mails, des informations médicales, des photos, etc. étaient glanés à l'insu des riverains.
— 2. L'accoutumance vise à vaincre la résistance que ne manque pas de susciter la révélation des incursions. On gagne du temps grâce aux services d'une armée d'avocats dont le travail consiste à faire trainer la communication de documents à la justice, à multiplier les manœuvres dilatoires, à exploiter les moindres failles de la loi, puis, en dernier recours, à passer un accord pour payer une amende réduite. Pendant ce temps, on développe le site incriminé pour accoutumer les utilisateurs à s'en servir, au point qu'il leur paraît indispensable.
— 3. L'adaptation consiste à faire semblant de reconnaître ses torts, à faire amende honorable, à promettre des remèdes, à déplacer quelques cadres désignés comme responsables de l'erreur, à faire quelques concessions aux décisions judiciaires (comme le floutage des visages sur les photos de rues), mais sans renoncer à la quête de données.
— 4. Enfin, la redirection permet de reprendre l'incursion en proposant ce qui apparaîtra comme un nouveau service, par exemple en faisant passer *Google Maps* pour une entreprise de cartographie du monde avec tous ses milieux naturels (sentiers de randonnée, étangs, parcs) et les services utiles (lignes

de ferry, autoroutes, etc.). En 2011, Google franchit la frontière entre l'extérieur et l'intérieur en géolocalisation les gens à l'intérieur des aéroports, centres commerciaux, hôtels, restaurants. On peut alors vendre des visites virtuelles qui acheminent les clients vers tel ou tel lieu de consommation.

2. Leur exploitation pour concevoir des prédictions de comportements

Que fait-on de toutes ces données ? Éric Schmidt, un cadre de Google déclara à Davos qu'Internet allait disparaître, non au sens d'être anéanti, mais au sens où le réseau allait se fondre complètement dans le paysage quotidien grâce aux objets connectés. Des architectures informatiques vont être implantées partout dans le monde réel. Cette invention provient d'une technique de l'éthologie : la télémétrie consiste à poser un émetteur miniature d'un signal radio sur un animal pour le suivre à distance. Appliquée aux hommes détenteurs d'un téléphone mobile, cette technique permet de suivre les migrations de troupeaux humains. La mise sur le marché d'objets connectés permet de multiplier les capteurs, l'essentiel ensuite étant de structurer les données de façon à pouvoir les exploiter.

Par exemple, les compagnies d'assurance attendent des données très précises sur la conduite au volant de leurs assurés, de façon à contrôler leur comportement en temps réel, en allant même jusqu'à bloquer le démarrage du véhicule si nécessaire. On pourra ainsi punir le conducteur en augmentant ses primes, ou le récompenser avec des bons points. Même chose pour les assurances médicales qui pourront contrôler le respect d'un régime alimentaire ou d'un traitement médical par les assurés. Les assureurs ne se contentent pas des contrats signés par les assurés car les contrats supposent de leur faire confiance, ce qui ne donne aucune certitude. Les assureurs veulent éliminer la part de risque inhérente à leur activité. Aussi réclament-ils des programmes qui décideraient automatiquement de sanctionner les mauvais conducteurs, avant toute perte pour eux. Ils instaurent la notion de « décontrat », non pas au sens d'annulation de contrat, mais au sens de suppression des relations contractuelles et de leur remplacement par l'exécution unilatérale de « décisions » automatiques.

La gestion des flux automobiles démontre comment on arrive déjà à orienter les comportements par des « décisions » automatiques (ralentissements, filtrages, déviations, etc.). La gestion automatisée du parc de stationnement d'une ville permet de faire tourner les places, non pour faciliter le service mais pour obtenir le meilleur rendement pour la société gestionnaire. Elle peut aussi pousser les automobilistes à « préférer » le service d'un véhicule Uber, plutôt que d'attendre le passage d'un bus. Toutes ces techniques d'orientation des comportements ont été rendues possibles par la maîtrise en temps réel de multiples données géolocalisées.

Les objets connectés introduits dans les maisons, comme les thermostats ou les aspirateurs robots, élargissent la collecte à l'intérieur même des maisons. Les aspirateurs permettent de cartographier avec précision toutes les pièces, et si l'acheteur refuse de livrer ses données, il est privé de la plupart des fonctionnalités de l'appareil. Les matelas connectés analysent votre sommeil : rythme cardiaque, respiration, horaire et durée du sommeil, positions du corps, etc. Reliés au téléphone, ils déclenchent des applications pour le sport, le régime alimentaire. C'est tout le corps qui est connecté.

Certains se consolent en se disant que toutes ces données mélangées fournissent des statistiques anonymes, ce qui ne remettrait pas en cause leur vie privée, mais c'est oublier qu'il suffit « de trois petits bouts de données extraites des registres publics – date de naissance, code postal et sexe – pour désanonymer des métadonnées avec une « troublante facilité », par des techniques de ré-identification. » Grâce à des profils, on peut agir non pas sur des ensembles à partir de prédictions statistiques, mais véritablement sur des personnes.

On en arrive maintenant à explorer les émotions et des aspects profonds de la personne, grâce à des modèles psychologiques de personnalité. La collecte a commencé avec des applications sur Facebook permettant à l'utilisateur d'effectuer des tests psychométriques. Ce qui est présenté comme un aimable jeu avec soi-même a permis de dresser des profils de référence pour l'analyse de grandes populations. En croisant les données de tests de personnalité et les réseaux d' « amitié » de Facebook, on a pu restituer

entre 50 et 87 millions de profils psychologiques sur la population américaine.

Cette première expérience a inspiré ensuite le cabinet Cambridge Analytica pour mener une attaque de micro-ciblage comportemental à des fins politiques. Les modèles se sont affinés dans un intense aller et retour entre profils et analyse des données. Ainsi, pour évaluer un comportement, il est possible d'analyser les échanges de messages, en faisant abstraction de leurs contenus, car ce qui est révélateur, c'est plus le « comment » que le « quoi » : la longueur et la complexité des phrases plus que les mots, le partage ou le refus de partage d'images plus que les images elles-mêmes, la façon de donner rendez-vous plus que le rendez-vous, etc. Ainsi les utilisateurs se livrent-ils complètement sans le savoir. Cambridge Analytica possède entre 4000 et 5000 points de données sur chaque américain adulte. Il ainsi possible de repérer à l'avance des individus susceptibles de changer de marque de vêtement ou d'opinion politique. De telles prédictions poussent les publicitaires qui en sont informés à envoyer des messages agressifs pour retenir le client ou pour le capter.

En 2015, une petite société (Realeyes) a mis au point une technologie de lecture des émotions d'un individu qui regarde un programme vidéo afin d'améliorer l'efficacité des publicités. On arrive donc à déceler des manifestations de l'inconscient psychique. Plus les gens sont émus, plus ils dépensent. S'ouvre alors un nouveau domaine, « l'informatique affective », développée par Rosalind Picard. Il s'agit de restituer les émotions conscientes et inconscientes sous la forme d'un comportement codable et calculable. La finalité était au départ, comme toujours, bienveillante : aider un étudiant à préparer un entretien d'embauche, aider les enfants autistes à développer leurs aptitudes, former les joueurs pour qu'ils contrôlent l'expression de leurs émotions, etc. Au bout de trois ans, R. Picard fut remerciée et le projet fut entièrement réorienté vers la publicité ciblée et « personnalisée ».

3. La construction d'un pouvoir instrumentalisant

Après la collecte des données, puis leur transformation en prédictions de comportements, il reste à agir sur l'utilisateur. Comment ? En recourant à des ressorts bien connus de la psychologie comportementale. Par exemple, pour inciter les étudiant à manger des fruits de préférence à des pâtisseries, le responsable d'un resto U présentera les fruits devant les pâtisseries. On peut aussi pousser à une décision en rendant difficiles ou impossibles les autres choix alternatifs. Le mimétisme est également un ressort très puissant. En 2012, aux États-Unis, pour pousser des électeurs à aller voter, on a manipulé 61 millions d'utilisateurs de Facebook : à côté d'un message encourageant le vote, était disposé un bouton « j'ai voté », avec un compteur du nombre d'utilisateurs qui l'avaient cliqué ; apparaissaient aussi des photos d'amis qui avaient déclaré avoir voté. On obtint ainsi 340000 votants supplémentaires. Plusieurs expériences de ce type ont été menées avec des messages subliminaux.

Une des expériences les plus étonnantes eut lieu en 2016 avec le jeu Pokémon. Il s'agit d'une chasse au trésor virtuelle dans le monde réel. Une appli sur téléphone articulée avec le GPS et la caméra permet de chasser des créatures virtuelles, les Pokémon. Celles-ci apparaissent sur l'écran et leur capture est récompensée par des points. L'objectif est de capturer la série des 151 Pokémon. On a alors vu de véritables hordes de chasseurs envahir des rues, des jardins privés, des monuments. L'objectif pour les clients (pas pour les joueurs) était double : extraire des données nouvelles pour la cartographie de lieux extérieurs et intérieurs, publics et privés, et amener un flux de clients vers des pizzerias, des drugstores, des magasins dont les patrons avaient acheté des parts de visiteurs. Le jeu n'était qu'un leurre habile pour former un troupeau humain malléable, l'ignorance de l'utilisateur étant la condition première de réussite de cette entreprise.

S. Zuboff considère que le capitalisme de surveillance met en place un pouvoir « instrumentarien », à savoir « l'instrumentation et l'instrumentalisation du comportement à des fins de modification, de prédiction, de monétisation et de contrôle. » Peut-on dire qu'il s'agit d'un nouveau totalitarisme ? Les capitalistes de surveillance ne cherchent pas à éliminer des groupes ethniques, ni à réformer l'âme d'un peuple, alors que le totalitarisme nazi ou stalinien est d'abord politique ; il use de la violence et cherche à transformer les intentions des individus. Le pouvoir instrumentarien est avant tout un projet commercial,

indifférent à ce que pensent les hommes, et il n'use pas de violence physique.

Selon S. Zuboff, son inspiration vient essentiellement de la théorie comportementaliste de B. Skinner. Celui-ci a d'abord étudié le comportement animal (sur des pigeons, des rats) pour mettre au point des procédés permettant de changer les comportements et de construire des comportements artificiels. Puis, il a transposé ses recherches sur l'homme en partant du principe (posé par Watson en 1913) qu'il n'y a pas de différence fondamentale entre l'homme et l'animal. L'être humain doit être étudié ni plus ni moins comme un organisme. Sa liberté n'est qu'un leurre. Elle n'est « que l'ignorance qui attend son conquérant ». Skinner prône un behaviorisme radical, c'est-à-dire qui doit être l'étude d'une action dénuée de toute attribution subjective. Tout comportement peut être réduit à un schéma mettant en évidence des relations causales entre l'environnement et le comportement. Grâce à certaines technologies, on pourrait prédire et modeler avec efficacité le comportement humain, comme la physique et la biologie ont pu changer le monde.

Pour les behavioristes, la démocratie ne saurait constituer une solution, car elle ne fait que perpétuer l'illusion de la liberté. La bonne solution est une technique qui dépasse l'usage de la force et qui rejette le besoin de dominer l'âme humaine. Il faut développer une technologie comportementale puissante et précise, un outil universel de modification des comportements. Le capitalisme de surveillance réalise cette technologie. Il ne promeut aucun régime politique, aucune religion, aucune morale : le seul péché, c'est l'autonomie de l'individu, l'audace de faire obstruction à la collecte de ses données personnelles. Cette liberté est confisquée par les clients du numérique, sous l'impératif de la certitude. Même les gouvernements « exigent les machines à certitude qui promettent des moyens fiables de détection et de prédiction et même l'actuation automatique de contre-mesures. »

Le système chinois du crédit social est le plus avancé dans la collecte et l'exploitation des données à des fins de contrôle des individus et des entreprises. C'est l'apothéose du pouvoir instrumentarien. Le plus scandaleux, selon S. Zuboff, ce n'est pas le totalitarisme chinois, mais c'est que ce modèle ouvre la voie à des chemins similaires dans la Silicon Valley. La seule différence est dans la finalité ultime : pour la Chine, le contrôle de l'État ; pour la Silicon Valley, le profit commercial. « L'instrumentarisme recherche la totalité comme domination de marché et compte pour libérer la voie sur son contrôle de la division du savoir dans la société, rendue possible et assurée par Big Other. »

Le capitalisme de surveillance enserre les utilisateurs dans un esprit de ruche où tous les mouvements sont préalablement définis, gérés en harmonie, opérés à l'unisson en convergence vers l'efficacité maximale. Par exemple, on peut organiser un chantier à partir de la qualification de chaque employé ; si un employé non qualifié pour manier un marteau-piqueur s'en approche et le prend, un signal d'alerte retentit et l'outil se désactive automatiquement. Grâce à l'intelligence artificielle, « on peut fouiller le monde réel à la recherche de gens, d'objets et d'activités et leur appliquer des règlements. » Les lieux de travail sont conçus comme les laboratoires de Skinner pour les rats et les pigeons. On obtient des comportements calibrés, sûrs, harmonieux, sans résistance possible. L'esprit de ruche permet d'éliminer tous les éléments de chaos et de garantir les résultats fixés par le plan.

Dès que quelqu'un tombe malade, il reçoit automatiquement un rendez-vous médical ; le bus passe au moment où il arrive à l'arrêt ; chez son médecin, son dossier s'affiche tout de suite sur l'ordinateur, etc. Tout peut être prévu et organisé de telle sorte qu'il ne se produise aucune friction. En réalité, ce fonctionnement profite moins à la population qu'aux quelques-uns qui en tirent profit. Les considérations individuelles, comme le questionnement moral ou les repères politiques, sont écartées parce qu'elles font perdre du temps et qu'elles détournent de la convergence des comportements. Une nouvelle classe dominante apparaît, celle des ajusteurs de comportement, pour produire les comportements les plus efficaces du point de vue du collectif, au-delà des libertés individuelles.

Des psychologues ont longuement travaillé sur la conception des machines à sous pour les casinos de Las Vegas, de façon à ce que le joueur, en s'oubliant lui-même, soit pris dans une zone telle qu'il ne puisse plus se détourner du jeu, comme une main est prise dans un gant. Facebook applique les mêmes principes de l'addiction technologique ; il est conçu comme un média dont les utilisateurs n'éprouvent jamais le

besoin de détourner le regard. Il engloutit en masse le temps et la conscience de ses utilisateurs. Le réseau Facebook est un agencement de millions de miroirs, chaque « like » actionné donnant un nouveau détail sur la main, ce qui permet d'ajuster davantage le gant et de prédire ce que va faire l'utilisateur. L'utilisation se déroule comme une boucle de rétroaction de plus en plus courte et serrée. Il n'y a plus de refuge possible, plus de recoin, plus aucun sanctuaire dans lequel on pourrait échapper au pouvoir totalisant. La question « Mais qu'avez-vous donc à cacher ? » est posée pour déstabiliser l'utilisateur par un sentiment de culpabilité. Mais, en réalité, si l'on n'a rien à cacher, c'est que l'on n'a plus de vie privée, c'est que l'on n'est plus rien à ses propres yeux.

La règlementation européenne (RGPD) a pu nous redonner un espoir, mais ceux qui ont voulu se battre pour faire appliquer ses préconisations n'y sont pas parvenus, tant les obstacles sont considérables. Facebook refuse absolument, au nom du secret industriel, de donner le « texte fantôme » élaboré à partir des données personnelles. Par un subterfuge sur ses conditions d'utilisation, Facebook a fait passer en 2018 les données personnelles sous le coup des lois américaines, pour échapper à la règlementation européenne. Il faudrait une organisation collective des utilisateurs pour mener le combat.

4. Les rapports du capitalisme aux nouvelles technologies

Une question complexe se pose : comment s'articulent le capitalisme et les technologies ? Sans la traiter spécifiquement, S. Zuboff fournit quelques éléments de réponse. Son expression « capitalisme de surveillance » est discutable, car la surveillance n'est encore qu'un moyen en vue d'une autre fin : tirer profit des données personnelles. L'expression « capitalisme des données » aurait été plus adéquat et, en même temps, plus ironique avec l'équivocité du mot « données ».

Le capitalisme numérique s'est arrogé le droit de décider, à la place de l'individu, de ce qui resterait privé et de ce qui serait rendu public. Cette décision prise par les dirigeants de Google n'est pas un accident malheureux, ni une erreur occasionnelle, ni une nécessité économique, ni une conséquence nécessaire du développement technologique, mais bien un choix humain pour convertir des données gratuites en revenu. La décision d'investir dans le numérique consiste à saisir une bonne occasion, au bon moment, et à chercher tous les moyens de récupérer un retour sur investissement, rapide et maximal, sans aucun scrupule éthique.

On doit distinguer deux savoirs correspondant à deux textes numériques : 1. Le texte familier connu des utilisateurs et le texte fantôme connu des seuls usagers (les « *data scientists* »). Le paradoxe est que le texte fantôme en sait plus sur nous-mêmes que ce que nous pouvons connaître de nous-mêmes. On a formé un nouveau clergé qui sait ce que les autres ne savent pas. Quand une personne est harcelée sur Internet, elle sait qu'elle est harcelée ; mais quand on produit des informations sur elle sans qu'elle le sache, on franchit la limite du droit démocratique. Le capitalisme de surveillance est anti-démocratique, mais son pouvoir ne provient ni de l'État, ni de la seule technologie, ni de mauvaises intentions de certains. « Ce sont les conséquences d'une logique d'accumulation réussie. » La guerre de l'information tourne le dos à la démocratie. Trois questions se posent : Qui sait ? Qui décide ? Qui décide qui décide ? « Dans l'état actuel des choses, ce sont les entreprises capitalistes de surveillance qui savent. C'est la forme du marché qui décide. C'est la lutte concurrentielle entre les capitalistes de surveillance qui décide qui décide. » L'informaticien employé par les sociétés du numérique en est réduit à quelques questions de conscience morale : « Qu'ai-je réellement fait ? Quels sont l'application et l'usage ultimes des fruits de mon travail ? […] Suis-je satisfait d'avoir contribué à cet usage ? Ou bien mort de honte ? » Mais son employeur n'en a que faire.

Le capitalisme de surveillance introduit trois nouveautés par rapport aux formes antérieures du capitalisme : 1. Il affirme pour le capitaliste une liberté et un savoir illimités sur les individus ; 2. Il rompt avec toute idée de contrat et de réciprocité ; 3. Il construit une vision collectiviste nourrie par l'indifférence radicale sur le modèle de la ruche.

Ses profits sont énormes, avec très peu de masse salariale. En 2016, Google valait 532 milliards de dollars

avec seulement 75000 emplois, Facebook 332 milliards avec 18000 emplois, alors que General Motors a péniblement atteint, en 1965, 225 milliards avec 735000 emplois. Les entreprises du numérique réduisent au maximum le lien avec l'emploi, et, en conséquence, sont complètement indifférentes aux enjeux politiques de la société, aux conséquences sociales de leurs innovations.

Ce qui leur importe, c'est d'obtenir des produits qui attirent tout le monde, quelle qu'en soit la qualité éthique. C'est pourquoi la désinformation, les discours de haine, les escroqueries circulent sur les réseaux sociaux, tant que cela contribue au flux des utilisateurs. La prétendue « modération des contenus » n'est utilisée qu'en cas de menace de réduction du flux, non par un quelconque sens des responsabilités. Elle est sous-traitée auprès d'une main d'œuvre de plus de 100000 employés, qui ont pour consigne de ne pas effarer les utilisateurs. Des outils existent pour éliminer les *Fake news*, mais puisqu'elles attirent les utilisateurs, il ne faut pas les dépublier. Le sensationnalisme fait grimper le nombre de clics. « Tant que les tuyaux coulent à flots, peu importe ce qu'ils charrient. »

5. Le projet politique de l'Internet

Les sociétés du numérique se défendent de tout parti pris politique, au sens où elles ne sont ni de gauche, ni de droite, mais elles imposent bien un projet politique fondamental dans la formation d'une société sur le modèle de la ruche. « La société idéale de Google est une population d'utilisateurs distants et non de citoyens. Google idéalise les gens qui sont informés, mais seulement par les moyens que l'entreprise choisit. Ce qui signifie que nous devons être dociles, harmonieux et, par-dessus tout, reconnaissants. » En 2017, aux USA, un débat opposa le parti républicain, opposé à la réglementation restreignant l'emprise des sociétés numériques sur les données personnelles, et le parti démocrate considérant que ces données étaient la propriété de l'utilisateur. Le parti républicain l'a emporté. Cette dépossession des utilisateurs repose sur cinq prétentions du capitalisme de surveillance : 1. Il revendique la possession des données personnelles. 2. Il affirme le droit de les convertir en données comportementales. 3. Il revendique la propriété de ces dernières. 4. Il revendique le droit de savoir ce que révèlent ces prédictions comportementales. 5. Il s'arroge le droit de décider d'en faire ce qu'il veut. Il impose les conditions de tous ces droits.

Le capitalisme de surveillance vise à éliminer le plus possible tous les éléments d'incertitude sur le marché. Par exemple, au lieu d'envoyer un huissier pour procéder à une saisie de biens chez un vieux couple endetté, on préfère pratiquer le « décontrat », à savoir la « décision » automatique imposé par un logiciel sans aucun recours possible, car l'huissier demeure après tout un être humain sensible qui pourrait freiner la récupération de la dette. La confiance est d'emblée éliminée et remplacée par l'a priori de la méfiance ; la vie sociale est transformée en mécanique numérisée. Le sujet est dépourvu de projet et est réduit à l'état d'objet connecté, sans retrait possible, sans résistance, sans protection de ses droits.

Le capitalisme de surveillance est une force antidémocratique qui a réussi un coup d'État, non contre l'État lui-même, mais contre le peuple. C'est une forme de tyrannie qui se nourrit du peuple sans en émaner. Son but n'est pas la domination de la nature, mais la domination de la nature humaine. Certains d'entre nous resteront des sujets, tandis que tous les autres ne seront que des objets ; certains sont des stimuli, et la plupart ne sont que des réactions. La loi du marché des données n'est plus compatible avec la démocratie. Est-il juste de retirer à chacun d'entre nous la souveraineté sur sa propre vie ?

Jean-Marie Nicolle, le 1er mars 2021.