Les données à caractère personnel, carburant du capitalisme de surveillance

François Pellegrini, Elia Verdon

Les données à caractère personnel, carburant du capitalisme de surveillance

François Pellegrini, professeur d'informatique à l'université de Bordeaux, chercheur au LaBRI et à Inria Bordeaux Sud-Ouest (francois.pellegrini@u-bordeaux.fr)

Elia Verdon, doctorante contractuelle en droit public (CERCCLE) et en informatique (LaBRI), université de Bordeaux (elia.verdon@u-bordeaux.fr)

Résumé :
Le financement des services numériques par la monétisation indirecte conduit à une collecte globale et massive de données à caractère personnel, visant à mieux cibler les personnes pour mieux les servir et conserver leur clientèle. La pensée solutionniste encourage les organisations, tant privées que publiques, à agréger des données, y compris des données sensibles telles que les données de santé, dans des systèmes d'information censés produire des connaissances utiles à la résolution de crises ou de problèmes sociaux. Cependant, ces données sont aussi susceptibles d'être utilisées pour influencer le comportement individuel des personnes et, à plus grande échelle, le fonctionnement global des sociétés humaines.
L'Union européenne a entrepris de réguler l'usage des données à caractère personnel par une succession de textes, dont le RGPD, rapidement devenu un standard mondial. Les opérateurs privés sont cependant en charge de pans entiers de la régulation effective des contenus, pouvant conduire à des censures plus ou moins détectables. Une voie possible serait de considérer les réseaux sociaux comme des infrastructures, administrées comme des communs.

L'émergence des réseaux numériques, en mettant directement en relation de façon instantanée les fournisseurs de services et leurs usagers, a permis l'apparition d'un nouveau modèle économique : l'économie de l'attention. La surabondance de l'information, au sein de services prétendument gratuits mis à disposition sur les réseaux numériques, transforme l'attention des utilisateurs en une ressource rare (Simon, 1971).

La fourniture aux personnes – sans contrepartie apparente – d'informations et de services numériques implique que ces plates-formes soient rémunérées de façon indirecte, notamment par la présentation de publicités. *« Si le service est gratuit, c'est que vous êtes le produit »* dit l'adage. La captation de l'attention des usagers, devenue particulièrement lucrative, fait l'objet d'une bataille féroce entre les opérateurs de plates-formes numériques concurrentes pour notre « temps de cerveau disponible ». Chacune cherche à utiliser à son profit nos ressorts intimes et nos biais cognitifs afin de susciter notre envie d'informations nouvelles, nous soumettant à un déluge informationnel, voire à une « apocalypse cognitive » (Bronner, 2021).

Les véritables clients de ce marché sont les entreprises qui achètent des « impressions », c'est-à-dire le placement de leurs publicités devant les yeux de consommateurs susceptibles d'être influencés par elles. La performance de ce modèle économique dépend donc à la fois du nombre d'usagers

réguliers et de la qualité de leur ciblage : les usagers sont groupés, par affinités, en segments de marchés qui peuvent être combinés pour sélectionner des profils précis.

Le recrutement de nouveaux usagers s'appuie massivement sur l'effet de réseau : les personnes s'agrègent préférentiellement au réseau leur proposant le plus grand nombre de contacts, accroissant l'« attraction gravitationnelle » des acteurs déjà dominants et aggravant l'asymétrie informationnelle entre usagers et opérateurs de ces services. L'affinage des profils conduit pour sa part les multiples acteurs de cet écosystème (annonceurs, régies publicitaires, courtiers et agrégateurs de données d'usagers, bourses d'enchères en temps réel pour le placement d'impressions, sites rémunérés) à collecter de plus en plus de données sur l'activité des internautes.

Un « solutionnisme technologique » impulsé par des alliances privé-public

Le capitalisme de surveillance constitue le parachèvement de cette dynamique. Il vise à prédire et influencer le comportement des personnes de façon systématique, dans l'intérêt des entités mettant en œuvre les techniques de captation de l'attention. L'expérience humaine des utilisateurs de ces plates-formes, matière première et source de surplus de ce capitalisme informationnel, fait l'objet d'une extraction méthodique mobilisant les technologies les plus avancées (Zuboff, 2020). S'affranchissant des contraintes liées au déplacement de la matière, ces entreprises sont à même de collecter et d'agréger des masses considérables d'informations en tout point du globe, conduisant à une concentration du capital informationnel bien plus importante que celle du capital industriel lors du millénaire précédent.

La surveillance effectuée par les entreprises commerciales ne laisse pas indifférents les acteurs publics : la collecte massive de données de localisation et de comportement par les grandes sociétés privées, alors que cette collecte est généralement interdite aux gouvernements, place ces derniers en situation de dépendance lorsque des circonstances particulières semblent nécessiter le recours à de telles données, par exemple dans le cadre d'enquêtes criminelles ou pour la gestion de catastrophes naturelles. Le capitalisme de surveillance induit donc par nature une dynamique de collaboration entre intérêts privés et publics pour le contrôle des populations (Mattelart et Vitalis, 2014).

Le scandale « Cambridge Analytica » illustre pleinement l'utilisation des outils de surveillance commerciale à des fins étatiques. Le détournement de données de profilage issues de Facebook dans le but d'influer sur l'élection présidentielle étasunienne de 2016 et le référendum du Brexit de la même année, ainsi que l'utilisation de « fermes à trolls »[1] pour inonder les réseaux numériques d'informations clivantes lors de mouvements sociaux tels que Black Lives Matter ou les Gilets Jaunes, ont mis en évidence la fragilité de nos sociétés hyperconnectées face à ces influences. Elles démontrent la perméabilité de nos cerveaux face aux techniques manipulatoires exploitant nos mécanismes cognitifs (addiction aux jeux à récompense aléatoire, biais de jugement, etc.).

La généralisation de la pensée technicienne (Ellul, 1977) a conduit à considérer le fonctionnement des sociétés comme un ensemble de problèmes organisationnels et techniques à résoudre. Face au « manque d'agilité » supposé du secteur public, nombre de sociétés privées, voire d'individus, s'attachent à concevoir et déployer des solutions techniques permettant de gérer des situations particulières ou de crise. Cela a notamment été le cas lors de la pandémie de Covid-19, avec par

[1] Une « ferme à troll » est une entité, privée ou au service d'un État, chargée d'initier et/ou d'amplifier des campagnes de propagande, en produisant et/ou relayant des messages sur les réseaux sociaux, au moyen de multiples comptes créés sous des identités factices.

exemple la mise en œuvre de l'outil d'aide à la prise de rendez-vous de vaccination ViteMaDose, développé par un particulier, ou de la solution de suivi de contacts créée par Apple et Google, concurrente de celles proposées par certains États. Pour mettre en œuvre un suivi de contacts au sein de sa population lors de la pandémie, le gouvernement de la Corée du Sud a pour sa part organisé le croisement de données issues de multiples sources privées, telles que les relevés de cartes bancaires.

La promotion de ce solutionnisme technologique (Morozov, 2014) conduit à considérer les technologies numériques, parées des vertus de la neutralité objective, comme le remède à toutes les crises et la solution universelle aux divers maux de la société. Qui plus est, ces actions ne sont généralement pas sans contreparties : elles augmentent la dépendance des États vis-à-vis des grands acteurs privés qui souhaitent, sinon se substituer à eux, du moins les contrôler afin qu'ils ne s'opposent pas au développement de leurs marchés.

Les grandes entreprises du numérique possèdent des infrastructures de stockage et de calcul dont peu d'États disposent, ou alors à une bien moindre échelle (à part peut-être aux États-Unis pour la NSA, qui dispose de centres de données – *datacenters* – considérables dans l'Utah). Les tentatives pour faire émerger des « *clouds* souverains » en Europe ont pour le moment conduit à des impasses, les investissements et projets ayant été à chaque fois subvertis[2], et les prix très (trop ?) bas proposés par les entreprises étasuniennes rendant ces alternatives peu attractives. Pourtant, la nécessité d'infrastructures souveraines se fait encore plus criante au vu des mesures de censure que les entreprises étasuniennes peuvent mettre en œuvre concernant l'usage de leurs technologies, comme c'est actuellement le cas vis-à-vis des pays hostiles à l'Occident tels que la Corée du Nord, l'Iran et maintenant la Russie. Ces mesures, prises spontanément[3] ou à la demande de leur gouvernement, illustrent de façon flagrante la dépendance des États aux technologies qu'ils ne maîtrisent pas.

Comme Edward Snowden l'a révélé en 2013, les agences de renseignement étatiques bénéficient largement des masses de données collectées par les acteurs privés, soit en les moissonnant sur les plateformes en libre consultation (« *web scraping* »), soit en s'abreuvant directement auprès des serveurs de données, en collaboration ou non avec ces acteurs (notamment en siphonnant les données en transit entre les différents sites des entreprises).

Le couplage des outils de surveillance étatiques avec les données issues du privé permet une surveillance généralisée des populations. Celle-ci atteint son paroxysme avec la notion de « crédit social » telle qu'expérimentée dans certaines villes de Chine : le comportement des personnes, analysé en ligne ou par des caméras placées sur la voie publique, conduit à leur accorder des privilèges ou à leur retirer des marges de manœuvre, en termes d'accès à des services ou à des déplacements (seules les personnes disposant d'un score suffisamment élevé ayant le droit d'effectuer des déplacements de longue distance). Ce modèle de société est souvent présenté comme dystopique, mais des traitements opérés par le secteur privé pourraient tout autant induire des effets identiques en termes de contrôle social, comme lorsque, par l'étude du graphe social[4]

[2] En France, 150 millions d'euros d'argent public ont été dépensés pour financer deux solutions concurrentes, Cloudwatt et Numergy, portées par de grands groupes nationaux, sans résultat autre qu'une concurrence déloyale vis-à-vis d'un champion national existant, OVH. Le consortium de « *cloud* » européen Gaia-X, pour sa part, a très vite accueilli en son sein les plus gros industriels étasuniens du secteur, perdant par là-même toute velléité de souveraineté.

[3] On peut citer le cas de l'entreprise MongoDB qui, de son propre chef, a résilié tous ses contrats de fourniture de services en cours avec des clients situés en Russie et en Biélorussie.

[4] Le « graphe social » d'une personne décrit l'ensemble des personnes avec qui elle est en contact, ainsi que leurs interactions mutuelles. Aux États-Unis, il est utilisé pour déterminer le niveau social d'une personne indépendamment de ses dires, en se basant sur le niveau social de ses relations.

d’une personne, une banque déciderait ou non de lui accorder un crédit. Il en va de même dans le domaine assurantiel, par exemple avec les dispositifs destinés à offrir des bonus d’assurance automobile aux conducteurs ne conduisant pas de façon nerveuse (« *pay how you drive* »).

La manne des données de santé

Le secteur de la santé est identifié par de nombreux acteurs, tant publics que privés, comme un domaine dans lequel la collecte et le traitement massifs des données à caractère personnel sont censés leur apporter des bénéfices considérables. Notamment, la découverte de corrélations entre différents jeux de données issues des patients (données biologiques – y compris génétiques –, historique des traitements et des prises médicamenteuses, parcours de soins, etc.) serait susceptible d’apporter des connaissances nouvelles en termes de pharmacovigilance[5], d’évaluation de l’efficacité des pratiques médicales, de détection des signes avant-coureurs des maladies, etc. De là découle la volonté de centraliser les flots des données médicales issues du système de santé, au sein d’entrepôts et de centres de données dédiés, comme en France la « Plateforme de données de santé » (PDS), aussi appelée « Health Data Hub ».

L’existence de telles infrastructures pose de nombreuses questions. Une première concerne la sécurité des données : bien que la protection d’un équipement unique soit réputée plus facile à assurer que celle d’entrepôts hétérogènes et dispersés, la valeur d’un stock de données concentrées est bien plus grande et susceptible de bien plus de convoitises. Une deuxième concerne les enjeux de souveraineté : le recours à des technologies et fournisseurs étrangers peut être vu tant comme un risque de perte de compétences industrielles des entreprises locales, que comme une menace accrue d’accès par des acteurs de renseignement étrangers aux informations intimes de dirigeants et autres personnes d’intérêt.

L’usage de telles infrastructures peut également conduire à s’interroger sur la répartition de la valeur des connaissances extraites des données émanant des personnes. S’agit-il de prévenir ces personnes contre un risque direct pour elles (pharmacovigilance, signes avant-coureurs de maladies graves – pour autant qu’elles souhaitent en être informées) ? S’agit-il d’améliorer les pratiques médicales, en déterminant celles qui fonctionnent le mieux, ou d’encadrer la pratique des médecins ? S’agit-il pour un laboratoire de « repositionner » un médicament sur un nouvel usage, source de revenus accrus ? S’agit-il pour une compagnie d’assurances d’établir des profils de santé plus ciblés et des grilles tarifaires adaptées, conduisant à démutualiser le risque assurantiel et à faire peser une charge plus lourde sur les personnes en fonction de leur comportement, voire de leur hérédité ? Ces données pourraient-elles faire l’objet de réquisitions judiciaires, afin d’infirmer ou de confirmer une filiation ou un mobile de crime ?

Parce que les risques d’utilisations abusives de tels outils sont considérables, de nombreux garde-fous juridiques ont été mis en place pour garantir le secret médical, ou encore évaluer, par des comités d’éthique, des projets de recherche soumis.

Les tentatives de régulation de l’Union européenne

La situation d’asymétrie informationnelle majeure dans laquelle sont placées les personnes qui communiquent leurs données à de grandes entreprises du numérique dotées de capacité de surveillance étendues, laisse peu d’espoir à la préservation de l’intimité. Les marges de manœuvre

[5] Ce terme désigne les activités visant à détecter les effets secondaires, parfois de long terme (par exemple, le Médiator®), voire transgénérationnels (tels que ceux du Distilbène®), induits par l’usage des médicaments.

individuelles sont faibles : si certains revendiquent un droit à la déconnexion, celui-ci conduit à les priver des bénéfices des effets de réseau, en termes d'opportunités de rencontres et donc, notamment, de carrière. La rivalité du temps d'attention limite la présence sur plus de quelques réseaux sociaux, et incite à la grégarité. S'il est inopérant de partir seul d'un réseau social, en revanche, des phénomènes de « départ en vague » peuvent se produire. C'est ainsi que, lorsque le réseau social WhatsApp a entrepris de modifier ses conditions générales d'utilisation[6] (CGU) en 2021, des millions d'utilisateurs ont déserté ce réseau pour s'inscrire rapidement sur le réseau concurrent Signal (ce à quoi ce dernier ne s'attendait pas, cette arrivée massive conduisant à surcharger temporairement son infrastructure). Cependant, ces actions ne constituent pas une protection pérenne, chaque opérateur de plate-forme pouvant modifier ses CGU et devenir intrusif à son tour, une fois une clientèle suffisante captée. Les personnes ne peuvent être laissées seules face à des acteurs en position oligopolistique.

Parce que les individus ne sont généralement pas en position de force vis-à-vis des responsables du traitement de leurs données à caractère personnel, qu'ils soient publics ou privés, il revient à la loi de les protéger. À la suite de l'informatisation des administrations centrales dans les années 1970, et face aux risques que ces nouveaux outils pouvaient faire peser sur les personnes, les premières lois relatives à la protection des données à caractère personnel ont été élaborées en Europe. En France, ce processus a été initié suite à la divulgation dans la presse du projet « SAFARI »[7] visant à interconnecter tous les fichiers administratifs autour d'un identifiant unique des personnes (le NIR). En réaction à la crise politique provoquée par ce projet, considéré comme un fichage abusif des citoyens, la loi « Informatique et Libertés » a été votée le 6 janvier 1978. Cette loi définit un cadre protecteur pour les données des personnes, et crée l'autorité administrative indépendante chargée de la faire respecter : la Commission nationale de l'informatique et des libertés (CNIL). Plusieurs pays d'Europe sont allés dans le même sens, jusqu'à ce qu'une directive européenne de 1995 tente d'harmoniser les différents droits nationaux en la matière. Cette directive a également consacré le principe de libre circulation des données, dans le but de favoriser l'émergence d'un marché numérique mondialisé, auquel certaines législations nationales auraient pu porter atteinte. Le droit des données à caractère personnel a fait dès lors partie de « l'acquis communautaire ». Avec le développement de l'économie numérique, le périmètre des lois « Informatique et Libertés », visant initialement à protéger les personnes contre le fichage abusif par les administrations a été étendu, au début des années 2000, afin que les autorités de protection des données puissent également sanctionner les acteurs du secteur privé.

Le règlement européen général sur la protection des données à caractère personnel (RGPD), entré en vigueur en mai 2018, représente une avancée majeure pour la protection des résidents de l'Union européenne (UE). Alors que les lois nationales et la directive européenne de 1995 ne permettaient pas de sanctionner les fournisseurs de services numériques établis hors du territoire de l'UE, le RGPD offre à présent cette possibilité. Cet effet « extraterritorial », novateur dans le domaine des données à caractère personnel, ne constitue cependant pas une nouveauté conceptuelle en droit de l'UE. En effet, tout producteur de biens physiques souhaitant les distribuer au sein de l'Union européenne doit respecter les normes européennes visant à protéger les consommateurs contre les produits non conformes. Le RGPD transpose ce modèle aux fournisseurs de services numériques :

[6] En janvier 2021, WhatsApp a annoncé qu'à partir du 15 mai de la même année, elle partagerait certaines données des utilisateurs avec sa maison mère, Facebook, et que les utilisateurs n'acceptant pas ces nouvelles CGU seraient privés de certains services. Face au départ en masse des usagers vers des services concurrents, cette menace n'a pas été mise à exécution.

[7] Acronyme de « Système automatisé pour les fichiers administratifs et répertoires des individus »

toute entité désirant proposer délibérément des services numériques à des résidents européens est tenue de respecter les protections que le droit de l'UE accorde à ces personnes.

En quelques années, le RGPD s'est imposé comme un standard au niveau international. En effet, dès lors que des entreprises étrangères appliquent le RGPD aux résidents de l'UE, les nationaux de ces pays sont incités à revendiquer chez eux et pour eux les mêmes protections que celles accordées aux résidents européens. De là découle un mouvement de diffusion des principes « Informatique et Libertés » dans des pays n'ayant pas entamé cette démarche jusqu'alors. Cette dynamique a deux origines : d'une part, les entreprises souhaitant que leur pays bénéficie de la décision d'adéquation rendue par la Commission européenne[8] afin de faciliter leurs échanges de données avec l'Union européenne et donc fluidifier le marché local de la sous-traitance (motivation économique) et, d'autre part, les citoyens militant pour bénéficier localement de droits renforcés (revendication citoyenne).

Le RGPD contribue à réduire l'asymétrie informationnelle en obligeant les responsables du traitement des données à expliciter les finalités de ce traitement, ainsi qu'en instaurant une transparence sur les données détenues sur chacun et sur leur provenance, mettant ainsi en lumière les circuits d'échanges entre collecteurs et ré-utilisateurs des données. La protection qu'il offre n'est cependant effective que s'il est possible de contraindre les responsables du traitement à s'y conformer. S'il est relativement facile de sanctionner les responsables de traitement de données situés dans l'UE ou y disposant d'un établissement principal, ou encore les entreprises ciblant spécifiquement le marché européen et pour lesquelles une interdiction représenterait un manque à gagner significatif, en revanche, il est plus difficile de toucher un responsable de traitement situé hors de l'UE et qui collecterait des données de résidents européens pour fournir un service à des clients non européens.

L'autorégulation des plates-formes, source de censure pour les usagers

Les lois protégeant les données à caractère personnel permettent notamment à toute personne de faire corriger une donnée inexacte. C'est sur cette base que s'est développé le « droit à l'oubli » : il s'agit de la possibilité de demander à un moteur de recherche de supprimer ou d'amoindrir le lien entre le nom d'une personne et une page web contenant une information considérée comme obsolète. L'émergence de ce droit en Europe a été consacrée par une décision de 2014 de la Cour de justice de l'Union européenne faisant droit à la demande d'une personne, anciennement condamnée pour certains faits, que son nom ne conduise plus vers les articles de journaux en ligne relatant ces faits, au motif que la personne s'était amendée depuis. Il ne s'agit donc pas de supprimer l'accès aux articles de journaux sur le site de l'éditeur, mais de faire en sorte qu'ils ne soient plus référencés par les principaux moteurs de recherche. Pour autant, ces demandes ne peuvent être systématiquement acceptées car ce droit à l'oubli numérique s'oppose au droit du public d'être informé, notamment quand la personne en question est une personnalité publique. Cette mise en balance d'intérêts opposés doit être effectuée au cas par cas.

[8] Actuellement, 14 États tiers bénéficient d'une décision d'adéquation avec l'UE, tels que la Corée du Sud, le Japon, le Royaume-Uni, la Suisse, etc. Cette décision permet la libre circulation des données entre l'UE et l'État tiers. Les deux accords d'adéquation passés avec les États-Unis – le « Safe Harbor » puis le « Privacy Shield » – ont successivement été invalidés par la Cour de justice de l'Union européenne en 2015 et en 2020.

Face à l'afflux de demandes que cette décision phare allait provoquer, le législateur s'est interrogé sur le moyen de les traiter. Le recours systématique aux tribunaux risquant de les engorger, le RGPD a maintenu l'approche hybride d'exercice du droit à l'effacement : ces demandes doivent être adressées en premier lieu aux moteurs de recherche qui sont les responsables des traitements d'indexation, et seulement en cas de refus de ceux-ci est-il possible de saisir les tribunaux. Pour traiter les demandes qui leur sont faites, les principaux moteurs de recherche se sont dotés de comités d'éthique *ad hoc*, visant à éviter tout conflit d'intérêts. Pour autant, ce mécanisme place explicitement les grandes plateformes du numérique dans un rôle de régulation des contenus numériques.

Il en est de même dans le cadre de la lutte contre la diffusion de contenus illicites. Les dispositifs basés sur l'obligation de retrait rapide de tels contenus (par exemple dans le cadre de la lutte contre la « haine en ligne » et les messages à caractère terroriste, mais aussi, dans une moindre mesure, pour le respect du droit d'auteur) posent de nombreux problèmes. Notamment, ils placent les opérateurs de plateformes, soumis à des sanctions financières lourdes en cas d'inaction, dans un rôle de censeur. Face au nombre de requêtes, leur réaction est de retirer automatiquement les contenus signalés avant d'en faire éventuellement l'examen, conduisant à exacerber les campagnes de signalements abusifs de la part d'intérêts très particuliers, politiques ou commerciaux. Afin de se prémunir contre des accusations d'inaction, les responsables de plateformes mettent également en œuvre des systèmes automatisés de filtrage de contenus.

Au lieu du retrait pur et simple, certaines plateformes font en sorte que leurs moteurs de « recommandation » internes ne présentent pas au public les contenus jugés comme inadéquats ou juridiquement risqués pour la plateforme. La censure privée est alors plus insidieuse, car difficile à démontrer. C'est également le cas lorsque les plateformes telles que YouTube « démonétisent » de façon automatique certains contenus qui y sont placés (les auteurs ne touchant alors plus les revenus induits par les publicités visionnées), selon des critères souvent inconnus de leurs auteurs. Il s'agit, somme toute, d'un mécanisme local de crédit social, les revenus des auteurs dépendant des sujets qu'ils abordent. Les producteurs de contenus sont ainsi incités à s'abstenir de comportements pourtant licites.

Ces contrôles automatisés, par leurs effets directs mais aussi par l'autocensure induite, conduisent à faire apparaître comme déviant ce qui est « a-normal ». Ils participent à l'établissement d'une gouvernance algorithmique (Rouvroy, 2014), dans laquelle la diffusion des contenus est soumise à des décisions sur lesquelles les personnes n'ont aucune prise.

Le traitement de données à caractère personnel a ainsi contribué de façon significative à l'hégémonie des grands acteurs mondiaux du numérique. L'objectif de servir au mieux les consommateurs s'est traduit par la collecte massive de données les concernant, ainsi que leur exploitation en temps réel, afin d'orienter le comportement des personnes, dans l'intérêt des responsables du traitement des données à caractère personnel. La régulation du capitalisme de surveillance est un sujet encore largement ouvert, qui implique des relations de plus en plus étroites entre différents régulateurs : autorités de protection des données à caractère personnel bien sûr, mais également autorités de la concurrence, autorités de régulation des contenus audiovisuels, etc. Cette régulation découle de politiques publiques qui reflètent l'évolution de l'acceptabilité sociale des technologies proposées : recommandation algorithmique, usage de la biométrie (et notamment de la reconnaissance faciale) dans divers secteurs d'activité, etc. Ces politiques traduisent un compromis social entre envie de confort et de « sécurité », d'une part, et sentiment de surveillance, d'autre part.

Ce ressenti du public est mouvant, influencé par les récits tant des acteurs privés qui promeuvent une vision dans laquelle la technologie est au service de l'humanité que des acteurs publics qui, pour faire accepter certains dispositifs de contrôle de la population, utilisent parfois la peur.

Les mirages technologiques ne doivent pas conduire à éroder les grands principes sur lesquels se sont créées les sociétés démocratiques. Le modèle économique actuel des réseaux sociaux mondialisés, fondé sur la marchandisation de l'influence sociale, semble incompatible avec la pérennité de nos démocraties (Chavalarias, 2022). Au-delà de la protection de la vie privée des personnes et de la promotion d'une concurrence, largement illusoire, dans des secteurs où les effets de réseau jouent à plein, se posent également des enjeux de souveraineté et de protection de la sincérité du débat démocratique. L'autorégulation des grandes plateformes privées n'est pas exempte de biais[9], tout comme leur sujétion à la puissance étatique[10]. Entre ces deux écueils, il s'agit de concevoir une forme de régulation nouvelle, considérant les réseaux sociaux comme des infrastructures, et conduisant à les administrer comme des communs (Chavalarias, 2022), à l'image de la gouvernance de l'Internet. La construction de celle-ci s'est effectuée en plusieurs décennies. Au vu de la situation actuelle, dans laquelle les mécanismes de recommandation des réseaux sociaux ont conduit à une polarisation accrue des opinions, il n'est pas certain que nous disposions d'autant de temps.

Bibliographie

Bronner G., 2021, *Apocalypse cognitive*, PUF.

Chavalarias D., 2022, *Toxic Data. Comment les réseaux manipulent nos opinions*, Flammarion.

Ellul J., 2012 [1re éd. 1977], *Le système technicien*, Cherche Midi.

Ellul J., 2019 [1re éd. 1988], *Le bluff technologique*, Hachette.

Ganascia J.-G., 2009, *Voir et pouvoir : qui nous surveille ?*, Le Pommier.

Harcourt B., 2020, *La société d'exposition : désir et désobéissance à l'ère numérique*, Le Seuil.

Mattelart A. et Vitalis A., 2014, *Le profilage des populations. Du livret ouvrier au cyber-contrôle*, La Découverte.

Morozov E., 2014, *Pour tout résoudre, cliquez ici. L'aberration du solutionnisme technologique*, Fyp.

Nitot T., 2016, *Surveillance:// Les libertés au défi du numérique : comprendre et agir*, C&F Éditions.

O'Neil C., 2018, *Algorithmes. La bombe à retardement*, Les Arènes.

Rouvroy A., 2014, « Des données sans personne : le fétichisme de la donnée à caractère personnel à l'épreuve de l'idéologie des Big Data », in *Le numérique et les droits et libertés fondamentaux*, Étude annuelle du Conseil d'État, La Documentation française.

Simon H. A., 1971, « Designing organizations for an information-rich world », in M. Greenberger (dir.), *Computers, Communications, and the Public Interest*, Johns Hopkins Press.

[9] En témoignent les décisions de filtrage de contenus effectuées par les plates-formes elles-mêmes en matière de morale (nudité), de droits d'auteur ou de « droit à l'oubli ».

[10] Dans ce cas, c'est celle-ci qui impose ses règles aux plates-formes, comme la fermeture administrative de comptes de réseaux sociaux.

Tesquet O., 2021, *État d'urgence technologique. Comment l'économie de la surveillance tire parti de la pandémie*, Premier Parallèle.

Zuboff S., 2020, *L'âge du capitalisme de surveillance*, Zulma.