Tristan Nitot, *Surveillance://. Les libertés au défi du numérique : comprendre et agir*, Caen, C&F éditions, Coll. « Blogollection », 2016.

Annie Lochon
Docteure en sociologie
Cerrev, Unicaen.
Annie.lochon@gmail.com

Après une brève présentation de l'auteur, du statut du texte, du contexte de parution, un résumé et une critique de l'ouvrage seront réalisés.

Présentation de l'auteur :

Né en 1966, Tristan Nitot a notamment, après des études d'informatique, participé à *Mozilla Europe* et au développement du navigateur *Firefox* dès 1998. Il a été membre du Conseil national du numérique entre 2013 et 2015 puis du comité de prospective CNIL à partir de 2015. Depuis septembre 2019, il est Directeur général du moteur de recherche *Qwant*. C'est par conséquent un spécialiste des technologies et outils numériques et en particulier des logiciels libres. Il est légitime qu'il évoque le sujet de la surveillance de masse *via* les objets connectés à Internet.

Statut du texte

L'ouvrage est destiné au grand public plutôt qu'aux spécialistes. C'est clairement un texte de vulgarisation. Sans exposer toute l'histoire d'Internet, Tristan Nitot revient sur quelques-uns des enjeux, idéalismes et utopies qui l'ont fondé. Le propos pointe une partie des enjeux sociétaux de l'utilisation des technologies informatiques et numériques. Ces technologies ont transformé notre quotidien. Ni le téléphone ni la télévision n'étaient disponibles dans tous les foyers après la Seconde Guerre mondiale. Aujourd'hui, une majorité d'entre nous évolue avec dans sa poche un objet plus puissant que les premiers ordinateurs. Grâce à ce dernier, l'individu peut accéder à une quantité d'informations impressionnantes dans un délai très court. Mais le contrôle de cet appareil ne dépend pas seulement de l'utilisateur·trice.

Sur la forme, le texte est bien organisé, construit de façon logique. L'écriture est particulièrement accessible pour les personnes qui ne sont pas spécialistes du champ numérique ou souhaiteraient avoir une première approche des liens entre la surveillance et les droits des êtres humains au sens large. L'auteur appuie son argumentation sur les modalités de fonctionnement des outils et applications numériques ainsi que les règles juridiques qui les encadrent. Par ailleurs, l'illustration choisie pour la couverture, reprise pour l'annonce de chaque partie, est en adéquation avec le thème. Les deux cercles qui s'entrecroisent suggèrent des jumelles, accessoire de la surveillance dans l'imaginaire collectif et les représentations sociales.

Contextualisation du texte :

À la suite des attentats islamistes de 2013, en France[1], Manuel Valls, alors ministre de l'Intérieur, a repris la formule *« la sécurité est la première des libertés »*[2 et 3]. Le texte de Tristan Nitot indique que la surveillance et la sécurité qu'elle suppose sont des menaces pour les libertés et la vie privée. Il pointe en particulier les risques de dérives de la démocratie vers un État policier.

L'ouvrage débute par une courte préface de cinq pages signée d'Adrienne Charmet[4]. Cette dernière, historienne de formation, est engagée dans l'association la Quadrature du Net[5].

---

[1] Et plus largement depuis les attentats de New York en septembre 2001.

[2] Formule d'Alain Peyrefitte prononcée en mars 1981 lors des débats relatifs à la loi « sécurité et liberté ». Cette formule, ensuite employée par différentes personnalités politiques de tous bords, est souvent employée pour justifier la limitation d'autres libertés.

[3] La seule liberté citée explicitement dans la *Déclaration des Droits de l'Homme et du Citoyen de 1789* est la liberté d'expression (*cf*. article 11). La liberté est définie à l'article 4 de ce même texte comme tout ce qui ne nuit pas à autrui. URL : https://www.legifrance.gouv.fr/Droit-francais/Constitution/Declaration-des-Droits-de-l-Homme-et-du-Citoyen-de-1789, vérifié le 14/02/2014.

[4] Celle-ci a cessé ses fonctions au sein de l'association en juillet 2017 et est dorénavant chargée de mission au sein de l'Agence nationale pour la sécurité des systèmes d'information (ANSSI).

[5] *« La Quadrature du Net promeut et défend les libertés fondamentales dans l'environnement numérique. L'association lutte contre la censure et la surveillance, que celles-ci viennent des États ou des entreprises privées. Elle interroge la façon dont le numérique et la société s'influencent mutuellement. Elle œuvre pour un Internet libre, décentralisé et émancipateur »* [Source : https://www.laquadrature.net/nous/, consulté le 14/02/2019].

Résumé des principaux points

Dans *Surveillance*, Tristan Nitot commence son propos par un constat. Les technologies de l'information et de la communication ont pris une place importante dans notre quotidien, au point que notre téléphone peut nous indiquer qu'il est temps de partir pour un rendez-vous enregistré dans l'agenda de ce dernier ou enregistrer nos déplacements. Cette suggestion qui pourrait paraître être un service pratique et anodin incite l'auteur à se demander qui contrôle ces technologies. Son ouvrage s'articule autour de la question : « *comment saisir le potentiel positif de l'informatique connectée sans devenir victime de la surveillance de masse ?* »[6] Cette question est un prétexte pour examiner les traces numériques que chacun·ne d'entre-nous laisse non seulement sur ses appareils, mais aussi les applications et services connectés que nous utilisons. De ce fait, il interroge le lien entre les technologies informatiques et numériques et les libertés individuelles, dont la préservation de la vie privée. Il soulève ici des enjeux politiques et sociaux. L'ouvrage est structuré en quatre parties qui vont être présentées successivement.

La première partie de l'ouvrage est consacrée aux dangers de la surveillance de masse. Elle se compose de neuf sous-parties. La première sous-partie débute par une question : « *Est-il si grave de perdre le contrôle de son ordinateur et de son ordiphone ?* »[7] En effet, les ordinateurs et ordiphones collectent des données relatives aux activités que nous avons avec ceux-ci, les envoient à des sociétés qui ne sont pas toujours connues de leurs utilisateurs·trices et réalisent des tâches que ces derniers·ères ne lui ont pas demandées. Il apparaît que, d'un côté, les utilisateurs·trices ne connaissent ni le fonctionnement ni n'ont le contrôle de ces appareils, et, d'un autre côté, les compagnies informatiques ont une connaissance des habitudes d'utilisation des outils et applications numériques. Ce déséquilibre est une source d'inquiétude sur la protection des données personnelles. Cela conduit Tristan Nitot à aborder les risques personnels liés à l'utilisation des technologies de l'information et de la communication : « *manque de protection des données* »[8] et des sauvegardes des données, question de la propriété des données, traces des activités (podomètres, trajets Uber, GPS des ordiphones, *etc*.). Ainsi, nos pratiques religieuses, de santé, nos goûts sont à portée de clic des entreprises

[6] Tristan Nitot, *Surveillance://. Les libertés au défi du numérique : comprendre et* agir, Caen, C&F éditions, Coll. « Blogollection », 2016, p. 17.
[7] *Ibidem*, p. 21.
[8] *Ibid*., p. 23

du numérique, tout comme la géolocalisation par certaines applications ou l'envoi de données vers Internet. Il est désormais possible de croiser la localisation d'une personne et ses activités physiques. Comment ce croisement de données est-il et sera-t-il utilisé ? À ce propos, *Google* et *Facebook* sont les deux sociétés qui connaissent le mieux les activités de leurs utilisateurs·trices. Pour illustration, Tristan Nitot liste les types de données collectées par les différents services de *Google* afin d'observer que « *Google sait presque tout sur nous* »[9], sans que nous en ayons vraiment conscience. Tristan Nitot révèle que ces données ne sont pas tout à fait sécurisées. Il identifie cinq cas de figure : l'entreprise du numérique peut décider de les communiquer aux forces de police (aujourd'hui des éléments de pédopornographie, demain des opposants politiques s'inquiète l'auteur), abus de pouvoir d'un employé, piratage des serveurs par des services de sécurité nationaux ou par des pirates, utilisation à mauvais escient de données publiées par soi-même. Une grande plateforme de média social, quant à elle, incite les électeurs à voter ou met en avant certains types de contenu afin de mesurer les réactions en fonction de la nature positive ou négative du dit contenu[10]. Si le cadre éthique est loin d'être respecté dans ce dernier cas, cette étude interroge quant à son implication pour la sociologie de la réception. Tristan Nitot évoque en cinquième lieu la surveillance des États. Les affaires Échelon ou Snowden ont révélé au grand public l'ampleur des systèmes d'espionnage mis en place par les États. La responsabilité liée aux données massives ou *big data* [11]permet de mettre en relation des comportements en ligne ou d'achat et des faits de la vie quotidienne (entrée dans une relation amoureuse, grossesse, notamment). Or, la réalisation de ce lien peut avoir des implications importantes pour les usagers. Le septième point de cette première partie s'intéresse aux impacts de la surveillance sur la société. Tristan Nitot débute cette septième sous-partie par une réflexion philosophique sur la société de surveillance et du contrôle. Il mobilise en particulier le panoptique de J. Bentham, qui est construit pour que des prisonniers pensent qu'ils sont constamment surveillés et adoptent ainsi leurs comportements. C'est

[9] *Ibid*., p. 32
[10] Adam D. I. Kramer, Jamie E. Guillory, Jeffrey T. Hancock, « Emotional contagion through social networks », *Proceedings of the National Academy of Sciences*, Jun 2014, 111 (24) 8788-8790. URL : https://www.pnas.org/content/111/24/8788, consulté le 17/03/2020.
[11] Rappelons que pour être qualifiée de « données massives » ou « big data », une quantité de données doit répondre à trois caractéristiques selon la CNIL : un volume important (mesuré à minimum en térabits soit 10^{12} bits), vélocité (rapidité de la collecte et du traitement des données) et être variées (textes, photos, vidéos, *etc*.).

ici le cœur du système : agir sur les comportements individuels et conformer aux normes sociales (de quelle culture ? pour compléter la pensée de Tristan Nitot) afin de faciliter les contrôles et la sécurité. La réflexion de Tristan Nitot peut se poursuivre en se demandant si la servitude volontaire, telle que l'a pensée Étienne de La Boétie, ne se complète désormais pas par la surveillance volontaire. Pour autant, chacun de nous a besoin d'une part d'intimité. « *La liberté exige la sécurité sans intrusion* »[12]. Des textes sur les droits des êtres humains et garanties de la vie privée sont rappelés ainsi que le rôle des institutions telles que la CNIL pour la protection de la vie privée. Or, le numérique semble apporter une « *érosion de la vie privée* »[13], érosion qui va de pair avec un manque de confiance des citoyens·nes dans les institutions. Pourtant ce problème est similaire pour les plateformes de Réseaux sociaux numériques (RSN) ou médias sociaux grâce auxquelles les utilisateurs·trices partagent des informations sur eux-mêmes, et renoncent volontairement à une part de leur vie privée sous prétexte de n'avoir rien à cacher. D'autre part, ces RSN ne proposent à leurs utilisateurs·trices qu'une partie des informations disponibles sur la plateforme au moyen d'un algorithme de sélection. Cet aperçu sur les modes de vie individuels ne pourrait-il pas conduire à une augmentation des cotisations d'assurance grâce à un croisement de données ? En outre, la transparence totale est-elle souhaitable ? Tristan Nitot répond par la négative en rappelant que Marc Zuckerberg[14] et Éric Schmidt[15] ont des comportements qui garantissent leur vie privée. Par ailleurs, créativité, secrets commerciaux doivent être respectés. Aussi, la transparence totale n'est pas souhaitable.

La deuxième partie de l'ouvrage a pour objet les mécanismes de la surveillance de masse. Elle commence par un constat : médias sociaux d'un côté, et politique de sécurité de l'autre favorisent l'érosion de fait de la vie privée. Puisque chacun devient dépendant des objets informatiques connectés, il nous faut comprendre leur fonctionnement afin de mieux contrôler les informations transmises et leur usage. Il s'agit d'éviter que l'outil informatique « *nous contrôle*

[12] Bruce Schneier, « The Value of Privacy », 19 mai 2006. URL : https://www.schneier.com/blog/archives/2006/05/the_value_of_pr.html, consulté le23/03/2020. Citation reprise à la page 51 de l'ouvrage.
[13] Tristan Nitot, *Op. Cit.*, 2016, p. 54.
[14] Fondateur de *Facebook*.
[15] Président-directeur de *Google* de 2001 à 2011. Président exécutif d'*Alphabet Inc*. entre 2015 et 2017.

ou permette à d'autres de nous contrôler »[16]. L'utilisateur·trice contrôle peu d'éléments du matériel utilisé en dehors des données qu'il ou elle produit. Il·Elle ne contrôle pas les logiciels qu'il·elle utilise, n'en connaît pas le code, ne peut le modifier, est contraint par des contrats d'utilisation, le piège de la gratuité, *etc*. Cela engendre un déséquilibre entre utilisateurs·trices et développeurs. C'est pourquoi des pionniers de l'informatique ont inventé des logiciels libres. Mais, là encore, il faut savoir exporter ses données vers les logiciels libres. De plus, l'absence de vérification du code peut conduire à des abus, comme l'a révélé, en septembre 2015, l'affaire Volkswagen et leur logiciel qui modifiait la mesure de la pollution réelle des voitures. C'est pourquoi la connaissance du codage est essentielle en raison de la confiance qu'elle apporte aux utilisateurs·trices. Par ailleurs, le recours à des applications payantes ne garantit pas la sécurité des données, surtout lorsqu'il est nécessaire d'utiliser le *cloud* ou l'infonuagique, c'est-à-dire de stocker des données en dehors de nos appareils. Or, les ordinateurs et smartphones ne sont plus les seuls à collecter des données et les envoyer aux fabricants : voitures, télévision, console de jeux, montres, application de quantification de soi (nombre de pas, *i.e.*). Bref, tous les objets connectés et les applications que nous utilisons. En outre, des traçages existent aussi dans l'espace public. Il s'agit de « *beacons* ». Ils servent notamment à mesurer le temps accordé à un panneau publicitaire. Tristan Nitot pose ensuite la question de l'efficience de la surveillance de masse pour lutter contre des problèmes de sécurité comme le terrorisme. En effet, cela ne revient-il pas à multiplier les données dans la recherche d'informations très précises ? Cela est d'autant plus préoccupant que ces dispositifs sont souvent adoptés après la réalisation d'actes de terreur. Citons à ce propos la loi n° 2015-912 du 24 juillet 2015 relative au renseignement adoptée à la suite des attentats de janvier 2015. Ce qu'il s'agit de prévenir en contrôlant l'accès aux données des utilisateurs·trices, selon Tristan Nitot, est l'avènement d'un État policier. Selon lui, le décryptage des discours sécuritaires afin de limiter les jeux sur les émotions est un des moyens de ne pas tomber dans ce piège, tout comme l'adhésion à des associations du type de la Quadrature du Net ou d'adopter des systèmes informatiques qui limitent la surveillance de masse.

La troisième partie porte sur les limites possibles à la surveillance. Tristan Nitot identifie sept principes qui redonnent du contrôle aux utilisateurs·trices :

[16] Tristan Nitot, *Op. Cit.*, 2016, p. 65.

utiliser des logiciels libres, le contrôle des lieux de stockage de données au moyen de l'auto-hébergement, chiffrer les échanges, trouver un modèle économique qui ne dépend pas du profilage des utilisateurs·trices, proposer une ergonomie de bon niveau, être compatible avec les systèmes existants et à venir et apporter un plus concret et immédiat par rapport aux offres existantes.

La dernière partie propose des solutions pour limiter la surveillance au quotidien. En premier lieu, il est nécessaire d'identifier quels types de données doivent être protégées et contre quelles menaces. Les collectes et fuites de données personnelles doivent être empêchées. Pour cela, il est possible de changer le système d'exploitation de ses appareils, avoir des antivirus, réaliser des sauvegardes des disques durs des ordinateurs, chiffrer ces disques durs, choisir son navigateur, ses mots de passe, ses extensions[17], adopter un moteur de recherche respectueux de la vie privée, bloquer la publicité ou non, éviter certains services de messagerie, créer son propre domaine, apprendre à chiffrer ses courriels, paramétrer *Google*, limiter l'utilisation des médias sociaux ou en utiliser des alternatifs, développer un *cloud* personnel font partie des solutions qui peuvent être mises en œuvre par les utilisateurs·trices. Ces solutions sont relativement faciles à mettre en œuvre, d'autant que l'auteur fournit des indications sur la manière de procéder. Certaines faisaient partie de mes habitudes au moment de la lecture de cet ouvrage. D'autres solutions proposées par Tristan Nitot sont venues les compléter.

Il ressort de cette lecture une révision adaptée au début du XXI^{ème} siècle de la citation de Jean de La Fontaine (1621 – 1695) *« L'adversaire d'une vraie liberté est un désir excessif de sécurité »*, ou encore celle de Benjamin Franklin (1706-1790) « *Ceux qui abandonnent une liberté essentielle pour une sécurité minime et temporaire ne méritent ni la liberté ni la sécurité* »[18]. Or, la surveillance numérique est le moyen actuellement le plus développé pour prétendre à une certaine forme de sécurité. L'auteur soulève le problème que cette surveillance est généralisée, massive alors qu'une minorité menace cette sécurité. Cela ne revient-il pas à

[17] *Firefox* propose une extension qui permet de limiter les données récoltées par *Facebook*, *i.e.*

[18] Lettre adressée en 1755 par Franklin au gouverneur colonial, au nom de l'Assemblée de Pennsylvanie [source : https://www.telerama.fr/medias/etats-d-urgence-liberte-et-securite-arretons-de-citer-benjamin-franklin,135221.php].

chercher une petite aiguille dans une gigantesque botte de foin, pour reprendre une métaphore utilisée par Tristan Nitot ?

Cependant, la surveillance n'est pas seulement exercée par les États, quelle que soit leur forme de régime politique, mais aussi par des entreprises privées. Les objectifs de la surveillance sont alors plus difficiles à identifier.

Critique

Tristan Nitot, en particulier dans la première partie, tend à confondre les intérêts des grandes entreprises du numérique avec ceux des États. Si les outils de la surveillance sont communs, il semble que la sécurité et le maintien des pouvoirs existants ne soient pas forcément le premier intérêt de ces grandes entreprises (ou alors je suis beaucoup plus naïve que je ne le pensais).

L'apport au débat de société de cet ouvrage est important puisqu'il propose des clés de réflexion sur le numérique et des solutions techniques afin de mieux contrôler nos données, ce qui est un atout indéniable de l'ouvrage. Si un lecteur averti en vaut deux, remercions Tristan Nitot de ses avertissements. Ainsi, quelques jours après la première lecture de cet ouvrage, l'auteure de cette note critique a pu mesurer les traces qu'elle laissait en découvrant qu'elle pouvait accéder à son historique du week-end sur l'ordinateur utilisé au bureau. Si l'on peut être tenté d'y trouver un côté pratique, dans un premier temps, je me suis demandée, dans un second temps, qui d'autre pouvait faire le lien entre les pratiques personnelles et professionnelles. J'ai opté pour un changement de navigateur. Tristan Nitot suggère qu'il est relativement simple d'installer et d'utiliser son propre matériel afin de le contrôler et de limiter les données que l'on offre aux grandes entreprises. À titre personnel, je ne sais pas si je tenterai de faire cela sans l'aide d'une personne ayant davantage de connaissances dans l'utilisation de ces systèmes.

L'objectif proposé par Tristan Nitot au début de son livre était d'exposer le potentiel positif de l'informatique connecté en limitant la surveillance de masse. Le texte atteint tout à fait cet objectif.

Cependant, l'apport au débat scientifique est relativement limité. Si un peu de philosophie politique est présente dans l'ouvrage, ces points sont peu détaillés. Les solutions proposées sont plutôt individuelles que collectives, et l'ouverture d'un débat public sur ces questions est peu mise en valeur. Tristan Nitot termine sur la réappropriation citoyenne et les enjeux politiques, le rôle des associations. Ce sont

des questions qu'il est effectivement temps de nous poser collectivement. Apprendre à coder devrait ainsi être une des compétences à développer chez tous les citoyens.nes, ce qui n'est pas envisagé dans l'ouvrage.