

# INTERNATIONAL JOURNAL OF **DIGITAL AND DATA LAW**

---

REVUE INTERNATIONALE DE DROIT  
DES DONNÉES ET DU NUMÉRIQUE



Vol. 7 - 2021



ISSN 2553-6893

**International Journal of Digital and Data Law**  
**Revue internationale de droit des données et du numérique**

**Direction :**  
**Irène Bouhadana & William Gilles**

ISSN : 2553-6893

**IMODEV**  
49 rue Brancion 75015 Paris – France  
[www.imodev.org](http://www.imodev.org)  
[ojs.imodev.org](http://ojs.imodev.org)

*Les propos publiés dans cet article  
n'engagent que leur auteur.*

*The statements published in this article  
are the sole responsibility of the author.*

**Droits d'utilisation et de réutilisation**

Licence Creative Commons – Creative Commons License -



Attribution

Pas d'utilisation commerciale – Non Commercial

Pas de modification – No Derivatives

## À PROPOS DE NOUS

La **Revue Internationale de droit des données et du numérique (RIDDN)/ the International Journal of Digital and Data Law** est une revue universitaire créée et dirigée par Irène Bouhadana et William Gilles au sein de l'IMODEV, l'Institut du Monde et du Développement pour la Bonne Gouvernance publique.

**Irène Bouhadana**, docteur en droit, est maître de conférences en droit du numérique et droit des gouvernements ouverts à l'Université Paris 1 Panthéon-Sorbonne où elle dirige le master Droit des données, des administrations numériques et des gouvernements ouverts au sein de l'École de droit de la Sorbonne. Elle est membre de l'Institut de recherche juridique de la Sorbonne (IRJS). Elle est aussi fondatrice et Secrétaire générale de l'IMODEV. Enfin, associée de BeRecht Avocats, elle est avocate au barreau de Paris et médiatrice professionnelle agréée par le CNMA.

**William Gilles**, docteur en droit, est maître de conférences (HDR) en droit du numérique et en droit des gouvernements ouverts, habilité à diriger les recherches, à l'Université Paris 1 Panthéon-Sorbonne où il dirige le master Droit des données, des administrations numériques et des gouvernements ouverts. Il est membre de l'Institut de recherche juridique de la Sorbonne (IRJS). Il est aussi fondateur et Président de l'IMODEV. Fondateur et associé de BeRecht Avocats, il est avocat au barreau de Paris et médiateur professionnel agréé par le CNMA.

**IMODEV** est une organisation scientifique internationale, indépendante et à but non lucratif créée en 2009 qui agit pour la promotion de la bonne gouvernance publique dans le cadre de la société de l'information et du numérique. Ce réseau rassemble des experts et des chercheurs du monde entier qui par leurs travaux et leurs actions contribuent à une meilleure connaissance et appréhension de la société numérique au niveau local, national ou international en analysant d'une part, les actions des pouvoirs publics dans le cadre de la régulation de la société des données et de l'économie numérique et d'autre part, les modalités de mise en œuvre des politiques publiques numériques au sein des administrations publiques et des gouvernements ouverts.

IMODEV organise régulièrement des colloques sur ces thématiques, et notamment chaque année en novembre les *Journées universitaires sur les enjeux des gouvernements ouverts et du numérique / Academic days on open government and digital issues*, dont les sessions sont publiées en ligne [ISSN : 2553-6931].

IMODEV publie deux revues disponibles en open source ([ojs.imodev.org](https://ojs.imodev.org)) afin de promouvoir une science ouverte sous licence Creative commons **CC-BY-NC-ND** :

1) la *Revue Internationale des Gouvernements ouverts (RIGO)/ International Journal of Open Governments* [ISSN 2553-6869] ;

2) la *Revue internationale de droit des données et du numérique (RIDDN)/ International Journal of Digital and Data Law* [ISSN 2553-6893].

## ABOUT US

The **International Journal of Digital and Data Law / Revue Internationale de droit des données et du numérique (RIDDN)** is an academic journal created and edited by Irène Bouhadana and William Gilles at IMODEV, the Institut du monde et du développement pour la bonne gouvernance publique.

**Irène Bouhadana**, PhD in Law, is an Associate professor in digital law and open government law at the University of Paris 1 Panthéon-Sorbonne, where she is the director of the master's degree in data law, digital administrations, and open governments at the Sorbonne Law School. She is a member of the Institut de recherche juridique de la Sorbonne (IRJS). She is also the founder and Secretary General of IMODEV. Partner at BeRecht Avocats, she is an attorney at law at the Paris Bar and a professional mediator accredited by the CNMA.

**William Gilles**, PhD in Law, is an Associate professor (HDR) in digital law and open government law at the University of Paris 1 Panthéon-Sorbonne, where he is the director of the master's degree in data law, digital administration and open government. He is a member of the Institut de recherche juridique de la Sorbonne (IRJS). He is also founder and President of IMODEV. Founder and partner at BeRecht Avocats, he is an attorney at law at the Paris Bar and a professional mediator accredited by the CNMA.

**IMODEV** is an international, independent, non-profit scientific organization created in 2009 that promotes good public governance in the context of the information and digital society. This network brings together experts and researchers from around the world who, through their work and actions, contribute to a better knowledge and understanding of the digital society at the local, national or international level by analyzing, on the one hand, the actions of public authorities in the context of the regulation of the data society and the digital economy and, on the other hand, the ways in which digital public policies are implemented within public administrations and open governments.

IMODEV regularly organizes conferences and symposiums on these topics, and in particular every year in November the Academic days on open government and digital issues, whose sessions are published online [ISSN: 2553-6931].

IMODEV publishes two academic journals available in open source at [ojs.imodev.org](https://ojs.imodev.org) to promote open science under the Creative commons license CC-**BY-NC-ND**:

- 1) the *International Journal of Open Governments/ la Revue Internationale des Gouvernements ouverts (RIGO)* [ISSN 2553-6869] ;
- 2) the *International Journal of Digital and Data Law / la Revue internationale de droit des données et du numérique (RIDDN)* [ISSN 2553-6893].

## LA SURVEILLANCE NUMÉRIQUE EN TEMPS DE PANDÉMIE

par **Ana Cristina AGUILAR VIANA**, Doctorante à l'Université Paris 1 Panthéon-Sorbonne et à l'Université Fédérale du Parana (Brésil).

---

**L**e contrôle de la santé publique est un devoir des gouvernements. Pour exercer ce devoir de manière efficace, un État peut utiliser certaines prérogatives limitant les droits et garanties des citoyens. La pandémie du coronavirus a révélé en 2020 des situations inquiétantes concernant la surveillance de la population, notamment avec le soutien des nouvelles technologies, dont l'efficacité permet aux États d'exercer des contrôles plus rigoureux afin de maîtriser la propagation du virus.

Grâce aux commodités offertes par les nouvelles technologies, un grand nombre de nations utilisent des dispositifs numériques pour lutter contre la progression du virus. Toutefois, la réalité s'est avérée un exercice de surveillance intensifiée face à la pandémie, lequel accélère aussi le processus de transformation numérique de la société, dont les citoyens sont surveillés de façon toujours plus continue.

Donc, ce qui devait devenir une exception dans une situation d'urgence se transforme en condition permanente sous la justification de la surveillance du virus et de la santé. Cette pratique peut excéder les limites de la vie privée des gens, car elle peut violer les limites de l'intimité et c'est la raison pour laquelle on s'interroge sur la mesure dans laquelle les gouvernements peuvent agir. Désormais, face à une situation régulière d'urgence et à ces limitations constantes des garanties et des droits fondamentaux, les instruments de contrôle et de surveillance doivent être considérés et étudiés.

De ce fait, pour appréhender le scénario contemporain de la surveillance des individus en une période de transformation numérique, ainsi que ses violations, il est essentiel de considérer en premier lieu l'étude de la surveillance et aussi les aspects caractéristiques de l'univers des données. Pour cette raison, nous identifions dans cet article en première approche, les étapes et les phases de la surveillance mises en évidence par la recherche bibliographique, ainsi que le scénario contemporain du capitalisme de surveillance résultant des données. Puis, dans un deuxième moment, nous examinons les types de surveillance et de violations des droits des citoyens qui sont évoqués pendant la pandémie du coronavirus.

## § 1 – THÉORIES DE LA SURVEILLANCE ET LE CAPITALISME DE SURVEILLANCE

Aujourd'hui, les études sur la surveillance sont considérées comme un sujet d'analyse interdisciplinaire. Pour Florent Castagnino, la surveillance peut être étudiée par discipline, comme le droit, la sociologie, la géographie et même les mathématiques. Il est également possible de mener des recherches à travers les objets et/ou agents de surveillance, comme la police, les caméras, la biométrie, la géolocalisation. Toutefois, l'étude peut être développée sur un objet spécifique, comme l'emprisonnement, la cybercriminalité, les données personnelles, les bases de données, etc. La surveillance est également exploitée par le biais de ses fonctions. Enfin, il est possible de l'examiner en envisageant ses finalités, qui peuvent être sécuritaires, de santé, économiques<sup>1</sup>.

Sous tous ces aspects, il est possible de classer les études de surveillance en trois phases théoriques<sup>2</sup>, ou trois flux analytiques<sup>3</sup>. La première étape peut être nommée études panoptiques, ou modernes. La deuxième étape est la théorie des réseaux de surveillance, ou études postmodernes. La troisième étape englobe l'univers des études menées – avec de multiples perceptions – à propos de la surveillance exercée par les nouvelles technologies. Ainsi, la situation actuelle de la transformation numérique, qui résulte de l'utilisation et de l'expansion des données aboutit à ce que l'on appelle le capitalisme de surveillance.

### A) Les théories sur la surveillance

Le premier type de théorie est le modèle panoptique qui a été initialement développé par Jeremy Bentham, puis utilisé par Michel Foucault. Jeremy Bentham est reconnu comme le père de la philosophie utilitaire<sup>4</sup>. Bien qu'il s'intéresse à la morale, l'auteur a apporté une contribution pertinente à la pensée moderne par le biais panoptique<sup>5</sup>.

L'intellectuel a développé plusieurs modèles panoptiques, mais celui de la prison est le plus connu. Son intention était de proposer un exercice de surveillance dans lequel le contrôleur n'est pas apparent. En d'autres termes, le surveillé ne savait pas s'il était contrôlé ni quand cela se passait. Par la suite, Michel Foucault, sur le modèle de Bentham, a évoqué les régimes

<sup>1</sup> F. CASTAGNINO, « Critique des Surveillances Studies. Éléments pour une sociologie de la surveillance », *Déviance et société*, 2018, n° 1, Vol. 42, pp. 9-40.

<sup>2</sup> T. MAŠA; K., BERT-JAAP, "Surveillance Theory and Its Implications for Law", R. BROWNSWORD, E. SCOTFORD, K. YEUN (eds), *The Oxford Handbook of Law, Regulation and Technology*, Jul. 2017.

<sup>3</sup> F. CASTAGNINO, op.cit.

<sup>4</sup> A. BRUNON-ERNST, « Une revue pour la recherche sur Bentham et l'utilitarisme », *Revue d'études benthamiennes*, n° 14, 2018 : <http://journals.openedition.org/etudes-benthamiennes/812>.

<sup>5</sup> M. BOZOVIC, « Introduction: an Utterly Dark Spot », in J. Bentham, *The Panopticon Writings*, Verso, 1995.

disciplinaires, dans une modification du système de sanction. Si, auparavant, il y avait une condition de punition, le système disciplinaire est devenu le modèle pour exercer un contrôle sur la société.

Dans cette première conception, la surveillance était comprise comme une conséquence des organisations bureaucratiques, de l'État-nation. Ses caractéristiques principales étaient les suivantes : i) la surveillance était principalement physique, confinée à des espaces physiques fermés et visibles ; ii) l'acteur principal de la surveillance était l'État, avec ses institutions ; iii) les individus étaient l'objet de la surveillance ; iv) la surveillance visait à la discipline<sup>6</sup>.

La deuxième étape de la théorie de la surveillance a commencé à la fin des années 1970 et est considérée comme post-panoptique en raison des changements du scénario politico-économique<sup>7</sup>. Si dans les modèles précédents, on avait mis en relief l'individu, le corps et l'institution, dans les théories postmodernes, la surveillance était une question de « surveillance et de visibilité », et est devenue universelle et intrusive pour son caractère technologique<sup>8</sup>.

Gilles Deleuze<sup>9</sup>, en référence à Michel Foucault et à son travail de discipline, a souligné que la société était passée d'une société de discipline à une société de contrôle. En effet, le contrôle n'était pas seulement sur les corps des personnes, sur les domaines physiques et individuels. Avec la mondialisation et la postmodernité, la société était contrôlée de manière abstraite, par des flux. L'environnement, qui était vertical, est devenu un rhizome. Depuis, personne ne sait plus où se trouvent le début ou la fin de cet environnement. Cette structure a complètement changé la manière dont la société était contrôlée. Grâce à ce phénomène, le contrôle est fluide, tout comme la société.

Le type de contrôle, mentionné par Deleuze, a été incorporé par Haggerty et Ericson pour démontrer le changement à la fois de l'objet du contrôle et de l'institution qui le contrôle. De plus, ce contrôle ne résidait pas seulement dans l'État, mais aussi, et notamment, dans les grandes entreprises. En résumé, les principales caractéristiques de la deuxième étape de la théorie de la surveillance étaient : i) son abstraction, car la surveillance était numérique, reproductive, souvent invisible ou opaque ; ii) les principaux acteurs de la surveillance étaient dans les entreprises ; iii) le consommateur était l'objet de surveillance<sup>10</sup>.

Bien que distinctes, les études qui ont en commun l'analyse des nouvelles technologies permettent de prévoir une troisième étape

<sup>6</sup> A. VIANA, V. VALLE, « Estudos sobre vigilância: do panóptico ao big-other » (*non publié*).

<sup>7</sup> Ibidem, p.12.

<sup>8</sup> K. HAGGERTY, R. ERICSON, "The Surveillant Assemblage", *British Journal of Sociology*, Vol. 51, 2000.

<sup>9</sup> G. DELEUZE, "Postscript on the Societies of Control", *October*, Vol. 59, 1992.

<sup>10</sup> A. VIANA ; V. VALLE, op.cit.

d'études sur le sujet<sup>11</sup>. Elles ont en commun de faire passer la surveillance de l'État-nation/marché à l'entrée des domiciles. L'individu devient un acteur de la surveillance<sup>12</sup>. Le fait que les gens participent activement à la surveillance est largement exploré par les auteurs. En effet, l'internet permet aux utilisateurs de participer et de s'exposer de manière quotidienne et instantanée. L'individu, qui était le passif de la relation, devient un acteur.

Steve Mann repense le concept de surveillance en examinant la participation de l'utilisateur en tant qu'acteur du système et propose une « sousveillance ». L'intention est de mettre en évidence l'activité du point de vue d'une personne impliquée, généralement donné par un appareil d'enregistrement portable. La surveillance des yeux faite « depuis le ciel », passe à « la terre ». Les enregistrements qui étaient effectués par de grands appareils, sont maintenant de sujet à sujet<sup>13</sup>.

À son tour, Anders Albrechtslund, nomme « surveillance participative » les actions des personnes dans les réseaux sociaux et leurs relations de pouvoir. Son idée est de considérer la surveillance comme une pratique mutuelle, qui est modelée sur les caractéristiques des réseaux sociaux en ligne<sup>14</sup>. Pour Bernard Harcourt, la société elle-même choisit de s'exposer. Ainsi, la société du spectacle devient celle de l'exposition. L'auteur voit aussi que le pouvoir n'est pas vertical, mais pluriel, structuré en réseaux et horizontal. Il fait allusion à un miroir, car cette exposition constitue une image déformée qui n'est donc qu'un reflet.

David Lyon comprend la surveillance contemporaine par l'utilisation de la base de données. Il s'agit d'une méthode efficace de contrôle des comportements pour influencer les personnes et les populations et pour anticiper et prévenir les risques<sup>15</sup>. Pour Lyon, on assiste à un monde de relations à distance, où beaucoup de connexions n'impliquent pas de personnes directement liées et où il n'est pas nécessaire de voir les visages de ceux qui sont en contact. Les personnes sont devenues des doubles<sup>16</sup>.

Finalement, la prochaine étape de la surveillance est celle que l'on peut nommer « uberveillance ». C'est un type de surveillance électronique qui est omniprésent. Elle vient de la technologie qui permet d'intégrer des dispositifs de surveillance dans le corps humain. Bien que la plupart des applications pratiques à court terme des interfaces cerveau-machine sans fil soient médicales,

<sup>11</sup> Ibid.

<sup>12</sup> D. LYON, "Surveillance as social sorting: privacy, risk, and digital discrimination", *Psychology press*, 2003.

<sup>13</sup> S. MANN, "Sousveillance. Inverse Surveillance in Multimedia Imaging", accessible à : <http://wearcam.org/acmmm2004sousveillance/mann.pdf>.

<sup>14</sup> A. ALBRECHTSLUND, "Online Social Networking as Participatory Surveillance", accessible à : <https://journals.uic.edu/ojs/index.php/fm/article/view/2142/1949>.

<sup>15</sup> D. LYON, op.cit, p.1.

<sup>16</sup> H. KOSKELA, "Webcams, TV Shows and Mobile Phones: Empowering Exhibitionism", *Surveillance and Society*, n° 2, 2004, p. 199.

Elon Musk exprime le souhait que ces dispositifs puissent aider l'intelligence humaine à concurrencer l'intelligence artificielle<sup>17</sup>.

En synthèse, les principales caractéristiques de la troisième étape sont : i) une surveillance physique, abstraite et numérique ; une surveillance confinée et ouverte, stable et liquide, visible et opaque ; ii) les principaux acteurs sont l'État, les entreprises et les individus eux-mêmes ; iii) l'objet de la surveillance est le citoyen, iv) la surveillance vise à la fois la discipline et le contrôle d'accès.

### **B) La société des données et le capitalisme de surveillance**

La révolution numérique a pour grande caractéristique la collecte de données. La profondeur, l'amplitude et la vitesse de cette collecte sont les éléments fondateurs de ce nouveau moment qui a surtout dans les grandes données, dans l'intelligence artificielle et dans l'internet des objets ses principaux instruments de changement. La matière première de tous ces dispositifs est la donnée.

Aujourd'hui, tout peut être source de données. Les goûts, les recherches faites dans les réseaux ou par satellites, les photos, les vidéos, les appareils photo, le GPS. Grâce aux smartphones, les personnes remplissent quotidiennement des données pour l'utilisation, la sauvegarde et la création de profils. Tout est personnalisé. Les données sont obtenues, traitées, analysées, vendues et revendues<sup>18</sup>.

Grâce à ces bases de données, on crée des données dupliquées qui sont en constante mutation et qui serviront de balise pour prédire les goûts des sujets, formatés selon les informations de leurs profils, de leurs personnalités.<sup>19</sup> Les bases de données reposent sur les données sauvegardées. Colin Burke souligne que la composition et l'interprétation de ces données produisent la vie et le corps du sujet en duplication des données. Ce sont des couches d'identités algorithmiques<sup>20</sup>.

Cette réalité peut être traduite par les mots « anticipation », « prédiction » et « manipulation ». Avec la « datification », les actions sont transformées en données quantifiées en ligne, ce qui permet un suivi en temps réel et une analyse prédictive. La prévisibilité est assurée par le calcul effectué grâce à l'exploitation des données de manière probabiliste. Le calcul effectué à cette fin

---

<sup>17</sup> EMBEDDED SURVEILLANCE STUDIES, « Elon Musk Unveils Pig He Claims Has a Computer Implant in Brain ». Accessible à : <http://uberveillance.com>

<sup>18</sup> S. ZUBOFF, « Big Other: Surveillance Capitalism and the Prospects of an Information Civilization », accessible à : <https://cryptome.org/2015/07/big-other.pdf>

<sup>19</sup> D. LYON, op.cit, p.1.

<sup>20</sup> C. BURKE, « Sousveillance: A Network Analysis of the US Surveillant Assemblage », *Surveillance & society*, Vol 18, n° 1, 2020, accessible à : <https://ojs.library.queensu.ca/index.php/surveillance-and-society/issue/view/835>.

est inconnu, car il s'agit d'une boîte noire. Par conséquent, ce qui est connu, c'est un ensemble de prédictions probabilistes<sup>21</sup>.

Cette situation conduit à un type spécifique de surveillance appelé la surveillance des données, la « dataveillance ». Elle désigne, en bref, la surveillance continue des citoyens sur la base de leurs données et notamment de leurs données en ligne. La « dataveillance », contrairement à la surveillance traditionnelle, est courante et continue pour tout type de finalité et pour une durée indéterminée. Elle permet de construire et d'affiner les profils des personnes et leurs comportements<sup>22</sup>.

À cet égard, Aron Darmody et Detlev Zwick associent la surveillance omniprésente ainsi que la conception de choix algorithmiques à l'autonomie et à la liberté de choix. Ces éléments ne sont donc pas visualisés comme des opposés, mais comme des compléments qui construisent un monde parfait (même si c'est un conte de fées).

La conjoncture de la surveillance exercée en ce moment, en rapport avec les transformations technologiques et leurs impacts sur les autres systèmes, consacre ce que la doctrine désigne comme le capitalisme de surveillance. Le capitalisme de surveillance est un mode d'accumulation énoncé par Shoshana Zuboff qui a dans le « big data » sa composante fondamentale. Cette nouvelle formule prédit et modifie le comportement humain dans le but de produire des revenus et de contrôler le marché. L'objectif est de saisir et de convertir les données. Il s'agit d'une extraction qui se fait sans dialogue ni consentement, ce qui révèle la relation indifférente entre les entreprises et les populations<sup>23</sup>.

C'est une perspective qui façonne le concept de Big-other, un nouveau régime, où les données sont portées à l'intérieur et à l'extérieur du corps des individus, ce qui engendre des possibilités d'observation, d'interprétation, de communication, d'influence, de prédiction et, enfin, de modification de la totalité de l'action de la personne. Il s'agit d'un régime institutionnel omniprésent en réseau qui enregistre, modifie et commercialise l'expérience des individus, leurs communications, leurs pensées, dans le but d'établir de nouvelles voies de monétisation et de profit<sup>24</sup>.

Le « Grand Autre » c'est le pouvoir souverain d'un futur proche qui anéantit la liberté atteinte par l'État de droit. Il s'agit d'un nouveau régime, où les données sont véhiculées à l'intérieur et à l'extérieur du corps des individus, qui engendre des possibilités d'observation, d'interprétation, de communication, d'influence, de prévoyance et, enfin, de modification de la totalité de l'action de

<sup>21</sup> M. ANDREJEVIC, "The Big Data Divide", *International Journal of Communication*, n° 8, 2014, pp. 1673-1689.

<sup>22</sup> J. DIJCK, "Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology", *Surveillance and Society*, 2014, Vol. 12, pp. 197-208.

<sup>23</sup> A. VIANA, « Capitalismo de vigilância », in: Cl. DE SOUZA, F. ALVIM, J. BARREIROS NETO, H. DANTAS (org.), *Dicionário de eleições*, 1ed.curitiba, Juruá, 2020, Vol. 1, pp. 1-137.

<sup>24</sup> Ibid.

la personne. Contrairement au pouvoir de la société de masse, il n'y a pas d'échappatoire au Grand Autre. Il n'y a pas de place où l'Autre n'est pas.

L'esprit d'anticipation conduiront à un monde d'automatisation. Il s'agit d'un « conformisme d'anticipation », selon lequel le choix de l'individu est prédéterminé pour s'inscrire dans les objectifs d'évasion des sanctions et de camouflage social. Autrement dit, il y a une forte possibilité de distinction entre le comportement qu'une personne aurait effectivement adopté et celui qu'elle a choisi comme solution instrumentale<sup>25</sup>.

## §2 – LA SURVEILLANCE PENDANT LA PANDÉMIE

Lors de la pandémie du coronavirus, de multiples solutions numériques ont été adoptées, notamment des outils de suivi numérique qui permettent de surveiller les individus grâce à leur téléphone intelligent. La recherche de nouveaux modes d'analyse des données, y compris l'apprentissage automatique et l'intelligence artificielle, en particulier dans des crises telles que la pandémie actuelle, est une réalité pour de nombreux pays<sup>26</sup>.

La situation de l'utilisation de ces dispositifs a, dès le début, suscité plusieurs questions sur les limites des droits fondamentaux des citoyens. Puis, avec la permanence du virus, la vigilance a été maintenue, ce qui amène aussi d'autres questions.

### A) La surveillance pendant la pandémie : les procédures

D'abord, il faut souligner que les États disposent de mécanismes pour contrôler la propagation du virus, avec le soutien de divers dispositifs. Il existe plusieurs solutions pour l'exercice d'une surveillance qui cherche à suivre les individus à travers leurs téléphones. Le GPS, le Bluetooth, ou même la reconnaissance faciale peuvent être utilisés. La géolocalisation, par exemple, est fréquemment employée. Elle permet de reconstituer les mouvements de la population, d'identifier les zones à forte densité et à risque, ainsi que de contrôler la conformité des mesures de confinement de manière globale ou individualisée<sup>27</sup>.

La géolocalisation peut être obtenue par le biais de réseaux sociaux tels que Facebook et de plateformes comme Google Maps, qui disposent des données GPS de leurs utilisateurs. Par conséquent, Facebook et Google ont ouvert les données « agrégées et anonymes » aux chercheurs et aux autorités dans le

<sup>25</sup> S. ZUBOFF, "Big other: Surveillance Capitalism and the Prospects of an Information Civilization", *Journal of Information Technology*, n° 30, 2015, accessible à : <https://cryptome.org/2015/07/big-other.pdf>.

<sup>26</sup> D. LYON, "Cellphone Tracking Might Help Stamp Out Covid-19. But at What Cost?", *Ottawa Citizen*, 6 avril 2020, accessible à : <https://ottawacitizen.com/opinion/lyon-cellphone-tracking-might-help-stamp-out-covid-19-but-at-what-cost/wcm/a58e9d06-1709-4152-8ec3-ea57cc9d5d0d/>.

<sup>27</sup> A. CHERIF, « Tracking du Covid-19 : comment font les autres pays ? », *La Tribune* : <https://www.latribune.fr/technos-medias/tracking-du-covid-19-comment-font-les-autres-pays-844772.html>.

cadre de la pandémie<sup>28</sup>. Par ailleurs, les opérateurs de télécommunications disposent de nombreuses informations en raison des données mobiles collectées qui sont automatiquement générées lorsqu'une personne utilise un appareil mobile.

En plus, il est possible de cartographier la propagation du virus à partir d'objets connectés tels que les cartes bancaires et de transport. D'autre part, la vidéosurveillance et la reconnaissance faciale sont une réalité pour contrôler la propagation du virus et sont des cas plus dangereux. Elles sont réalisées sans le consentement des utilisateurs et sont utilisées massivement dans les espaces publics<sup>29</sup>.

La reconnaissance algorithmique des visages est un exemple clé de la manière dont les technologies de l'information transforment la surveillance et les relations de pouvoir. Les médias sociaux, la vidéosurveillance, le contrôle des frontières, la publicité ciblée et le profilage policier ne sont que certains des domaines dans lesquels les algorithmes de reconnaissance de visages sont testés et mis en œuvre.

Au MIT, des chercheurs mènent un projet visant à observer le développement d'applications de traçage de contacts en vue de freiner la propagation de le Covid-19<sup>30</sup>. Dans le cadre des recherches menées sur ces applications, ils ont identifié 47 pays qui utilisent des applications de suivi. Le tableau ci-dessous indique la quantité de dispositifs utilisés, ainsi que certains pays qui les ont utilisés pendant la pandémie.

|                                 |                                                                                          |
|---------------------------------|------------------------------------------------------------------------------------------|
| GPS                             | • Chine, Thaïlande, Corée du Sud, Singapour, Israël, Russie, États-Unis, Italie, Pologne |
| Bluetooth                       | • France, Singapour                                                                      |
| Carte bancaire                  | • Chine, Corée du Sud, Singapour                                                         |
| Bracelet                        | • Allemagne, Hong-Kong, Abu-Dhabi                                                        |
| Reconnaissance faciale et vidéo | • Chine, Corée du Sud, Singapour, Russie                                                 |

Source : auteur

<sup>28</sup> Ibid.

<sup>29</sup> Ibid.

<sup>30</sup> P. O'NEIL, T. MOSLEY, B. JOHNSON, "A flood of Coronavirus Apps Are Tracking us. Now It's Time to Keep Track of Them", *MIT Technology Review*, 7 May 2020, accessible à : <https://www.technologyreview.com/2020/05/07/1000961/launching-mitr-covid-tracing-tracker/>

Avec tous ces outils, les États ont également commencé à créer des applications pour le suivi des contacts. Dans un premier temps, chaque pays a développé un type d'application. Certains services sont produits localement par de petits groupes, tandis que d'autres sont des opérations mondiales.

La Chine, par exemple, dispose d'un dispositif technologique développé par le gouvernement à travers un système de notation de ses citoyens appelé Sésame Crédit.<sup>31</sup> Au début de la pandémie, Alipay, une filiale de la société Alibaba, a développé, en coopération avec le gouvernement, l'application Alipay Health Code. Ajouté au système de Crédit Sésame, Alipay Health Code affiche un code QR coloré qui conditionne le niveau de liberté des citoyens chinois.<sup>32</sup>

En août 2020, Apple et Google ont lancé un outil qui permet d'identifier les coronavirus dans le monde entier. À partir de cet outil, plusieurs gouvernements ont créé des applications, comme le Brésil et plusieurs États des États-Unis.

### **B) La surveillance pendant la pandémie : un modèle courant**

C'est une réalité qui soulève une question sur les limites du pouvoir de l'État par rapport aux garanties individuelles. De nombreux pays appliquent de nouvelles mesures de surveillance pour suivre les déplacements de population. Toutefois, ces mesures n'indiquent que peu de choses sur le moment ou la manière dont elles seront retirées une fois la crise terminée.<sup>33</sup>

Les recherches du MIT soulignent que très peu d'informations sont fournies sur ces applications et sur la manière dont elles pourraient affecter la société. Combien de personnes les téléchargeront et les utiliseront et quelle doit être leur utilisation pour réussir ? Quelles données collecteront-elles et avec qui seront-elles partagées ? Comment ces informations seront-elles utilisées à l'avenir ? Des politiques ont-elles été mises en place pour prévenir les abus ?

Certains principes sont pertinents et il faut en discuter lorsque la surveillance de masse est envisagée. Certains ont trait à la protection des données, comme la proportionnalité, la limitation

---

<sup>31</sup> P. CROQUET, « En Chine, un système de notation des citoyens encore flou mais aux ébauches effrayantes », *Le Monde*, 28 décembre 2018, accessible à : [https://www.lemonde.fr/pixels/article/2018/12/28/en-chine-un-systeme-de-notation-des-citoyens-encore-flou-mais-aux-ebauches-effrayantes\\_5403357\\_4408996.html](https://www.lemonde.fr/pixels/article/2018/12/28/en-chine-un-systeme-de-notation-des-citoyens-encore-flou-mais-aux-ebauches-effrayantes_5403357_4408996.html).

<sup>32</sup> L. NEVEU, « Comment fonctionne l'application contre le covid-19 en Chine ? », *Futura tech*, accessible à : <https://www.futura-sciences.com/tech/actualites/smartphone-fonctionne-application-covid-19-chine-80593/>

<sup>33</sup> K. BALL, S. DIBB, S. DEGLI ESPOSTI, "Why Governments and Corporations Need to Demonstrate Principled Authority in the Face of Global Health Surveillance", accessible à : <https://medium.com/surveillance-and-society/why-governments-and-corporations-need-to-demonstrate-principled-authority-in-the-face-of-global-ba1bc1573f2c>

de la finalité, le consentement et d'autres principes de protection des données.<sup>34</sup>

À ce sujet, principe d'autorité consiste à ce qu'une institution exerce son autorité d'une manière digne de confiance. Son acceptabilité par le public dépend de sa compétence, de sa bienveillance et de son intégrité.<sup>35</sup> La bienveillance est le facteur le plus important. Le suivi de la localisation des smartphones était acceptable à condition qu'il soit mis en œuvre en tenant compte des intérêts de la communauté. Pour Kristie Bell, cela suscite de nombreuses questions. Quels sont les intérêts de la communauté qui doivent être prioritaires ? Ceux des personnes bien portantes ? Ceux des malades ? Ceux des travailleurs clés ? Ceux des individus immunisés ? Ceux des personnes qui ont récemment voyagé ? Ceux des « étrangers » ?<sup>36</sup>

La surveillance de masse est utilisée. Mais il existe des risques de dommages à long terme pour le tissu de la société, non seulement si la surveillance ne répond pas aux différents intérêts de la communauté ni ne les protège, mais aussi si les préoccupations morales ne sont pas prises en compte et maintenues, qu'elles soient fondées sur les principes de protection des données, les principes de liberté d'information ou l'autodétermination en matière d'information.

C'est pourquoi de nombreux militants de la protection de la vie privée ont exprimé leurs préoccupations liées aux mesures de surveillance autoritaires en réclamant une transparence totale.<sup>37</sup> En effet, les chercheurs du MIT énumèrent certaines questions concernant ces applications, afin de vérifier : 1) si les personnes les utilisent volontairement ; 2) s'il y a des limites à l'utilisation des données ; 3) si les données seront détruites après un certain temps ; 4) si la collecte de données est minimisée ; 5) si l'application ne collecte que les informations dont elle a besoin ; 6) si l'effort est transparent.

Le but et le temps d'utilisation de ces données sont d'une immense valeur. Il ne faut pas oublier le cas Cambridge Analytica. Au moyen d'une application intitulée « This is your digital life » – présentée sous la forme d'un questionnaire psychologique –, l'entreprise a utilisé des traces numériques dans le cadre de la campagne de Brexit et de l'élection présidentielle de Donald Trump.<sup>38</sup> En résumé, grâce aux données non autorisées des personnes, il a été possible d'identifier leurs comportements et, sur cette base, de chercher à influencer leurs décisions politiques. Le cas de Cambridge Analytica s'est imposé en reconnaissance du fait que le pouvoir de contrôle sur les données personnelles a des

<sup>34</sup> Ibid.

<sup>35</sup> Ibid.

<sup>36</sup> Ibid.

<sup>37</sup> Ibid.

<sup>38</sup> A. CASILLI, P. DEHAYE, J. SOUFRON. « Stopcovid est un projet désastreux piloté par des apprentis sorciers », *Le Monde*, 25 avril 2020, accessible à : [https://www.lemonde.fr/idees/article/2020/04/25/stopcovid-est-un-projet-desastreux-pilote-par-des-apprentis-sorciers\\_6037721\\_3232.html](https://www.lemonde.fr/idees/article/2020/04/25/stopcovid-est-un-projet-desastreux-pilote-par-des-apprentis-sorciers_6037721_3232.html).

conséquences directes sur la réalité.<sup>39</sup> En effet, même les données anonymes, qui sont présentées comme meilleures parce qu'elles n'établissent pas de relation directe avec la personnalité de la personne, sont en réalité envahissantes, parce que les données anonymes sont croisées avec d'autres données anonymes des mêmes personnes, ce qui établit finalement une double création parfaite de données pour l'exercice de la surveillance. Ces applications de surveillance correspondent à des modèles prédictifs, créés par abstraction au moyen d'algorithmes, grâce aux liens entre les êtres humains. Ces modèles consistent à enregistrer les relations quantifiées entre des paires de signaux. Les transmetteurs de signaux sont associés à une quantité qui mesure la probabilité que l'on soit porteur du virus<sup>40</sup>.

Par conséquent, l'une des critiques est que toutes les applications suivent les données disponibles dans les ordinateurs portables des personnes, ce qui, en fait, ne reflète pas la réalité. Cela signifie que les applications sont peu sûres, car leur base d'informations est fragile. En outre, la représentation numérique imparfaite des liens entre les êtres humains peut être enrichie ou croisée avec d'autres modèles et ainsi traiter les informations agrégées dans un tout autre but que la traque des virus<sup>41</sup>.

D'autre part, le système conduit à une diminution fondamentale des libertés individuelles : la liberté de circulation (en particulier entre les pays qui refusent d'avoir des systèmes de suivi ou qui prendront ce prétexte pour renforcer leur force), la liberté de travailler et aussi de se réunir ou d'avoir une vie privée<sup>42</sup>.

Ces questions sont vitales, non seulement pour la santé publique, mais aussi pour la justice publique, pour les droits et libertés et pour le bien commun, avertit l'auteur. Si des mesures extraordinaires sont prises pour lutter contre le Covid-19, il est primordial que l'utilisation des données personnelles à des fins de surveillance se fasse dans le respect de la loi et des droits des individus. En d'autres termes, d'autres valeurs doivent être prises en compte en plus de celles, très importantes, qui consistent à essayer de ralentir et d'arrêter une pandémie<sup>43</sup>.

La vie privée, les libertés civiles et les droits de l'homme sont des valeurs essentielles qui doivent être maintenues parallèlement à l'appel clair à la protection des vies, de la santé et du bien-être social. Il est donc essentiel que toutes les discussions sur la surveillance se déroulent de manière transparente et ouverte, avant que de nouvelles mesures ne soient mises en œuvre<sup>44</sup>.

<sup>39</sup> Ibid.

<sup>40</sup> LUNDI MATIN. « Stopcovid : Cybernétique, éthique et colégram », *Lundi matin* 242, par. 6, accessible à : <https://lundi.am/stopcovid-cybernetique-ethique-et-colegram>.

<sup>41</sup> Ibid.

<sup>42</sup> A. CASILLI, P. DEHAYE, J. SOUFRON, op.cit, p.1.

<sup>43</sup> D. LYON, « Cellphone Tracking Might Help Stamp Out Covid-19. But at What Cost? » op.cit., p.1.

<sup>44</sup> INTERNATIONAL CIVIL LIBERTIES MONITORING GROUP, *Joint Statement: Digital Surveillance Technologies and Covid-19 in Canada*, accessible à : <https://iclmg.ca/digital-surveillance-covid-19/>.

Pour que le contrôle nécessaire de la pandémie ne fasse pas fi des droits fondamentaux, les applications numériques de surveillance utilisées par les pays doivent établir des règles précises. Le type de poursuites et la technologie qui seront adoptés doivent être clairement délimités et soigneusement spécifiés. La manière dont ces données seront utilisées doit également être décrite dans la norme, ainsi que ses limites. En d'autres mots, il est essentiel que les données à utiliser et leurs objectifs soient énumérés, avec leurs motivations. Il n'est pas possible d'accepter l'utilisation d'une trace de données sans en expliquer la raison et en démontrer la nécessité.

Selon Cynthia Fleury, la défense des libertés publiques et individuelles est un héritage historique non négociable de l'État de droit. Le consentement des citoyens à la limitation de leurs droits est orienté vers un bien collectif, mais, pour elle, le concept de liberté négative, de protection de la sphère d'autonomie contre l'action de l'État, ne peut pas être complètement renoncé sous la conséquence de l'anéantissement de la liberté. Fleury affirme que le développement d'un outil numérique de surveillance épidémiologique est sans doute souhaitable, mais il doit être entouré de conditions<sup>45</sup>.

Les autorités compétentes pour l'utilisation des données doivent être clairement définies dans le protocole décrivant la situation d'urgence. La compétence de l'autorité est pertinente, car elle impose la garantie que l'utilisation éventuelle par un autre agent correspond à une violation de la compétence et donc que l'acte sera révoqué. L'imposition d'une amende pour déviation de la concurrence ou de la finalité doit être insérée dans la règle d'urgence. De plus, les données doivent être exclues. En d'autres termes, des protocoles et règlements spécifiques doivent prévoir l'obligation d'éliminer toutes les données ajoutées dans la situation d'urgence, afin d'empêcher qu'elles ne soient utilisées à d'autres fins.

L'utilisation des données ne peut être autorisée que pour l'usage spécifique limité à la pandémie. Toutes ces données doivent être exclues après avoir respecté les mesures de lutte contre la pandémie. Autrement dit, le moment auquel les données seront disponibles est pertinent, et la garantie de leur exclusion empêche leur utilisation ultérieure à d'autres fins. Le rapport entre l'utilisation et la finalité du projet et la manière dont les données sont traitées doit également être précisé.

L'utilisation des données des demandes pour d'autres activités non liées à la situation d'urgence ne peut pas être autorisée, qu'elles soient étatiques ou non étatiques. Ainsi, la réglementation relative à l'établissement des applications de suivi doit être attentive à : i) la délimitation précise du modèle utilisé ; ii) la

<sup>45</sup> C. FLEURY. « Nous sommes entrés dans une ère de “bien(sur)veillance” », *Le Monde*, 29 avril 2020, accessible à :

[https://www.lemonde.fr/m-perso/article/2020/04/29/cynthia-fleury-nous-sommes-entres-dans-une-ere-de-bien-sur-veillance\\_6038163\\_4497916.html](https://www.lemonde.fr/m-perso/article/2020/04/29/cynthia-fleury-nous-sommes-entres-dans-une-ere-de-bien-sur-veillance_6038163_4497916.html).

délimitation de la création des enregistrements de données ; iii) la délimitation des autorités compétentes pour l'utilisation des données et des applications ; iv) la délimitation de la période et de la finalité de l'application.

La surveillance contemporaine se fait à l'aide de la base de données dont la matière première n'est plus les sujets, ni les corps physiques, mais leurs données. Il est possible de contrôler efficacement les comportements afin d'influencer les personnes et les populations, d'anticiper et de prendre des risques.

L'admirable monde ancien dont la surveillance dépendait de la ville et de l'« apparence » de la surveillance pour la discipline des corps est supplanté. L'observation de visages, de corps, des personnes entières ne sont qu'un point de ce système hybride. La surveillance devient décentralisée, des compositions hybrides. Elle est ainsi un amalgame de technologie et d'information sur les corps, une Personne 2.0. Elle se transmet de l'espace matériel au cyberspace, ce qui implique un remplacement du modèle panoptique de l'apparence par la surproduction en ligne de données et une circulation accrue des images<sup>46</sup>.

Grâce aux données collectées dans ces applications, les individus ont subi des restrictions au droit d'aller et venir, comme en Chine, où les résultats des données collectées ont donné lieu à l'attribution d'un code QR qui autorise ou non la circulation dans certains lieux. Le fait est que la surveillance et le contrôle ont été exercés non pas sur le corps physique des personnes, mais sur leurs données collectées, associées à d'autres données disponibles, ce qui ne correspondait pas à la réalité offline. De cette manière, ceux qui avaient un code QR orange ne pouvaient même pas quitter leurs résidences parce qu'ils avaient été dans un endroit où une personne contaminée s'était rendue aussi. Ils n'avaient pas nécessairement été contaminés. Ils n'avaient pas forcément eu de contact avec quelqu'un contaminé. Cela signifie donc qu'une personne en bonne santé a été empêchée de circuler librement dans la rue parce que la collecte et l'enregistrement des données indiquaient de manière erronée une maladie qu'elle n'avait pas.

Autrement dit, avec la transformation du monde analogique en monde numérique, la surveillance commence à se faire par le biais des données et non des personnes. Bien que les corps physiques fassent l'objet d'un contrôle et d'une surveillance (par le biais de caméras, de reconnaissance faciale, de drones, entre autres), ils sont en fin de compte considérés comme des données couplées à d'autres données de manière automatique par des algorithmes de calcul.

Ces faisceaux et flux de contrôle peuvent être exercés par plusieurs acteurs. En effet, la matière première de la surveillance est constituée d'abord de données et, grâce à elles, de personnes aussi. Les personnes sont transformées non seulement en chiffres, mais aussi en chiffres dupliqués, enregistrés et reproduits qui

---

<sup>46</sup> A. Viana, « Vigilâncias híbridas », op.cit, p. 20.

servent de matériel pour établir la prédiction de la volonté des gens, l'anticipation de leurs goûts et la manipulation de leurs choix. L'individu, en fin de compte, est conditionné par l'algorithme grâce à des chiffres aléatoires. Le pouvoir, par conséquent, dépend largement de la maîtrise des données et de la possession d'algorithmes sophistiqués et efficaces.

## CONCLUSION

Au début de la pandémie, Giorgio Agamben a souligné, à travers la pensée de Foucault, que les gouvernements de sécurité ne travaillaient pas nécessairement en produisant l'urgence, mais en l'exploitant et en la dirigeant lorsqu'elle se produisait : pour un gouvernement totalitaire comme celui de la Chine, pour l'auteur, l'épidémie avait été le moyen parfait de tester la possibilité d'isoler et de contrôler toute une région<sup>47</sup>.

La surveillance n'existe pas seulement en Chine, avertit M. Agamben, et l'omniprésence des contrôles peut être pire que les totalitarismes. On passe à l'État de surveillance, c'est-à-dire un État dans lequel, pour des raisons de sécurité (ou de santé publique), des limites sont imposées aux libertés individuelles<sup>48</sup>.

C'est exactement ce qui se passe en ce moment à cause du Covid-19. Ce qui serait une situation d'urgence est devenu une pratique courante, en raison du prolongement de la pandémie et des exigences en matière de contrôle sanitaire. Les libertés des personnes sont limitées de toutes les façons. Ce sont les droits d'aller et venir qui sont limités. C'est le droit au travail, à remplir une fonction sociale qui est également entravé.

Tous ces contrôles se font sur la base de nouvelles technologies. Pour tout cela, la surveillance se fait de toutes les manières, avec un mélange de pouvoir disciplinaire, de pouvoir biologique et d'éléments de surveillance des données. Les personnes et leurs données sont constamment surveillées.

En 2020, l'État de droit a été remplacé par l'État de surveillance.

---

<sup>47</sup> G. AGAMBEN. « L'épidémie montre clairement que l'état d'exception est devenu la condition normale », *Le Monde*, 24 mars 2020, accessible à : [https://www.lemonde.fr/idees/article/2020/03/24/giorgio-agamben-l-epidemie-montre-clairement-que-l-etat-d-exception-est-devenu-la-condition-normale\\_6034245\\_3232.html](https://www.lemonde.fr/idees/article/2020/03/24/giorgio-agamben-l-epidemie-montre-clairement-que-l-etat-d-exception-est-devenu-la-condition-normale_6034245_3232.html).

<sup>48</sup> G. AGAMBEN. « Nouvelles réflexions », *Lundi matin*, accessible à : <https://lundi.am/nouvelles-reflexions>.