



## LE LÉVIATHAN NUMÉRIQUE : L'ALLIANCE ÉTAT-CORPORATIONS TECHNOLOGIQUES [IM.UQAM.CA](http://IM.UQAM.CA) ET SA RÉSISTANCE AU CADRE DES DROITS DE L'HOMME

Regards de l'IEIM par Yeison Grisales Garcia | Février 2026

### Introduction

Vous est-il déjà arrivé d'ouvrir une application de réseaux sociaux et d'y voir apparaître une publicité étrangement précise, correspondant exactement à une conversation récente ou à une pensée fugace ? Avez-vous déjà eu l'impression que votre téléphone « vous écoutait » ? Vous publiez une photo de voyage à l'étranger, et quelques jours plus tard, un proche qui a donné un « like » vous raconte avoir été soumis à un contrôle minutieux à la frontière. Ces expériences, autrefois perçues comme anecdotiques, sont devenues des éléments ordinaires de la vie contemporaine. Elles révèlent une réalité plus profonde : chaque clic, chaque déplacement, chaque interaction numérique alimente une infrastructure de surveillance d'une ampleur sans précédent.

*« Cet essai analyse comment nos activités en ligne alimentent une surveillance de masse issue d'une alliance structurelle entre les États et les grandes entreprises technologiques. Il soutient que cette alliance forme un « Léviathan numérique », un pouvoir hybride qui reconfigure/contourne les limites des droits de l'homme, et plaide pour faire de la défense de la vie privée et de l'autonomie un enjeu politique central.*

Contrairement à l'image classique d'un État omniscient incarné par un « Big Brother » unique, cette surveillance ne relève plus d'un centre de pouvoir isolé. Elle est le produit d'une alliance structurelle entre les États et les grandes entreprises technologiques, alliance souvent opaque, mais extraordinairement efficace.

Sous les discours rassurants de la sécurité nationale, de la personnalisation des services ou de l'innovation économique se cache l'une des transformations les plus significatives du

pouvoir politique au XXI<sup>e</sup> siècle. Cet article soutient que cette coopération n'est ni accidentelle ni marginale : elle constitue une stratégie coordonnée de résistance du pouvoir face aux limites imposées par le droit international des droits de l'homme, les constitutions libérales et les mécanismes démocratiques de contrôle.

Dans cet article, le « Léviathan numérique » désigne une forme contemporaine de pouvoir hybride, issue de l'alliance durable entre les États et les grandes corporations

technologiques. Ce pouvoir combine la capacité coercitive et juridique de l'État avec l'infrastructure numérique, les données massives et les logiques économiques du capitalisme de surveillance. À la différence du Léviathan hobbesien classique, centralisé et exclusivement étatique, le Léviathan numérique est distribué, opaque et inscrit dans l'architecture du code, ce qui lui permet d'exercer une surveillance continue, souvent invisible, sur les individus et les populations<sup>1</sup>.

À travers les apports de Shoshana Zuboff, Lawrence Lessig, Michel Foucault et plusieurs théories contemporaines de la science politique, cet article analyse comment cette alliance reconfigure la souveraineté, fragilise la vie privée, et altère les fondements mêmes du contrat social démocratique. Il ne s'agit pas d'un débat strictement technologique : c'est l'un des débats politiques centraux de notre époque.

## 1. Cadre théorique : comprendre le pouvoir à l'ère numérique

Pour analyser le Léviathan numérique, il est nécessaire de mobiliser un cadre interdisciplinaire permettant de saisir à la fois les logiques politiques, juridiques et économiques de la surveillance contemporaine.

### 1.1 L'État, la sécurité et la maximisation du pouvoir

En science politique, les approches réalistes offrent une première clé de lecture. Kenneth Waltz et John Mearsheimer rappellent que, dans un système international dépourvu d'autorité centrale, les États cherchent rationnellement à maximiser leur puissance afin d'assurer leur survie<sup>2</sup>. À l'ère numérique, cette quête de puissance ne se limite plus aux domaines militaire ou économique: elle s'étend au contrôle des flux d'information et des données.

Dans cette perspective, l'alliance avec les grandes entreprises technologiques apparaît comme une stratégie rationnelle. Ces acteurs privés possèdent les infrastructures, les plateformes et les données indispensables à l'exercice du pouvoir dans le cyberspace. La sécurité nationale devient alors l'argument central justifiant l'expansion de la surveillance et la restriction des droits individuels.

### 1.2 La sécuritisation: transformer l'exception en norme

La théorie de la sécuritisation développée par Barry Buzan et Ole Wæver permet de comprendre comment cette expansion est légitimée<sup>3</sup>. Un enjeu devient une « question

<sup>1</sup> M. FOUCAULT, *Surveiller et punir. Naissance de la prison*, Paris, Gallimard, 1975.

<sup>2</sup> K. N. WALTZ, *Man, the State, and War A Theoretical Analysis*, New York, Columbia University Press, 1959.; J. J. MEARSHEIMER, *The Tragedy of Great Power Politics*, New York, W. W. Norton, 2001.

<sup>3</sup> B. BUZAN, O. WÆVER et J. DE WILDE, *Security: A New Framework for Analysis*, Boulder, Lynne Rienner, 1998.

de sécurité » lorsqu'il est présenté comme une menace existentielle nécessitant des mesures exceptionnelles. Terrorisme, cybercriminalité ou désinformation sont ainsi mobilisés pour justifier des dispositifs de surveillance massive, souvent en dehors des cadres juridiques ordinaires.

La sécuritisation fonctionne comme un rituel de légitimation: elle transforme des atteintes graves aux droits fondamentaux en réponses présentées comme nécessaires et inévitables.

### 1.3 Biopouvoir et gouvernementalité numérique

Michel Foucault offre une perspective essentielle pour comprendre la nature de ce pouvoir. Dans les sociétés modernes, le pouvoir ne s'exerce plus principalement par la violence spectaculaire, mais par des mécanismes de biopouvoir et de gouvernementalité, qui administrent les populations en agissant sur leurs comportements<sup>4</sup>.

### 1.4 Le code comme forme de régulation

Cette dynamique serait impossible sans l'infrastructure technique qui la soutient. Lawrence Lessig a montré que, dans le cyberspace, « le code fait loi ». L'architecture des logiciels, des plateformes et des réseaux régulent les comportements aussi efficacement que les normes juridiques traditionnelles<sup>5</sup>.

*« La surveillance numérique constitue aujourd'hui l'expression la plus aboutie de ce biopouvoir. En collectant, analysant et exploitant les données personnelles, les États et les entreprises orientent les conduites, classent les individus et anticipent leurs actions, souvent sans qu'ils en aient conscience. »*

Or, ce code est majoritairement conçu et contrôlé par des entreprises privées. Les choix techniques, collecte massive de données, absence de chiffrement par défaut, interfaces manipulatrices, constituent autant de décisions politiques déguisées en nécessités techniques.

### 1.5 La vie privée comme droit de pouvoir

Enfin, Carissa Véliz rappelle que la vie privée n'est pas un luxe ni une préférence individuelle, mais un droit fondamental de protection contre les abus de pouvoir<sup>6</sup>. Sa violation systématique menace l'autonomie individuelle, l'égalité et le fonctionnement même de la démocratie. Ce cadre normatif est indispensable pour évaluer le Léviathan

<sup>4</sup> M. FOUCAULT, Histoire de la sexualité, vol. 1 : La volonté de savoir, Paris, Gallimard, 1976.

<sup>5</sup> L. LESSIG, Code: Version 2.0, New York, Basic Books, 2006.

<sup>6</sup> C. VÉLIZ Privacy Is Power: Why and How You Should Take Back Control of Your Data, London, Bantam Press, 2020.

numérique non seulement comme un fait politique, mais comme une atteinte profonde aux droits humains.

## 2. L'anatomie de l'alliance État-corporations

L'alliance entre États et entreprises technologiques se matérialise à travers des mécanismes concrets, juridiques et économiques, qui rendent la surveillance de masse à la fois légale, rentable et difficilement contestable.

### 2.1 Le droit comme instrument de reconfiguration

Les États jouent un rôle central dans la création de cadres juridiques permissifs. Des législations comme la section 702 du Foreign Intelligence Surveillance Act aux États-Unis autorisent la surveillance massive de communications sans mandat individuel, sous prétexte de sécurité nationale<sup>7</sup>. Ces dispositifs externalisent la surveillance vers les entreprises privées, qui sont légalement contraintes de coopérer tout en bénéficiant d'une immunité juridique. Le droit n'est pas suspendu: il est reconfiguré afin de rendre acceptable ce qui serait autrement incompatible avec les droits fondamentaux.

### 2.2 La logique économique du capitalisme de surveillance

Du côté des entreprises, Shoshana Zuboff décrit un modèle économique fondé sur l'extraction des données comportementales<sup>8</sup>. L'expérience humaine est transformée en matière première, puis en produits de prédiction commercialisés sur des marchés spécialisés.

Les États sont devenus des clients majeurs de ce capitalisme de surveillance. Ils achètent des données, utilisent des outils d'analyse prédictive ou exploitent les infrastructures privées pour suivre des populations entières. La logique économique et la logique sécuritaire se rejoignent et se renforcent mutuellement.

### 2.3 Technologies de contrôle et biopouvoir numérique

Les technologies de reconnaissance faciale illustrent parfaitement cette symbiose. Développées par des entreprises privées, elles sont déployées par les forces de l'ordre et les agences frontalières, souvent sans cadre réglementaire clair<sup>9</sup>. Elles permettent un contrôle automatisé des corps et des déplacements, prolongeant le biopouvoir foucauldien dans l'espace numérique.

---

<sup>7</sup> Foreign Intelligence Surveillance Act Amendments Act, 50 U.S.C. § 1881a (2008)

<sup>8</sup> S. ZUBOFF, *The Age of Surveillance Capitalism*, New York, PublicAffairs, 2019.

<sup>9</sup> K. HILL, « The Secretive Company That Might End Privacy as We Know It », *The New York Times*, 18 janvier 2020.

### 3. Une résistance venue d'en haut : l'architecture de l'impunité

L'alliance État-corporations ne se contente pas d'exercer le pouvoir: elle résiste activement aux limites que les droits de l'homme tentaient d'imposer.

#### 3.1 Sécuritisation et normalisation de l'exception

La sécuritisation transforme la surveillance de masse en norme juridique. Les juridictions, confrontées à des arguments fondés sur la sécurité nationale, acceptent

*« La bataille pour les droits humains du XXI<sup>e</sup> siècle se joue désormais dans le droit, dans la technologie et dans les choix collectifs que nous faisons quant au futur numérique que nous souhaitons habiter. »*

souvent le principe de la surveillance tout en se contentant d'exiger des garanties procédurales minimales<sup>10</sup>. Cette normalisation de l'exception vide les droits fondamentaux de leur substance: la violation devient une question technique, non plus un problème de principe.

#### 3.2 Le code comme architecture de l'impunité

Parallèlement, l'impunité est intégrée dans l'architecture technique elle-même. Les plateformes sont conçues pour maximiser la collecte de données, limiter la transparence et décourager les choix favorables à la vie privée<sup>11</sup>. Cette régulation par le code est souvent invisible, mais redoutablement efficace.

#### 3.3 Une souveraineté déformée

Cette dynamique transforme profondément le contrat social. Les citoyens ne cèdent plus une part limitée de liberté à l'État: ils abandonnent l'ensemble de leur vie numérique à un réseau hybride d'acteurs publics et privés, largement soustrait au contrôle démocratique.

## 4. Implications et perspectives

Si ces tendances se poursuivent, l'avenir risque d'être marqué par une surveillance prédictive permanente, où les comportements sont anticipés, classés et neutralisés avant même qu'ils ne se manifestent. Les biais algorithmiques risquent d'amplifier les discriminations, créant des citoyens numériques de première et de seconde zone.

<sup>10</sup> CEDH, Big Brother Watch et autres c. Royaume-Uni, 2018.

<sup>11</sup> L. LESSIG, op. cit.

Dans un tel contexte, la capacité de résistance démocratique est fragilisée: s'organiser, communiquer et contester devient de plus en plus difficile sous un regard constant.

Pourtant, l'horizon n'est pas figé. Des cadres juridiques comme le RGPD, le principe de « *privacy by design* » et le développement de technologies respectueuses de la vie privée montrent qu'une autre trajectoire est possible. Comme le souligne Lessig, le choix du code est un choix politique<sup>12</sup>.

## Conclusion

L'analyse démontre que le Léviathan numérique n'est pas une dérive accidentelle, mais le produit d'une alliance stratégique entre États et corporations technologiques. En combinant sécurité nationale, capitalisme de surveillance et architecture du code, cette alliance a construit un pouvoir hybride capable de contourner et de neutraliser les limites imposées par les droits de l'homme.

Face à ce pouvoir, la défense de la vie privée et de l'autonomie humaine ne relève pas d'une nostalgie analogique, mais d'un impératif politique majeur. La bataille pour les droits humains du XXI<sup>e</sup> siècle se joue désormais dans le droit, dans la technologie et dans les choix collectifs que nous faisons quant au futur numérique que nous souhaitons habiter.

Le temps est venu de décider si le code et la loi serviront la liberté ou la surveillance.

---

<sup>12</sup> Ibid

## Références

### Législation

*Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008*, 50 USC § 1881a (2008). (Loi américaine sur la surveillance du renseignement étranger – Amendements de 2008).

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données – RGPD), [2016] JO L 119/1.

### Jurisprudence

Big Brother Watch et autres c. Royaume-Uni, [2018] CEDH 741 (Cour européenne des droits de l'homme).

In re National Security Agency Telecommunications Records Litigation, 700 F Supp 2d 1182 (ND Cal 2010).

### Ouvrages

FOUCAULT, Michel. Histoire de la sexualité, vol. 1 : La volonté de savoir, trad. Ulises Guiñazú (Mexico : Siglo XXI Éditeurs, 2019).

FOUCAULT, Michel. Surveiller et punir : Naissance de la prison, trad. Aurelio Garzón del Camino (Mexico : Siglo XXI Éditeurs, 2009).

GREENWALD, Glenn. Nulle part où se cacher : Edward Snowden, la NSA et l'État de surveillance américain (New York : Metropolitan Books, 2014).

LESSIG, Lawrence. Code : Version 2.0 (New York : Basic Books, 2006).

MEARSHEIMER, John J.. La tragédie des grandes puissances (New York : W.W. Norton & Company, 2001).

VÉLIZ, Carissa. La vie privée est un pouvoir : pourquoi et comment reprendre le contrôle de vos données (Londres : Bantam Press, 2020).

WALTZ, Kenneth N.. L'Homme, l'État et la guerre : une analyse théorique (New York : Columbia University Press, 2001).

## Auteur

**Grisales Garcia Yeison** est candidat à la maîtrise en droit international et politique internationale à l'Université du Québec à Montréal (UQAM). Ses intérêts de recherche portent principalement sur la transformation de la souveraineté étatique à l'ère numérique, la gouvernance globale des technologies, les rapports entre États, acteurs corporatifs et organisations internationales, ainsi que les impacts des technologies numériques sur les droits fondamentaux et le droit international des droits de l'homme.

*Ce texte a été retenu dans le cadre de l'appel à propositions 2025-2026 de l'Institut d'études internationales de Montréal sur le thème des alliances et des résistances.*

*Les articles publiés n'engagent que leurs auteurs ou autrices et ne reflètent pas nécessairement les points de vue de l'IEIM, ni ceux de ses membres et partenaires.*

Institut d'études internationales de Montréal

Université du Québec à Montréal

400, rue Sainte-Catherine Est

Bureau A-1540, Pavillon Hubert-Aquin

Montréal (Québec) H2L 3C5

514 987-3667

[ieim@uqam.ca](mailto:ieim@uqam.ca)

[www.ieim.uqam.ca](http://www.ieim.uqam.ca)

**UQAM**



**Institut d'études  
internationales  
de Montréal**