



Ligue des
droits et libertés

Droits et libertés

Le capitalisme de surveillance

Menaces à la démocratie et aux droits!



- Une crise pour les démocraties
- La ville intelligente, qu'ossa donne?
- Quelles réponses, quelles ripostes?

Fondée en 1963, la Ligue des droits et libertés (LDL) est un organisme sans but lucratif, indépendant et non partisan, issu de la société civile québécoise et affilié à la Fédération internationale pour les droits humains (FIDH). Elle vise à faire connaître, à défendre et à promouvoir l'universalité, l'indivisibilité et l'interdépendance des droits reconnus dans la *Charte internationale des droits de l'Homme*.

Collaboration à ce numéro

Michelle Albert-Rochette
Yannick Baumann
Jean Claude Bernheim
Jacob Boivin
Mélina Chasles
Simone Chen
Lise Chovino
Silviana Cocan
Julie Desrosiers
Elisabeth Dupuis
Martine Éloy
Montserrat Emperador
Badimon
Nicole Filion
Maxim Fortin
Véronique Fortin
Pierre-Louis Fortin-Legris
Delphine Gauthier-Boileau
Laurence Grondin-Robillard
Emanuel Guay
Pierre Henrichon
Marie-Pier Jolicoeur
Lynda Khelil
Eve-Marie Lacasse
Normand Landry
Stéphane Leman-Langlois
Anne-Sophie Letellier
Mélania Martel
Stéphanie Mayer
Gérald McKenzie
Tim McSorley
Cynthia Morinville
Lyne Nantel
Dominique Peschard
Anne Pineau
Alessandra Renzi
Catherine St-Arnaud-Babin
Fatima Gabriela Salazar
Gomez
Sepideh Shahamati
Rémy-Paulin Twahirwa
Tamara Vukov
Shoshana Zuboff

Comité de rédaction

Silviana Cocan
Elisabeth Dupuis
Martine Éloy
Lynda Khelil
Stéphane Leman-Langlois
Stéphanie Mayer
Dominique Peschard
Alexandra Pierre
Anne Pineau
Fatima Gabriela Salazar
Gomez

Révision linguistique

Marcel Duhaime
Carmen Fontaine
Claire Lalande
Alexia Leclerc

Traduction

Dominique Lemoine

Correction d'épreuves

Elisabeth Dupuis
Lynda Khelil
Karina Toupin

Illustration de

la page couverture

Chloloula

Crédits photos

AK Rockefeller
André Querry
Arturo Castaneyra
ev
Scott Rodgerson
TheeErin

Impression

Katasoho
www.katasoho.com

Sauf indication contraire, les propos et opinions exprimés appartiennent aux auteurs et autrices et n'engagent ni la Ligue des droits et libertés, ni la Fondation Léo-Cormier.

La reproduction totale ou partielle est permise et encouragée, à condition de mentionner la source.

Revue de la Ligue des droits et libertés

Volume 41, numéro 1, printemps / été 2022

Dépôt légal

Bibliothèque nationale du Québec
Bibliothèque nationale du Canada
ISSN 2564-5099

Cette revue est une publication de la Ligue des droits et libertés, réalisée avec l'appui financier de la Fondation Léo-Cormier. Elle est distribuée à leurs membres et est disponible sur commande et en ligne.



Ligue des
droits et libertés



FONDATION LÉO-CORMIER
pour l'éducation aux droits et libertés

Dans ce numéro

Éditorial

- 3... Les deux années de pandémie n'auront pas été une école de la démocratie
Stéphanie Mayer

6... Hommage à Lucie Lemonde

Collectif de militant-e-s de la Ligue des droits et libertés

Un monde sous surveillance

- 10... Les dangers de la lutte contre les méfaits en ligne
Tim McSorley

Ailleurs dans le monde

- 12... Le sel de la Terre
Rémy-Paulin Twahirwa

Un monde de lecture

- 51... Pour une lucidité collective vis-à-vis des GAFAM
Delphine Gauthier-Boileau

Le monde de Québec

- 53... Retour sur la crise au Service de police de la Ville de Québec
Mélina Chasles et Maxim Fortin

Le monde de l'environnement

- 56... Les ficelles du capitalisme de surveillance
Cynthia Morinville

Dossier : Le capitalisme de surveillance : menaces à la démocratie et aux droits!

- 14... Présentation
Elisabeth Dupuis

État des lieux

- 15... Une crise pour les démocraties
Shoshana Zuboff
- 21... Lexique du capitalisme de surveillance
Martine Éloy
- 22... À la lumière du droit international des droits de la personne
Silviana Cocan
- 24... Une culture de surveillance
Stéphane Leman-Langlois
- 26... Pas de quoi contrecarrer le modèle d'affaires des GAFAM
Anne Pineau

Discriminations et exclusions

- 28... Forces policières et capitalisme de surveillance
Dominique Peschard
- 31... Le secteur de l'intelligence artificielle et l'embourgeoisement de Parc-Extension
Collectif de chercheur-euse-s et militant-e-s
- 34... La ville intelligente : Qu'ossa donne?
Entrevue avec Lyne Nantel par Martine Éloy et Dominique Peschard
- 37... La dissolution de la société dans le capitalisme de surveillance
Jacob Boivin et Laurence Grondin-Robillard
- 40... Le capitalisme de surveillance like la fracture numérique
Lise Chovino et Catherine St-Arnaud-Babin

Perspectives et alternatives

- 42... Quelles réponses, quelles ripostes?
Pierre Henrichon
- 44... Renforcement de la vie privée et éthique du design numérique
Michelle Albert-Rochette et Marie-Pier Jolicoeur
- 47... Mobilisations et médias sociaux : quelles opportunités et quels enjeux?
Anne-Sophie Letellier et Normand Landry
- 49... Quelle place pour le droit de dire non à l'intelligence artificielle?
Entrevue avec Fatima Gabriela Salazar Gomez par Lynda Khelil

Éditorial

Les deux années de pandémie n'auront pas été une école de la démocratie

Stéphanie Mayer, Ph. D., enseignante de science politique au Cégep, vice-présidente de la Ligue des droits et libertés

Pour les fins de la mémoire collective, il importe de rappeler quelques pans de l'histoire pandémique des derniers mois. En vertu de la *Loi sur la santé publique* du Québec, le gouvernement de la Coalition Avenir Québec (CAQ), par la voix du premier ministre François Legault, a déclaré le 13 mars 2020, l'état d'urgence sanitaire (EUS) dès les premiers moments de la pandémie de la COVID-19. Notons que l'EUS est une disposition exceptionnelle qui permet à l'État d'agir en contexte d'urgence, c'est-à-dire lors d'une situation extraordinaire qui demande une attention immédiate. Dans de telles circonstances, tous et chacun-e a la juste attente que le gouvernement y apporte toute son attention par-delà la partisanerie. De plus, très peu contestent qu'une fois la COVID-19 déclarée mondiale, il y avait urgence d'agir, ni la part d'improvisation que cette pandémie impliquait. Selon la Ligue des droits et libertés (LDL), cette situation n'excuse pas les dérapages et les violations de droits humains auxquels sa gestion a donné lieu (pensons aux couvre-feux, aux nombreux constats d'infraction, à la limitation du droit de manifester, au déni de droits aux personnes itinérantes ou incarcérées).

Banalisation de l'état d'urgence sanitaire et les tendances autoritaires de la CAQ

Deux ans plus tard, après des ressacs et des vagues de contagion ainsi que des variations sur les mesures populationnelles, l'EUS est encore en place, ayant été renouvelé 113 fois en date du 18 mai 2022, aux 10 jours environ comme le permet la loi, sans consulter les parlementaires. Pour la LDL, il est devenu évident que le gouvernement s'accommode bien des pouvoirs conférés par cette loi, qu'il considère les consultations citoyennes et les débats démocratiques comme du sable dans l'engrenage de sa gestion de la pandémie. Plusieurs des ténors de la CAQ – son chef a fortiori – agissent comme des chef-fe-s d'entreprises ou des pères de famille alliant autoritarisme et paternalisme – par chance, le discours guerrier contre la COVID-19 ne nous a pas été resservi. On nous a demandé d'être dociles, de respecter les consignes, de se faire vacciner, d'être patient-e-s. Notre confiance comme un chèque en blanc : on ne nous a jamais demandé notre avis directement ou si peu, indirectement par le truchement des élu-e-s au Parlement à Québec.

Sans nier le caractère extraordinaire de la pandémie, des voix se sont élevées depuis plus d'un an pour exiger la fin de l'EUS et le rétablissement des débats parlementaires à l'Assemblée nationale (AN). D'ailleurs, une campagne à l'initiative de la LDL a été lancée en mai 2021, appuyée par 128 organisations de divers horizons, pour réclamer la fin de l'état d'urgence au Québec. Malgré le soutien manifesté à l'endroit de notre campagne, il faut rappeler combien il était – et il demeure – difficile de formuler un discours critique à l'encontre des mesures du gouvernement sans se voir délégitimer ou reléguer à la posture fourre-tout de complotistes ou d'antivaccins. Plus encore il a fallu – et il faut encore – user d'une imagination communicationnelle pour susciter un peu d'indignation à l'égard du maintien banalisé de l'EUS. Or, il nous semble que ce dernier soit une normalisation d'une gestion autoritaire des questions sociales par le gouvernement et une perte évidente de pratiques démocratiques.

Notre confiance comme un chèque en blanc : on ne nous a jamais demandé notre avis directement ou si peu, indirectement par le truchement des élu-e-s au Parlement à Québec.



Crédit : André Querry

« Fausse levée de l'état d'urgence sanitaire » : le projet de loi 28 est une illusion

Affirmer que le gouvernement de CAQ apprécie les pouvoirs conférés par l'EUS et qu'il y trouve son confort serait un euphémisme comme en atteste le PL 28 – *Loi visant à mettre fin à l'état d'urgence* – déposé le 31 mars 2022 par le ministre de la Santé et des Services sociaux, Christian Dubé. On aurait tort de faire confiance au titre, car le PL 28 ne vise pas dans les faits à mettre fin à l'EUS; au contraire, il le prolonge. En l'état, le PL 28 permet au gouvernement de se prévaloir de différents pouvoirs discrétionnaires (résultant de décrets, mesures et arrêtés adoptés sous l'état d'urgence sans consultation parlementaire), jusqu'au 31 décembre 2022. La LDL n'a pas raté l'occasion d'aller devant la Commission de la Santé et des Services sociaux du Québec, le 6 avril 2022, pour dénoncer ce qui nous semble une aberration en termes de droits humains et de pratiques démocratiques.

La LDL devant la Commission s'est exprimée en ces termes :

À vrai dire, le PL 28 propose une sortie progressive de l'état d'urgence afin de prolonger les mesures d'urgence qui avantagent et protègent le gouvernement et non la population. [Si le PL 28 est adopté, il aura] pour effet de maintenir un droit des rapports collectifs de travail d'exception dans les domaines de la santé et de l'éducation en conférant [au gouvernement] la noblesse d'un vote de l'Assemblée nationale. [Si le PL 28 est adopté, il] n'absout en rien deux années de gestion autoritaire et ne corrige d'aucune façon l'absence de débats ou de mécanismes consultatifs ayant entouré l'adoption effrénée d'une pléthore de décrets et d'arrêtés ministériels depuis mars 2020 (Mémoire de la LDL, avril 2022)¹.

Si le PL 28 est adopté à l'AN, ce sera parmi les premiers véritables débats parlementaires et probablement l'un des derniers, au sujet la gestion de la pandémie par le gouvernement de la CAQ, en raison de l'imminence du déclenchement des élections provinciales. Dans le parlementarisme québécois et devant un gouvernement majoritaire, le rôle conféré aux partis de l'opposition dans notre démocratie représentative reste réduit et depuis deux ans, quasiment nul. À ce titre, rappelons que François Legault s'est fait élire en promettant de réformer le mode de scrutin et que le PL 39 – *Loi établissant un nouveau mode de scrutin* – a été abandonné, lequel envisageait de mettre en place un mode de scrutin proportionnel avec compensation régionale. Le maintien de l'EUS a permis de mettre hors champ des débats parlementaires la question de la gestion par la CAQ de la pandémie et plus largement, celle de la santé et de son système public affaibli par des années de politiques néolibérales.

Il ne faut pas être dupes du calendrier électoral automnal! Il est quasiment impossible que le ministre Dubé rende des comptes de sa gestion des deux dernières années devant l'AN dans les délais prévus par la *Loi sur la santé publique* du Québec avant que la chambre ne soit dissoute et les élections déclenchées. En d'autres mots, le gouvernement tente, avant les élections, d'avoir l'assentiment des parlementaires pour se laver les mains de toute reddition de compte concernant la gestion pandémique et de ses abus avérés de la disposition de l'EUS.

1. En ligne : <https://liguedesdroits.ca/memoire-le-pl-28-est-une-illusion-letat-durgence-continue/>

Prendre soin de nos solidarités pour lutter et faire société

Face à tous les gouvernements et plus particulièrement lorsqu'il se révèle être si ouvertement favorable à des politiques publiques d'austérité et lorsqu'il adopte des pratiques autoritaires de gestion de la population, comme c'est le cas pour la CAQ, les titulaires des droits – c'est-à-dire nous – ont le besoin voire le devoir d'être solidaires et organisé-e-s pour remettre les autorités face à leurs devoirs en termes de droits humains et de pratiques démocratiques, pour exposer nos vues sur l'immédiat et l'avenir.

Or, le maintien sur la durée de l'EUS illustre notre lente accoutumance à la gestion bureaucratique et autoritaire du social : ce qui est à l'antipode d'une école de la démocratie. Si le néolibéralisme altère subtilement les relations sociales, nous soumettant à des logiques de performance et de compétition mutuelle, la pandémie de la COVID-19 aura, pour sa part, exacerbé ce mouvement de manière pernicieuse en faisant des autres des dangers : des transmetteurs de la maladie. Le spectre de la contagion affectera durablement nos manières d'interagir, de s'approcher, de se soutenir, d'être ensemble, de s'aimer, de s'entraider... L'individualisme, l'isolement et la peur d'être contaminé-e-s par les autres ont mis à rude épreuve nos solidarités, des conditions qui laissent le champ libre à des gouvernements peu démocratiques.

Les titulaires des droits – c'est-à-dire nous – ont le besoin voire le devoir d'être solidaires et organisé-e-s pour remettre les autorités face à leurs devoirs en termes de droits humains et de pratiques démocratiques, pour exposer nos vues sur l'immédiat et l'avenir.

Saviez-vous que la Ligue des droits et libertés fêtera en 2023 son 60^e anniversaire? Le contexte nous force à admettre que la défense collective des droits humains et leur réalisation reste tributaire des mobilisations sociales. La pandémie de la COVID-19 aura brutalement rappelé la précarité structurelle des droits sociaux au Québec (par exemple : la santé, l'éducation, le logement, la culture, le travail) et pour la réalisation pleine et entière des droits humains, leur interdépendance demeure une condition. Alors que l'avenir est incertain, les luttes en faveur des droits humains devraient être un lieu de convergence afin que la société soit plus juste, inclusive et solidaire. Heureusement, le calendrier des activités du 60^e anniversaire de la LDL permettra, entre autres, de prendre la mesure des luttes sociales et politiques conduites depuis 1963 et celles qui nous attendent collectivement, voilà déjà une belle manière de prendre soin de nos solidarités pour continuer à faire société.



Hommage à Lucie Lemonde



Lucie Lemonde, qui nous a quitté-e-s le 6 février 2022, a marqué d'innombrables militant-e-s des droits humains au Québec et ailleurs, d'étudiant-e-s en droit ainsi que des confrères et consoeurs universitaires et dans le monde juridique.

Les témoignages de militant-e-s de la Ligue des droits et libertés, publiés dans ces pages, nous font découvrir une femme aux multiples facettes, une femme et une militante exceptionnelle.

Lucie et la justice sociale

Lucie a joué à la Ligue des droits et libertés (LDL) un rôle central dans de multiples dossiers en faveur de la liberté d'expression et du droit de manifester. Travaillant toujours en étroite collaboration avec les militant-e-s, elle a porté la voix de la LDL, dans l'espace public, auprès des autorités politiques ainsi que devant différentes instances internationales.

Dans le dossier des poursuites-bâillons, elle ne s'est pas contentée de l'adoption des dispositions visant à contrer ce type de poursuites. Elle s'est lancée dans une tournée à la grandeur du Québec, visant à en faire connaître la portée et surtout à renforcer la volonté et la capacité de groupes de citoyen-ne-s à mener dans l'espace public les débats et les luttes autour de divers enjeux de justice sociale. Plus récemment, elle a été l'initiatrice du projet *Entraves à la liberté d'expression : les règlements municipaux sous la loupe*, qui s'avère être un outil très efficace de revalorisation de l'exercice du droit de manifester collectivement.

Lucie a aussi été au cœur du dossier concernant les conditions de détention et la violation des droits des femmes incarcérées à l'établissement Leclerc. Ses interventions ont su rejoindre des pans de la population traditionnellement peu sensibles à la question des droits des détenu-e-s, suscitant une réflexion collective sur les effets discriminatoires du recours à la judiciarisation et à l'emprisonnement.

Ce qui a sans cesse été marquant chez Lucie, c'était non seulement la rigueur de ses analyses, mais aussi sa grande sensibilité à l'égard des victimes de violations de droits, faisant d'elle une porte-parole convaincue et convaincante lorsqu'il s'agissait d'intervenir pour faire cesser toute situation d'injustice.

Nicole Filion, présidente de la LDL de 2000 à 2007 et coordonnatrice de 2007 à 2018

Le monde de Lucie

Lucie Lemonde portait bien son nom. Lucie avait en tête, dans sa défense des droits, non seulement des catégories, les *ceuses* qui subissaient les violations, elle avait une vision d'ensemble, multisectorielle. Elle avait le monde en tête.

Lucie me remplaça à la présidence. Il était temps... Je crois qu'elle était la première femme élue à la tête de la LDL même si de nombreuses femmes y ont milité ou travaillé.

Lucie a donné un élan à la défense des droits sociaux et économiques et aux droits carcéraux à la défense desquels elle avait été active à l'Office des droits des détenu-e-s. Elle a aussi brassé la cage à la Fédération internationale des droits humains.

Lucie, complexe, fidèle à ses principes, toujours à prendre avec humour le meilleur et le pire, et en révolte devant les situations inacceptables. Lucie qui abhorrait les orthodoxies, les points de vue fermés, mais qui avait une façon délicate de te faire sentir que t'étais dans les patates, que t'avais mal compris. Et qui faisait réfléchir aux actions à mener pour éviter de rentrer dans le mur et pour faire avancer notre cause.

L'amitié qui nous liait elle et moi, empreinte de chaleur, je la partageais avec tant d'autres, profondément tristes de son départ.

J'aurais tellement voulu être avec elle les derniers temps de sa vie. Nous étions loin physiquement, elle dans le Mile End, nous en Gaspésie, mais si proches. S'il y a un paradis, elle y est certainement. Les saint-e-s et les anges n'auront pas la vie tranquille, mais il y aura du plaisir.

Entre nous, on peut dire d'elle : *no bullshit!!!*

Merci Lucie.

Gérald McKenzie, président de la LDL
un bon *boutte* vers la fin du XX^e siècle



Crédit : André Query

Lucia, tête première

Je l'ai rapidement appelée Lucia, en prononçant à l'italienne (comme si je connaissais l'italien!). C'était plus drôle, plus chantant, plus fantaisiste. Car s'il y avait la rigueur, l'intelligence acérée et la parole vraie, il y avait aussi une volonté de s'inscrire à l'extérieur des sentiers battus du droit, dans les ruelles, les cafés et les manifestations citoyennes, dans les parloirs des prisons et les centres de réadaptation et, bien sûr, dans les locaux de la LDL, où elle tenait salon. C'était une rassembleuse, et de sa petite personne, elle soufflait sur toutes les braises pour mener à terme les plus grands projets. Je l'adorais. Je ne lui ai jamais rien refusé et je m'ennuierai longtemps de ses appels impératifs : « Julie, c'est Lucie. Écoute, pourrais-tu...? » Elle m'avait repérée étudiante et m'avait évidemment montré le chemin de la LDL, où elle me réservait une place *de jeune* au conseil d'administration. Je m'y suis fait les dents à ses côtés, avant de lui demander de codiriger ma thèse de doctorat sur les mesures d'isolement et les mesures disciplinaires dans les centres de réadaptation. Nous avons beaucoup écrit ensemble. Elle a conforté certaines de mes positions intellectuelles, mais elle a également incarné un modèle de femme différent, qui ne cherchait ni à plaire ni à convaincre, qui avait confiance en elle sans être prétentieuse, qui traçait son chemin tête première, travaillait fort sans avoir l'air d'y toucher et faisait de ses collaboratrices et collaborateurs ses ami-e-s. C'est peut-être ce qu'elle m'a appris de plus précieux; que la collaboration est égalitaire, en toutes circonstances.

Julie Desrosiers, professeure, Université Laval

Lucie, ma source d'inspiration

J'ai connu Lucie pendant mon baccalauréat en droit. Elle m'a enseigné le cours de droit carcéral. C'est alors que j'ai compris qu'elle allait être ma source d'inspiration et ma mentore dans ma vie professionnelle. Lucie a toujours été là lorsque j'avais besoin de me faire rassurer et de me faire écouter et elle était à mes côtés pour militer pour le respect des droits humains.

Son départ crée un immense vide. Elle me manque à chaque jour de ma pratique et je ne saurais combien la remercier pour avoir donné ce sens à ma vie. En ton honneur, Lucie, je continuerai de lutter contre les injustices dans les milieux carcéraux et je rendrai à bon port tous les dossiers que nous avons commencés ensemble.

Je sais que tu veilles déjà sur nous tous comme tu l'as toujours fait. Maintenant, prends soin de toi là-haut. Merci d'avoir été cette femme extraordinaire et inspirante que je n'oublierai jamais.

Mélanie Martel, avocate en droit carcéral

Une grande dame

Lucie était juriste, mais elle était surtout une militante contre les injustices subies par les personnes exclues et les plus vulnérables de la société : les itinérant-e-s, les détenu-e-s, les personnes démunies ignorées par les médias ou les pouvoirs en place. Pour elle, le droit n'était pas un exercice formel dont le but était de remporter une joute oratoire. C'était avant tout un instrument pour que justice soit rendue.

J'enseignais la physique lorsque je me suis impliqué à la LDL en 2001 et je n'avais aucune formation juridique. Lucie est une de celles qui m'ont initié au domaine des droits. Grande pédagogue, elle était capable d'expliquer en langage simple les enjeux de droits et même les jugements de la Cour suprême!

Lucie a été très engagée dans la défense de la liberté d'expression et du droit de manifester. Elle a été au cœur des interventions pour la défense des droits des manifestant-e-s lors du Sommet des Amériques en 2001, du G20 à Toronto en 2010 et de la grève étudiante en 2012. Son action dans la défense de ces droits a été une véritable école pour plusieurs jeunes qui sont par la suite devenus des militant-e-s de la LDL. Elle a également eu une contribution marquante pour défendre les droits des personnes détenues, notamment lors de l'intervention de la LDL pour dénoncer la situation scandaleuse des femmes détenues à la prison Leclerc ces dernières années.

Une grande dame, discrète, modeste, une femme d'équipe qui ne cherchait pas les projecteurs, mais qui n'était jamais loin lorsque des droits étaient bafoués. Merci Lucie!

Dominique Peschard, président de la LDL de 2007 à 2015 et militant

Ma chère Lucie,

Je te connaissais de nom avant d'arriver à la LDL en 2018. Je connaissais ton parcours et tes apports majeurs sur les questions de droit carcéral, du droit de manifester et de droits de la personne de manière générale. Au niveau du Québec et du Canada, mais aussi au niveau mondial, ne l'oublions pas.

Et je t'ai finalement rencontrée en personne, en 2018. Nous avons eu notre première discussion sur les questions carcérales et les luttes de la LDL sur ces questions dans la salle de réunion *pas-de-fenêtre-avec-tables-grises* à l'ancien bureau de la LDL sur la rue Beaubien.

Et je suis ressortie de cette rencontre soufflée. Soufflée par tes connaissances et ton énergie, mais aussi soufflée par ta grande ouverture, ton humour et tes dons de conteuse. Grâce à ce talent particulier, j'ai pu aisément m'approprier le passé si vaste de la LDL.

Le temps passant, tu es rapidement devenue une amie. Une amie qui me manque et qui continuera de me manquer.

Merci d'avoir œuvré d'arrache-pied toute ta vie pour la bonification des droits et des libertés pour toutes et tous.

Et, bien égoïstement, merci d'avoir été de passage dans ma vie, aussi court ce passage fut-il. Celle-ci s'en retrouve enrichie.

Bon voyage, mon amie.

Eve-Marie Lacasse, coordonnatrice de la LDL de 2018 à 2021

La fougue de Lucie

Lucie Lemonde a été une des premières à dénoncer le transfert des femmes incarcérées à la prison Tanguay vers l'établissement Leclerc en 2016. Sa détermination a mené à la création de nouvelles alliances entre les groupes de défense des droits des personnes incarcérées et des groupes féministes, chose qui ne s'était pas vue depuis plusieurs années au Québec. Ces alliances se sont concrétisées par la création de la Coalition d'action et de surveillance sur l'incarcération des femmes au Québec, la CASIFQ, dont Lucie était une membre fondatrice.

Lucie avait une fougue pour défendre les droits des femmes et des personnes incarcérées, qui pendant presque 40 ans de lutte ne s'est jamais essouffée. Par ses prises de paroles dans les médias, ses conférences et ses cours à l'Université, Lucie a sensibilisé des milliers de personnes aux conditions d'incarcération et à une réflexion plus large sur l'usage de la prison comme solution aux problèmes sociaux au Québec et au Canada.

Lors des rencontres importantes, Lucie était la première à vouloir *brasser la cabane*. Elle nous rappelait de ne pas nous laisser mener par les langues de bois des politicien-ne-s et a continué à lutter pour un changement de fond malgré l'immobilisme ambiant. Sa contribution aux luttes sociales au Québec est inestimable et son décès est une grande perte.

Au-delà de la militante infatigable, nous avons appris à connaître Lucie comme étant une femme rassembleuse, sensible, à l'écoute, drôle et passionnée. Lucie nous manquera non seulement comme collègue, mais également comme amie.

Solidairement et affectueusement,

La CASIFQ



Crédit : André Query

« Écoute, je vais te conter ça »

Octobre 2012. Je suis étudiante au doctorat. À la sortie d'un colloque académique, je croise Lucie Lemonde, que je ne connais alors que de réputation. Je me présente. On discute un peu des présentations, mais rapidement, la discussion prend un virage. Lucie me dit : « Implique-toi donc à la Ligue des droits et libertés! »

Lucie Lemonde, c'était ça.

Je venais de rencontrer une personnalité académique renommée, dans un contexte académique et juridique... et la première chose qu'elle me dit, c'est de sortir de la tour d'ivoire universitaire pour mettre mes recherches, et le droit, au service des transformations sociales.

Je l'ai écoutée. Et depuis 10 ans, à coups de rapports sur le droit de manifester, de colloques sur les profilages et d'innombrables réunions animées, j'ai eu la chance de lutter aux côtés de Lucie, à la Ligue des droits et libertés. Mais aussi et surtout, j'ai eu la chance d'apprendre d'elle.

Apprendre de Lucie-la-prof, qui enseignait comme personne le droit carcéral et les droits des personnes détenues.

Apprendre de Lucie-la-militante, qui savait s'indigner, dire les choses telles qu'elles sont (« Les femmes sont envoyées dans un pénitencier qui est complètement scrap »), tout en luttant pour gagner.

Apprendre de Lucie-l'amie, tout sourire au café du coin, avec son *mini-me* un sucre, mais toute colère aussi, contre la dernière injustice : « Écoute je vais te conter ça, ma fille! ».

Lucie Lemonde, c'était ça.

Et tellement, tellement plus.

Avec gratitude et tout plein d'amour, je te dis salut, Lucie!

Véronique Fortin, professeure, Université de Sherbrooke, et militante

L'héritage de Lucie

J'ai connu Lucie Lemonde alors que j'étais coordonnateur de l'Office des droits des détenu-e-s (ODD) et que nous travaillions, entre autres, sur la reconnaissance et l'exercice du droit de vote des détenu-e-s, au début des années 1980. Jeune avocate, elle s'est immédiatement impliquée dans les recours que nous avons entrepris et dans cette lutte qui a ultimement abouti devant la Cour suprême en 2002, et s'est conclue par une avancée démocratique indéniable.

Peu de temps après le début de sa militance à l'ODD, elle soulignait que « (s)on aversion pour la prison a coïncidé avec (s)on éveil au féminisme ou plutôt en a été la suite logique, le contrecoup ». Elle adoptait donc le discours critique de l'époque, et plus particulièrement celui de l'ODD, une perspective abolitionniste qui avait été adoptée à la fin des années 1970 (La Vie en Rose, mars 1983, p. 36 et 37).

Dans les années qui ont suivi, elle a associé militance, acquisition de connaissances (doctorat et recherche) et diffusion des savoirs acquis (enseignement), sans négliger l'action, c'est-à-dire la participation à des groupes et des mouvements de contestation.

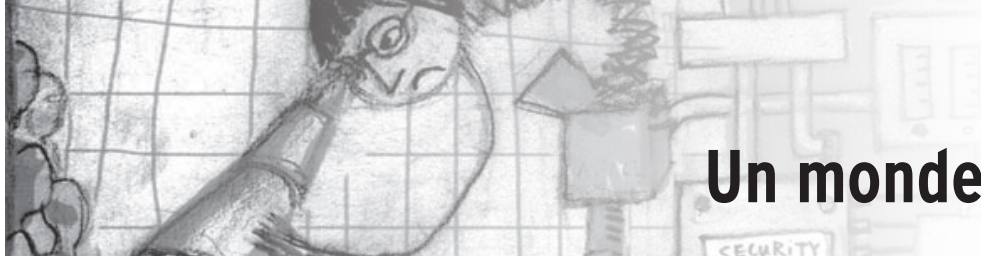
Ultimement, ce qui doit être souligné, c'est l'héritage qu'elle laisse : les militant-e-s qu'elle a inspirées et qui suivent ses traces.

Jean Claude Bernheim, militant

Lucie et moi

Lucie à la radio. Lucie au lancement d'un livre sur les prisons. Lucie dans le journal. Lucie en tournée d'ateliers auprès de groupes communautaires en Gaspésie, en Abitibi, dans le Bas-du-fleuve. Lucie qui coordonne la rédaction d'un rapport sur les abus des forces policières. Lucie à son café au coin de la rue. Lucie qui défend l'égalité des genres dans un organisme de « droits de l'Homme-avec-un-grand-H ». Lucie en commission parlementaire. Lucie sur le panel d'une commission populaire. Lucie et Nicole. Lucie qui donne un *lift*. Lucie outrée par les conditions d'arrestation et de détention d'un manifestant. Lucie qui dit ses quatre vérités au ministre de la Sécurité publique. Lucie et sa petite-fille. Lucie et ses étudiantes. Lucie grave avec son accent sérieux. Lucie à la campagne. Lucie avec ses résumés des arrêts de la Cour suprême. Lucie avec une pinte et un lot de bonnes histoires. Lucie et quelques confidences départementales. Lucie qui parle de la défense des détenu-e-s. Lucie et Natacha. Lucie et son réservoir d'indignation. Lucie et la protection contre les SLAPP. Lucie et la liberté d'expression. Lucie qui ricane. Lucie et l'avortement libre et gratuit. Lucie forte de toutes ses solidarités. Lucie debout. Lucie vivante dans la mémoire de nos cœurs.

Pierre-Louis Fortin-Legris, avocat et militant



Un monde sous surveillance

Proposition du gouvernement du Canada

Les dangers de la lutte contre les méfaits en ligne

Tim McSorley, coordonnateur national, Coalition pour la surveillance internationale des libertés civiles (CSILC)

Au cours des deux dernières décennies, nous en sommes venu-e-s à dépendre des plateformes en ligne pour des besoins de base, la communication, l'éducation et le divertissement. En ligne, nous voyons le *bon* – l'accès à des informations autrement difficiles à trouver, la communication avec des êtres chers – et le *mauvais*. Le *mauvais* englobe souvent des méfaits que nous connaissons bien, notamment les discours haineux, le racisme, la misogynie, l'homophobie, la transphobie, l'exploitation sexuelle de mineurs, l'intimidation et l'incitation à la violence, avec de nouvelles formes de harcèlement et d'abus qui peuvent se produire à une échelle beaucoup plus grande, et avec de nouveaux moyens de diffuser des contenus préjudiciables et illégaux.

Plusieurs sites de médias sociaux se sont engagés à remédier à ces méfaits. Toutefois, les modèles commerciaux axés sur la rétention de l'engagement de l'utilisateur, peu importe le contenu se sont avérés être incapables d'y parvenir. Les chercheurs ont constaté que lorsque ces plateformes en ligne suppriment du contenu *préjudiciable*, ce sont souvent les communautés qui subissent du harcèlement qui subissent le plus de censure. Par ailleurs, des gouvernements à travers le monde ont utilisé le prétexte de la lutte contre le discours haineux et les méfaits en ligne pour censurer et réduire au silence des opposants, notamment des défenseurs des droits humains.

Le gouvernement canadien promettait depuis 2019 de s'attaquer à ce problème, en le situant explicitement dans le cadre de la lutte contre la *haine en ligne*. Fin juillet 2021, le gouvernement a finalement dévoilé son projet pour s'attaquer aux méfaits en ligne, en même temps qu'il amorçait une consultation publique. Le fait que la consultation ait lieu au cœur de l'été, avec une élection imminente à l'horizon, a immédiatement suscité des inquiétudes. Quand les élections ont été déclenchées quelques semaines plus tard, les tables rondes avec des représentant-e-s du gouvernement qui pouvaient répondre aux questions concernant le projet ont été annulées.

L'approche du gouvernement était mauvaise et le projet lui-même encore pire. Comme l'a décrit Daphne Keller, chercheuse en cyberpolitique, la proposition initiale du Canada était « comme une liste des pires idées dans le monde – celles que les groupes de défense des droits humains – combattent dans l'UE, en Inde, en Australie, à Singapour, en Indonésie et ailleurs ».

Les chercheurs ont constaté que lorsque ces plateformes en ligne suppriment du contenu *préjudiciable*, ce sont souvent les communautés qui subissent du harcèlement qui subissent le plus de censure.

Quels étaient certains de ces problèmes?

Tout d'abord, plusieurs groupes ont exprimé des inquiétudes sur la portée de la proposition qui tentait de créer un seul système pour traiter cinq types de méfaits très différents – le discours haineux, le partage non consensuel d'images intimes, le matériel d'abus sexuel d'enfant, le contenu incitant à la violence et le contenu terroriste – et qui nécessitaient des solutions distinctes et spécifiques. En effet, ce qui est efficace dans un cas peut être inutile, voire nuisible, dans un autre.

Ensuite, l'inclusion du *contenu terroriste* était problématique en soi. Depuis que le Canada s'est joint à la *guerre contre le terrorisme* en 2001, nous avons vu comment l'application des lois sur le terrorisme a mené à la violation de droits humains, en particulier parce que la définition de *terrorisme* peut être détournée à des fins politiques. Pourtant, on voulait demander à des entreprises de médias sociaux d'identifier le *contenu terroriste* et, sur cette base, de signaler ce contenu et ses utilisateurs-trices à la police. C'était la recette parfaite pour induire du profilage racial et politique, en particulier envers les musulman-e-s, les autochtones et d'autres groupes de personnes racisées, et la violation de leurs droits et libertés.

Troisièmement, le projet aurait créé un nouveau et vaste régime de surveillance, appliqué par les entreprises de médias sociaux. Ces entreprises seraient ainsi tenues de surveiller tout le contenu visible et publié sur leurs plateformes au Canada, de le filtrer pour détecter les méfaits et de prendre « toutes les mesures raisonnables » pour bloquer le contenu préjudiciable, même en utilisant des algorithmes automatisés. Les plateformes devraient aussi agir dans un délai de 24 heures contre tout contenu signalé par des personnes utilisatrices – un délai incroyablement court. Avec des pénalités pouvant atteindre des millions de dollars, les plateformes auraient été incitées à supprimer le contenu d'abord, quitte à en assumer les conséquences par la suite. Cela serait une incitation massive à la censure de contenus controversés, même légaux.



Comme quatrième problème identifié, notons celui des nouvelles règles qui obligeraient les plateformes à partager automatiquement des informations avec les forces de l'ordre et les agences de sécurité nationale, privatisant encore davantage la surveillance et la criminalisation des internautes. Cela signifiait non seulement que les plateformes décideraient quel contenu supprimer, mais aussi qui et quoi devrait être signalé à la police. Comme l'ont souligné plusieurs critiques, impliquer davantage la police et les agences de renseignement n'est pas une approche souhaitable quand il s'agit de traiter les préjudices causés à des groupes qui font déjà face à des niveaux de criminalisation plus élevés.

Pourtant, on voulait demander à des entreprises de médias sociaux d'identifier le contenu terroriste et, sur cette base, de signaler ce contenu et ses utilisateur-trice-s à la police. C'était la recette parfaite pour induire du profilage racial et politique [...]

Le projet a aussi avancé l'argument ahurissant, qu'on devrait accorder au Service canadien du renseignement de sécurité (SCRS), sans justifications, une nouvelle forme de mandat qui *simplifierait* le processus pour obtenir les données de base sur les abonnés, ceci afin de faciliter les enquêtes sur les méfaits en ligne. Cela survient à un moment où des tribunaux ont critiqué le SCRS pour avoir enfreint des exigences de mandats plus strictes déjà en place.

Finalement, l'une des leçons claires tirées d'autres pays est la nécessité d'établir des règles rigoureuses en matière de transparence et de reddition de comptes, tant pour les plateformes que pour l'organisme responsable d'appliquer la réglementation sur les méfaits en ligne. Malheureusement, le projet du gouvernement canadien ne prévoyait pas de divulgations publiques significatives et comportait très peu d'exigences de transparence et de reddition de comptes.

Derniers développements

En février 2022, le ministère du Patrimoine a publié un rapport intitulé *Ce que nous avons entendu*, dans lequel il reconnaissait plusieurs des questions valables concernant l'approche du gouvernement. Il a annoncé un nouveau processus de consultation mené par un nouveau groupe consultatif d'expert-e-s pour examiner ces questions et formuler des recommandations sur ce que devrait être l'approche du gouvernement. Il est important de noter que le processus et les délibérations du groupe seront rendus publics.

Nous en sommes maintenant aux toutes premières étapes de ce processus. D'un côté, nous pouvons considérer qu'il s'agit d'une victoire : des groupes issus de secteurs très différents ont ensemble fait part de leurs préoccupations concernant un projet législatif vicié, et le gouvernement a accepté de le revoir. Cependant, une première lecture des documents d'orientation du nouveau projet envoie des messages contradictoires.

Le gouvernement semble concéder qu'un système basé principalement sur la suppression de contenu et sur une surveillance accrue est inacceptable. Les documents d'information mettent aussi davantage l'accent sur la protection de la liberté d'expression et de la vie privée.

En même temps, ces documents s'appuient explicitement sur un nouveau modèle britannique, présenté dans un projet de loi sur la sécurité en ligne et connu sous le nom de *devoir de diligence*. Bien que ce modèle soit basé sur l'idée que les plateformes doivent assumer la responsabilité de leurs actions, il a aussi été l'objet de vives critiques pour cibler lui aussi les contenus *lawful but awful* (légal mais ignoble). Par *légal mais ignoble*, on entend des contenus et des activités qui, bien que légaux, peuvent être considérés comme préjudiciables. Le problème est que les plateformes seraient non seulement tenues de déterminer si un contenu est illégal – ce qui peut déjà être difficile – mais aussi si un contenu légal doit être considéré comme préjudiciable. Ce flou pourrait conduire à une suppression et à une censure encore plus large de contenus.

Parallèlement à la nouvelle approche, l'idée de traiter les cinq mêmes méfaits dans le cadre d'un seul système demeure envisagée ainsi que le signalement obligatoire aux forces de l'ordre, bien que formulée différemment.

Divers groupes, dont la Coalition pour la surveillance internationale des libertés civiles (CSILC), continuent de travailler ensemble pour répondre aux propositions du gouvernement et pour développer des réflexions sur la meilleure façon de combattre les méfaits en ligne. Il s'agit manifestement d'un problème complexe, et il est plus facile d'en pointer les défauts que de développer des solutions concrètes. Ce qui semble clair, cependant, est que le fait de donner aux plateformes en ligne privées le pouvoir d'exercer une surveillance accrue et de supprimer du contenu non seulement ne résoudrait pas le cœur du problème, mais créerait davantage de dommages. Les gouvernements doivent plutôt investir dans des solutions hors ligne pour combattre les racines du racisme, de la misogynie, du sectarisme et de la haine. Il est tout aussi important que les gouvernements s'attaquent aux modèles commerciaux des plateformes de médias sociaux qui tirent profit de la surveillance et utilisent des contenus qui provoquent l'indignation et la division pour susciter l'engagement et fidéliser le public. Tant qu'il y aura des profits à faire en alimentant ces préjudices, nous ne pourrons jamais les éliminer vraiment.

Le problème est que les plateformes seraient non seulement tenues de déterminer si un contenu est illégal – ce qui peut déjà être difficile – mais aussi si un contenu légal doit être considéré comme préjudiciable. Ce flou pourrait conduire à une suppression et à une censure encore plus large de contenus.

Le sel de la Terre

Rémy-Paulin Twahirwa, militant abolitionniste et doctorant en sociologie à la *London School of Economics*

« *Europe pushes against me, I push back.* »
(Selina Thomspon, *salt*)

« *Vous êtes le sel de la terre. Mais si le sel perd sa saveur, avec quoi la lui rendra-t-on ? Il ne sert plus qu'à être jeté dehors, et foulé aux pieds par les hommes.* »
(Matthieu, 5 :13)

Le 24 février 2022, la Russie entamait l'invasion de l'Ukraine, une étape que plusieurs avaient prédite, mais dont peu avaient correctement évaluée la proportion et la durée. Ainsi, il est estimé que, depuis le début du conflit, plus de 11 millions de personnes ont fui l'Ukraine¹ ou été forcées de se déplacer à l'intérieur de leur pays faisant du conflit la plus importante *crise* de réfugié-e-s en Europe depuis la Deuxième guerre mondiale.

Depuis le début de l'invasion, les pays de l'Europe occidentale et leurs alliés ont déployé des efforts pour soutenir et accueillir les réfugié-e-s ukrainien-ne-s. À l'exception du mouvement *Réfugiés Bienvenus* qui a connu un succès mitigé en Allemagne alors que le pays a accueilli plus de 1.7 millions de demandeurs d'asile² entre 2015 et 2017, le vent de solidarité envers les Ukrainien-ne-s est particulièrement surprenant considérant les attitudes et discours anti-réfugiés et anti-(im)migration qui ont dominé l'espace médiatique et la scène politique en Europe depuis la fin des années 1990. Ainsi, au Royaume-Uni où je réside en ce moment, de nombreuses compagnies invitent leurs employé-e-s et/ou client-e-s à faire un don pour soutenir l'Ukraine et les Ukrainien-ne-s. De même, bon nombre de pays soutiennent militairement et économiquement les forces ukrainiennes, notamment par l'accueil de réfugié-e-s et l'adoption de sanctions économiques contre la Russie et ses oligarques.

Force est de constater que le traitement des personnes réfugiées dans la présente *crise* n'est pas équitable. Ainsi, de nombreuses personnes non-blanches, en particulier celles d'origine africaine³, les personnes roms⁴ et celles du Moyen-Orient⁵, ont dénoncé leur traitement en Ukraine et dans les

pays voisins. Les témoignages font état de refoulement à la frontière⁶, de détention⁷ – notamment en Ukraine et en Pologne – d'abus physiques et d'insultes à caractère racial. En somme, ce que le sociologue afro-américain W. E. Du Bois appelait la *ligne de couleur* continue de partager la Terre, même en temps de conflits, et de classer notre espèce entre celles et ceux dont la vie est digne d'être vécue⁸ et celles et ceux voué-e-s à vivre une vie fantomatique, une demi-vie, une vie morte. De fait, en raison des rémanences du colonialisme et de l'impérialisme qui hantent encore nos sociétés, les constructions ontologiques qui structurent encore notre compréhension de l'humain et du non-humain, du vivant, du mort et du vivant-mort, transparaît dans la manière dont le réfugié blanc, qu'il soit Ukrainien ou autre, constitue pour les populations européennes et nord-américaines, le *bon* réfugié, celui qui, à terme, est accueilli les bras ouverts, celui dont la vie, sans être aisée, demeure *envisageable* et *souhaitée*.

Dans l'ombre de ce *bon* réfugié, nous retrouverons ce que certains ont qualifié de *vies jetables*⁹, à savoir ces hommes et femmes, issues en grande partie d'anciennes colonies et/ou de territoires annexés par les empires européens et américains qui finissent trop souvent sur l'autel du capitalisme dans des emplois jugés tout récemment *essentiels*, mais dont les conditions de travail demeurent somme toute misérables et indignes. L'indignité, la vie morte, est bien sûr combattue quotidiennement par celles et ceux qui la rejettent en protestant qu'elle n'est pas le seul horizon de leur existence. Or, ce qui importe de mettre de l'avant ici, c'est que cette condition n'est pas le résultat d'une quelconque conspiration, d'un hasard, d'une opération mystique ou magique, ou alors d'une volonté malsaine, mais bien une continuation de la manière dont la Terre a été partagée et les vies humaines, hiérarchisées.

1. En ligne : <https://www.bbc.co.uk/news/world-60555472>

2. En ligne : <https://www.unhcr.org/5ee200e37/>

3. En ligne : <https://www.nytimes.com/2022/03/01/world/europe/ukraine-refugee-discrimination.html>

4. En ligne : <https://www.aljazeera.com/news/2022/3/7/ukraines-roma-refugees-recount-discrimination-on-route-to-safety>

5. En ligne : <https://www.reuters.com/world/arab-refugees-see-double-standards-europes-embrace-ukrainians-2022-03-02/>

6. En ligne : <https://www.irishtimes.com/news/world/africa/africans-trying-to-flee-ukraine-complain-of-being-blocked-and-of-racist-treatment-1.4813571>

7. En ligne : <https://www.independent.co.uk/news/world/europe/ukraine-refugees-detention-international-students-b2041310.html>

8. Sur ce thème, voir Judith Butler, *Vie précaire : les pouvoirs du deuil et de la violence après le 11 septembre 2001*. Ed. Amsterdam, 2005.

9. En ligne : <https://www.historiesofviolence.com/disposablelife>

[...] la *ligne de couleur* continue de partager la Terre, même en temps de conflits, et de classifier notre espèce entre celles et ceux dont la vie est digne d'être vécue et celles et ceux voué-e-s à vivre une vie fantomatique, une demi-vie, une vie morte.

Du partage de la Terre et la désignation de l'humain

En ce sens, le *double standard* dans l'accès au refuge met en lumière deux processus teintés par le colonialisme et l'impérialisme, à savoir le partage de la Terre et la désignation de l'humain. D'une part, le statut de réfugié, dès sa création en 1951, était un dispositif de classification des vies humaines qui excluait sciemment les personnes vivant dans les colonies et les empires. Le gouvernement britannique, par exemple, s'opposait à toute institutionnalisation des droits humains par l'Organisation des Nations Unies qui menacerait ses intérêts coloniaux et impériaux à la fin des années 1940. Ainsi, les diplomates britanniques proposaient une *clause coloniale* (devenue *clause territoriale*) permettant d'exclure les sujets (non-blancs) de la Couronne vivant dans une colonie. L'argument étant que les colonies n'étant pas à même de se gouverner elles-mêmes nécessitaient encore de la protection de l'Empire et que celui-ci assurerait leur bien-être.

Le droit à l'asile, dès lors, était réellement destiné qu'à préserver la conscience des puissances européennes face à ce qu'Aimé Césaire appelait, dans son *Discours sur le colonialisme*, le « crime contre l'homme blanc » qu'était l'hitlérisme et la solution finale, c'est-à-dire « d'avoir appliqué à l'Europe les procédés colonialistes et dont ne se relevaient jusqu'ici que les Arabes d'Algérie, les coolies de l'Inde et les nègres d'Afrique ». Il aura fallu attendre le début de la chute des empires coloniaux européens et le cycle des indépendances pour qu'enfin, dans le droit international, soit reconnu à l'ensemble de l'humanité le statut d'être humain. Entre le début de la marchandisation et l'exploitation du corps indigène en Afrique, dans les Amériques et en Asie et le processus de décolonisation entamée après la Deuxième guerre mondiale, la désignation de l'humain est donc effectivement liée à la déshumanisation du colonisé.

D'autre part, la *gestion* – dans le langage des bureaucrates néolibéraux – des réfugiés non-blancs issus de l'Ukraine met en évidence la manière dont la Terre a été partagée par les grandes puissances : c'est-à-dire qu'il trouve sa racine dans la frontière. Les êtres, la matière animale et végétale, la surface de la Terre comme son ventre, les eaux et l'atmosphère, tout est soumise à la ligne frontalière qui catégorise les appartenances culturelles et nationales, qui octroie les droits d'extraction,

de commercialisation, de transformation et d'exploitation du vivant comme du non-vivant. L'espèce humaine, elle-même, a été soumise aux cartes et à la géographie du Colon¹⁰. Celui-ci fit du monde un monde de nations, de *cultures*, de peuples, définitivement fixés à un territoire, à un espace, une cage dont les barreaux étranglent en ce moment celles et ceux dont l'unique crime est d'être nés du *mauvais côté* de la frontière. Les cris, les sifflements et les grincements qui hantent nos nuits dans nos forteresse-nations, n'est nul autre celui des hommes, femmes et enfants qui rongent les fers de la frontière et contestent l'assignation à résidence.

Il aura fallu attendre le début de la chute des empires coloniaux européens et le cycle des indépendances pour qu'enfin, dans le droit international, soit reconnu à l'ensemble de l'humanité le statut d'être humain.

Le surgissement des Monstres

« Le vieux monde se meurt, le nouveau monde tarde à apparaître et dans ce clair-obscur surgissent les monstres. », écrivait Antonio Gramsci dans *Les Cahiers de prison*. Or, nous voilà à nouveau (ou toujours?) dans ce *clair-obscur* où les Monstres établissent leur règne funeste et sanglant. L'ordre crépusculaire du Monde s'établit avec l'érection de murs, la construction et le placement de machines à vagues¹¹ et l'envoi de bateaux militaires dans la fosse commune qu'est la Méditerranée pour repousser les personnes exilées, l'achat et le déploiement de technologies de traç[qu]age, bref le renforcement du fantasme sécuritaire¹². À terme, il nous faudra bien atteindre ce qu'Octavia Butler appelle dans sa dystopie *La Parabole du Semeur* et *La Parabole des Talents* l'« âge adulte de notre espèce ». La crise ukrainienne se présente donc comme une occasion pour restructurer notre planète à partir de valeurs et de principes qui assurent à tou-te-s une vie digne d'être vécue où toutes les vies comptent réellement. Pour ce faire, il est urgent de redéfinir l'humain et ses droits pour que ces derniers ne soient pas dictés par l'appartenance à une nation, à un statut de citoyenneté ou à un territoire. Le clair-obscur n'a d'entreprise que parce qu'il précède le jour ; lutter pour faire jaillir la lumière et la vie n'a de prix que nos chaînes.

10. En ligne : <https://revueliberte.ca/article/1645/au-sortir-de-la-matrice-crepusculaire>

11. En ligne : <https://www.independent.co.uk/news/uk/politics/english-channel-crossings-wave-machine-island-b1765077.html>

12. En ligne : <https://liguedesdroits.ca/carnet-abolir-frontieres-fantasme-securitaire/>

Présentation

Le capitalisme de surveillance : menaces à la démocratie et aux droits!

Elisabeth Dupuis, responsable des communications, Ligue des droits et libertés

À divers moments de son histoire, la Ligue des droits et libertés (LDL) s'est intéressée aux enjeux de protection de la vie privée, notamment avec sa campagne *Gérard et Georgette, citoyens fichés* en 1986, puis aussi à la surveillance des populations au nom de la *guerre au terrorisme* à la suite des attentats du 11 septembre 2001. Dans un contexte où le développement technologique facilitait énormément la circulation de données personnelles, la préoccupation principale était de renforcer le régime de protection de ces données, tel que conçu à la fin du XX^e siècle. Avec le développement des entreprises numériques au cours des 20 dernières années, les enjeux ne sont plus du tout les mêmes.

En l'absence d'un cadre juridique contraignant et dans le flou des obligations des entreprises opérant dans le domaine numérique, une nouvelle forme de capitalisme s'est développée au cours des 20 dernières années. Les données comportementales de l'être humain deviennent alors le *nouveau pétrole*¹. La matière première n'est pas celle extraite de la terre, des champs ou des forêts; elle est générée au quotidien par les traces numériques que nous laissons dans toutes nos activités au travail, à la maison et pendant nos déplacements. Le comportement de chaque être humain devient source de profits sans qu'il sache comment, pourquoi, quand et qui se sert de ces données massives générées par l'utilisation d'applications numériques gratuites et de multiples objets connectés et géolocalisés. Les enjeux sont multiples et sans précédent. En 2018, dans un rapport du Haut-Commissariat aux droits de l'homme, on souligne que les technologies numériques, mises au point principalement par le secteur privé, en exploitant en permanence les données personnelles, « pénètrent progressivement dans le tissu social, culturel, économique et politique des sociétés modernes² ».

En effet, on s'aperçoit que les enjeux dépassent largement la seule question de la protection de la vie privée puisque d'autres droits humains sont aussi affectés. « L'intelligence artificielle rend possible une surveillance extrême des individus (tant par des entreprises privées que par l'État) susceptible d'affecter la liberté d'expression, la liberté d'association et la démocratie. La reconnaissance faciale met en péril le droit à l'anonymat et éventuellement le droit à l'égalité³. » En contrôlant la circulation de l'information, les réseaux sociaux peuvent avoir une influence sur les opinions et les comportements des personnes, exerçant ainsi un certain contrôle social. En outre, des algorithmes peuvent entretenir, voire aggraver, des pratiques discriminatoires.

D'autre part, les données accumulées par les entreprises privées sur l'ensemble de la population, alors que la capacité réelle de chaque individu de consentir à l'utilisation et au partage de ses données de façon libre et éclairée est difficile, voire impossible, deviennent de plus en plus accessibles aux forces policières par des mécanismes variés comme le système *Ring* d'Amazon. Ces forces policières se dotent de centres d'opération numérique et utilisent des systèmes de décisions automatisées alimentés avec des données renforçant un biais répressif envers certaines populations, ce qui entraîne plus de profilage et menace ultimement la présomption d'innocence.

Appréhender tous ces enjeux avec l'approche de l'interdépendance des droits, qui reconnaît que la réalisation d'un droit est intimement liée à celle des autres droits, ne peut que déclencher la sonnette d'alarme chez les militant-e-s pour la défense des droits humains. En consacrant un dossier sur le capitalisme de surveillance, le comité éditorial de la revue souhaite dévoiler les angles morts du capitalisme de surveillance, sensibiliser aux rapides et profondes transformations sociales et politiques qui s'opèrent ainsi qu'aux menaces que cela représente tant pour la démocratie que pour les droits humains. Finalement, ce dossier vise à susciter des débats publics dans la population, loin des chambres d'écho, sur ces enjeux qui nous concernent toutes et tous.

Bonne lecture!

1. En ligne : <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>

2. En ligne : <https://www.ohchr.org/fr/calls-for-input/reports/2018/report-right-privacy-digital-age>

3. En ligne : <https://liguedesdroits.ca/chronique-surveillance-ia/>

Capitalisme de surveillance

Une crise pour les démocraties

Shoshana Zuboff, professeure émérite à la *Harvard Business School* et auteure de *L'Âge du capitalisme de surveillance*

C'est avec la permission de Shoshana Zuboff et du New York Times que nous publions cette traduction du texte initialement publié le 12 novembre 2021 dans le New York Times¹.



Crédit : André Query, Une oeuvre de Maria Ezcurra, Festival Art Souterrain 2022

Facebook n'est pas une entreprise quelconque. Elle a atteint le cap du billion de dollars² en une seule décennie en appliquant la logique de ce que j'appelle le capitalisme de surveillance — un système économique construit sur l'extraction et la manipulation secrètes des données humaines — à sa vision d'un monde interrelié. Facebook et d'autres grandes entreprises du capitalisme de surveillance contrôlent désormais les flux de l'information et les infrastructures de communication dans le monde entier.

Ces infrastructures sont essentielles pour qu'une société démocratique soit possible, mais nos démocraties ont permis à ces entreprises de posséder, d'exploiter et d'arbitrer nos espaces d'information sans contraintes légales. Ceci a donné lieu à une révolution sournoise dans la manière dont l'information est produite, diffusée et son impact. Une série de révélations depuis 2016³, appuyées par le témoignage personnel et les preuves fournies par la lanceuse d'alerte Frances Haugen⁴, montrent les conséquences de cette révolution.

Les démocraties libérales à travers le monde sont maintenant confrontées à la tragédie des biens non-communs. Les espaces d'information que les gens supposent être publics sont régis uniquement par des intérêts commerciaux privés en vue d'un profit maximum. Internet, en tant que marché autoréglementé, s'est révélé être un échec. Le capitalisme de surveillance laisse dans son sillage une traînée de dégâts sociaux : la destruction massive de la vie privée, l'augmentation des inégalités sociales, l'empoisonnement du discours public par des informations non factuelles, la démolition des normes sociales et l'affaiblissement des institutions démocratiques.

Ces préjudices sociaux ne sont pas le fruit du hasard. Ce sont des effets étroitement liés à l'enchaînement des opérations économiques. Chaque préjudice ouvre la voie au suivant et dépend de ce qui l'a précédé.

Il n'y a aucun moyen d'échapper aux systèmes de surveillance, que nous soyons en train de magasiner, de conduire ou de nous promener dans le parc. Toutes les avenues de participation économique et sociale passent désormais par la maximisation du profit du capitalisme de surveillance, une situation qui s'est aggravée pendant presque deux ans de pandémie.

1. En ligne : <https://www.nytimes.com/2021/11/12/opinion/facebook-privacy.html>

2. En ligne : <https://www.bloomberg.com/news/articles/2021-07-01/facebook-fb-reaps-1-trillion-reward-for-grow-at-any-cost-culture?>

3. En ligne : <https://www.propublica.org/article/facebook-doesnt-tell-users-everything-it-really-knows-about-them>

4. En ligne : <https://www.nytimes.com/2021/10/03/technology/whistle-blower-facebook-frances-haugen.html>

La violence numérique de Facebook déclenchera-t-elle enfin notre engagement à nous réapproprier les biens non-communs? Allons-nous continuer d'ignorer les enjeux fondamentaux d'une civilisation de l'information : comment devrions-nous organiser et gouverner les espaces d'information et de communication du siècle numérique de manière à soutenir et promouvoir les valeurs et principes démocratiques?

Le capitalisme de surveillance laisse dans son sillage une traînée de dégâts sociaux : la destruction massive de la vie privée, l'augmentation des inégalités sociales, l'empoisonnement du discours public par des informations non factuelles, la démolition des normes sociales et l'affaiblissement des institutions démocratiques.

Recherche et saisie

Facebook, tel que nous le connaissons aujourd'hui, a été façonné à partir de la côte de Google. L'entreprise de Mark Zuckerberg n'a pas inventé le capitalisme de surveillance. Google l'a fait. En 2000, alors que seulement 25 % des informations mondiales étaient stockées numériquement⁵, Google était une petite entreprise avec un excellent produit de recherche, mais peu de revenus.

En 2001, pendant l'éclatement de la bulle technologique, les dirigeants de Google ont fait une percée avec une série d'inventions qui allaient transformer la publicité. Leur équipe a appris à combiner des flux massifs de données et d'informations personnelles avec des analyses informatiques avancées pour prédire où une publicité devrait être placée pour obtenir un maximum de clics. Au début, les prédictions étaient calculées en analysant les traces de données que les utilisateur-trice-s laissaient sur les serveurs de l'entreprise sans le savoir lorsqu'ils effectuaient des recherches et parcouraient des pages de Google. Les scientifiques de Google ont appris à extraire des métadonnées prédictives de ces traces numériques et à les utiliser pour analyser des modèles probables de comportement futur.

La prédiction était le premier impératif qui déterminait le deuxième impératif : l'extraction. Les prédictions lucratives nécessitaient des flux de données humaines à une échelle inimaginable. Les utilisateur-trice-s ne se doutaient pas que leurs données étaient secrètement recherchées et capturées dans tous les recoins de l'Internet et, plus tard, dans les applications, les téléphones intelligents, les appareils, les appareils photo et les capteurs. L'ignorance des

utilisateur-trice-s était considérée comme étant essentielle à la réussite. Chaque nouveau produit était un moyen d'accroître l'engagement, un euphémisme utilisé pour dissimuler des opérations illicites d'extraction.

À la question « Qu'est-ce que Google? », le cofondateur Larry Page a expliqué en 2001, dans un récit détaillé de Douglas Edwards, premier responsable de la marque Google, dans son livre *I'm Feeling Lucky*: « Le stockage est bon marché. Les appareils photo sont bon marché. Les gens généreront d'énormes quantités de données », a déclaré M. Page. « Tout ce que vous avez déjà entendu, vu ou vécu deviendra consultable. Votre vie entière sera consultable ».

Plutôt que de faire payer la recherche aux utilisateur-trice-s, Google a survécu en transformant son moteur de recherche en un moyen de surveillance sophistiqué pour saisir des données humaines. Les dirigeants de l'entreprise ont travaillé pour maintenir ces opérations économiques secrètes, dissimulées aux utilisateur-trice-s, aux législateur-trice-s et aux concurrents. M. Page s'est opposé à tout ce qui pouvait « agiter l'enjeu de la vie privée et mettre en danger notre capacité de collecter des données », a écrit M. Edwards.

L'ignorance des utilisateur-trice-s était considérée comme étant essentielle à la réussite. Chaque nouveau produit était un moyen d'accroître l'engagement, un euphémisme utilisé pour dissimuler des opérations illicites d'extraction.

Les opérations d'extraction à grande échelle ont été le fondement du nouvel édifice économique et ont supplanté d'autres considérations, à commencer par la qualité de l'information, car dans la logique du capitalisme de surveillance, l'intégrité de l'information n'est pas la source des revenus.

C'est dans ce contexte économique que la désinformation l'emporte. Pas plus tard qu'en 2017, Eric Schmidt, président-directeur général de la société mère de Google, Alphabet⁶, a reconnu le rôle des opérations de classement algorithmique de Google dans la diffusion d'informations corrompues. « Il y a une ligne que nous ne pouvons pas vraiment franchir »⁷, a-t-il déclaré. « Il est très difficile pour nous de comprendre la vérité ». Une entreprise dont la mission est d'organiser et de rendre toutes les informations du monde accessibles en utilisant les systèmes informatiques les plus sophistiqués ne peut pas discerner l'information corrompue.

5. En ligne : <https://www.nytimes.com/2021/10/03/technology/whistle-blower-facebook-frances-haugen.html>

6. En ligne : <https://www.cnbc.com/2017/11/21/alphabets-eric-schmidt-why-google-can-have-trouble-ranking-truth.html>

7. En ligne : <https://www.youtube.com/watch?v=X3VQro6q3u0&t=5131s>

Facebook, le premier disciple

M. Zuckerberg a commencé sa carrière d'entrepreneur en 2003, alors qu'il était étudiant à Harvard. Son site Web, Facemash, invitait les visiteurs à évaluer l'attractivité d'autres étudiants. Il a rapidement suscité l'indignation de ses pairs et le site a été fermé. Puis vinrent TheFacebook en 2004 et Facebook en 2005⁸, quand M. Zuckerberg a attiré ses premiers investisseurs professionnels.

Le nombre d'utilisateurs de Facebook a rapidement augmenté, mais pas ses revenus. Comme Google quelques années plus tôt, M. Zuckerberg ne pouvait pas transformer la popularité en profit. Au lieu de cela, il est allé de gaffe en gaffe⁹. Ses violations flagrantes des attentes des utilisateur-trice-s en matière de confidentialité ont provoqué une intense réaction du public¹⁰, des pétitions et des actions collectives. M. Zuckerberg semblait comprendre que la réponse à ses problèmes se trouvait dans l'extraction de données humaines, sans consentement, au profit des annonceurs, mais les complexités de cette nouvelle logique lui échappaient.

Il s'est tourné vers Google pour obtenir des réponses.

En mars 2008, M. Zuckerberg a embauché la directrice de la publicité en ligne de Google, Sheryl Sandberg¹¹, comme bras droit. Mme Sandberg avait rejoint Google en 2001 et jouait un rôle clé dans la révolution du capitalisme de surveillance. Elle a dirigé¹² la mise en place du moteur publicitaire de Google, AdWords, et de son programme AdSense, qui ont généré ensemble la majeure partie des 16,6 milliards de dollars de revenus de l'entreprise en 2007.

Multimillionnaire chez Google au moment où elle a rencontré M. Zuckerberg, Mme Sandberg avait une appréciation avisée des immenses opportunités de Facebook pour l'extraction de riches données prédictives. « Nous avons de meilleures informations que quiconque. Nous connaissons le sexe, l'âge, l'emplacement, et ce sont des données réelles, contrairement à ce que les autres déduisent », a expliqué Mme Sandberg, selon David Kirkpatrick dans *The Facebook Effect*.

L'entreprise avait de meilleures données et des données réelles parce qu'elle était au premier rang de ce que M. Page avait appelé votre vie entière.

Facebook a ouvert la voie à l'économie de la surveillance en adoptant de nouvelles politiques de confidentialité à la fin de 2009. L'organisation Electronic Frontier Foundation¹³ a averti que les nouveaux paramètres tout le monde éliminaient les options qui restreignaient la visibilité des données personnelles, les traitant plutôt comme étant des informations accessibles au public. TechCrunch¹⁴ a résumé la stratégie de l'entreprise : « Facebook oblige les utilisateur-trice-s à choisir leurs nouvelles options de confidentialité pour promouvoir la nouvelle option tout le monde et pour se dédouaner de tout méfait potentiel à l'avenir. En cas de contrecoup important contre le réseau social, il peut prétendre que les utilisateur-trice-s ont volontairement fait le choix de partager leurs informations avec tout le monde ».

Quelques semaines plus tard, M. Zuckerberg a défendu ces décisions¹⁵ auprès d'un intervieweur de TechCrunch. « Plusieurs entreprises seraient piégées par les conventions et leurs héritages. Nous avons décidé ce que seraient les normes sociales désormais et nous avons foncé », s'est-il vanté.

M. Zuckerberg a juste foncé parce qu'il n'y avait pas de lois pour l'empêcher de se joindre à Google dans la destruction totale de la vie privée. Si les législateur-trice-s voulaient le sanctionner en tant qu'impitoyable et insatiable profiteur, prêt à utiliser son réseau social contre la société, alors les années 2009 et 2010 auraient été le bon moment de le faire.

Un ordre économique déferlant

Facebook a été le premier disciple, mais pas le dernier. Google, Facebook, Amazon, Microsoft et Apple sont des empires de surveillance privée, chacun avec des modèles commerciaux distincts. Google et Facebook sont des entreprises de données et de surveillance capitaliste à l'état pur. Les autres opèrent dans d'autres secteurs d'affaires, par exemple, le secteur des données, des services, des logiciels et des produits physiques. En 2021, ces cinq géants américains de la technologie représentent cinq des six plus grandes entreprises¹⁶ cotées en bourse dans le monde.

À l'aube de la troisième décennie du 21^e siècle, le capitalisme de surveillance est l'institution économique dominante de notre époque. En l'absence de lois pour le contrebalancer, ce système gère presque tous les aspects de l'activité humaine dans le monde numérique. Les bénéfices de la surveillance propulsent maintenant l'économie de la surveillance dans l'économie normale, soit celle de l'assurance, du commerce de détail, du secteur bancaire et de la finance, de l'agriculture,

8. En ligne : <https://www.nytimes.com/2005/05/26/business/students-startup-draws-attention-and-13-million.html>

9. En ligne : <https://www.wsj.com/articles/SB120465155439210627>

10. En ligne : <https://www.theguardian.com/technology/blog/2009/sep/21/facebook-privacy>

11. En ligne : <https://money.cnn.com/2008/04/11/technology/facebook-sandberg.fortune/>

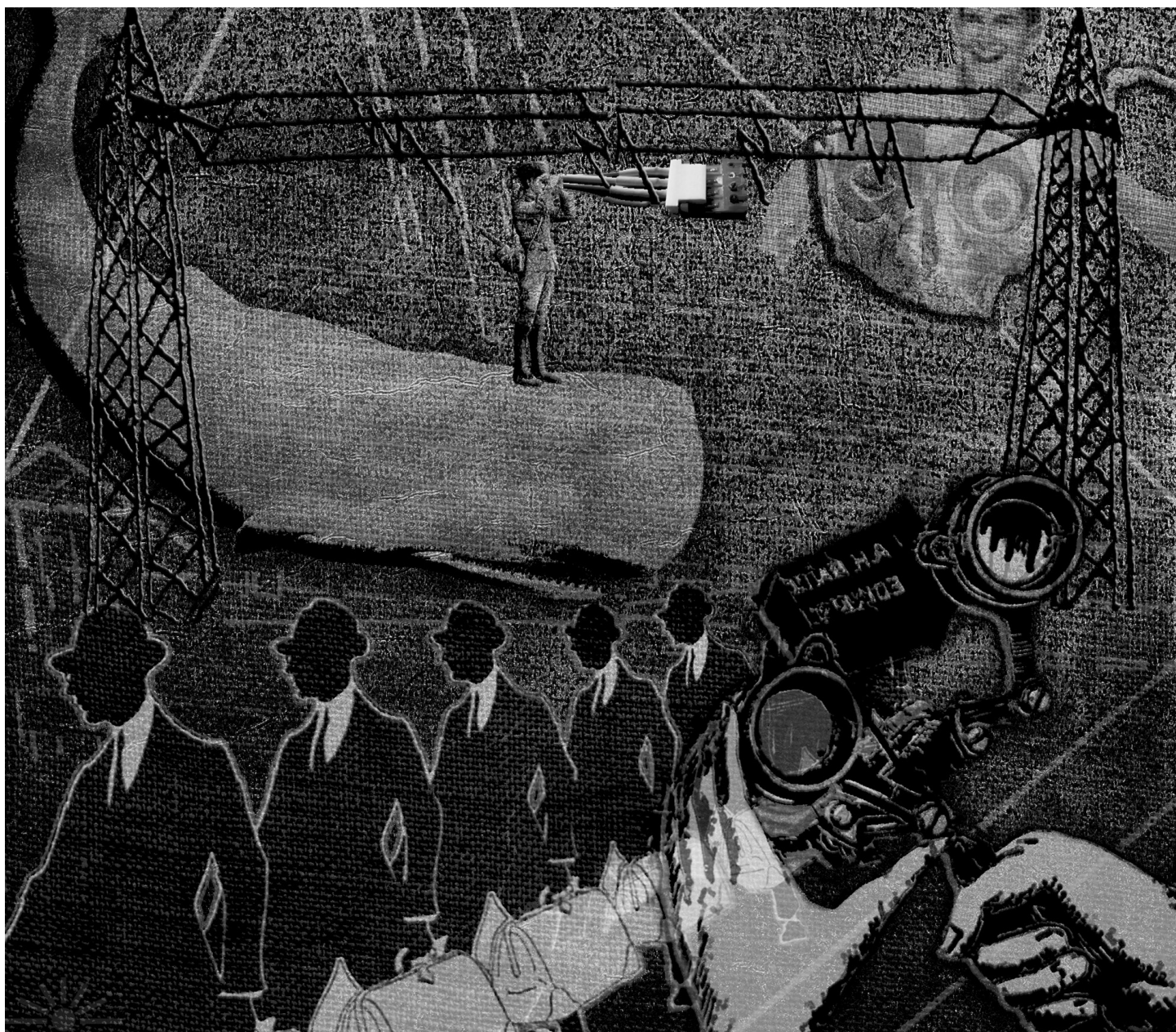
12. En ligne : <https://www.nytimes.com/2008/03/04/technology/04cnd-facebook.html>

13. En ligne : <https://www.eff.org/deeplinks/2009/12/facebook-new-privacy-changes-good-bad-and-ugly>

14. En ligne : <https://tcn.ch/3NeZLgI>

15. En ligne : <https://archive.nytimes.com/www.nytimes.com/external/readwriteweb/2010/01/10/10readwriteweb-facebook-zuckerberg-says-the-age-of-privac-82963.html>

16. En ligne : <https://www.visualcapitalist.com/the-biggest-companies-in-the-world-in-2021/>



Crédit : AK Rockefeller, dreaming is believing, CC BY-SA 2.0.

de l'automobile, de l'éducation, des soins de santé et plus. Aujourd'hui, toutes les applications et tous les logiciels, aussi anodins qu'ils puissent sembler, sont conçus pour maximiser la collecte de données.

Historiquement, de grandes concentrations de pouvoir corporatif ont été associées à des préjudices économiques. Mais quand les données humaines sont la matière première et que les prédictions du comportement humain en sont le produit, alors les dommages sont sociaux plutôt qu'économiques. Le problème est que ces nouveaux dommages sont habituellement vus comme des phénomènes distincts, sans liens les uns avec les autres, ce qui les rend impossibles à résoudre. En fait, chaque étape de dommages engendre les conditions pour l'étape suivante.

À l'aube de la troisième décennie du 21^e siècle, le capitalisme de surveillance est l'institution économique dominante de notre époque. En l'absence de lois pour le contrebalancer, ce système gère presque tous les aspects de l'activité humaine dans le monde numérique.

Tout commence par l'extraction. Pour un ordre économique basé sur l'extraction de données humaines, à grande échelle et de manière cachée, la destruction de la vie privée est une condition inéluctable de ses opérations commerciales. Une fois la vie privée mise au rancart, ces données humaines mal acquises sont concentrées dans les entreprises privées, où elles sont considérées comme des actifs d'affaires à déployer à volonté.

L'effet social est une nouvelle forme d'inégalité, reflétée par l'asymétrie colossale entre ce que ces entreprises savent de nous et ce que nous savons d'elles. L'ampleur de cette asymétrie est illustrée dans un document de Facebook coulé en 2018¹⁷, qui décrit son centre d'intelligence artificielle comme ingérant des billions de points de données comportementales chaque jour et produisant six millions de prédictions comportementales chaque seconde.

Ensuite, ces données humaines sont transformées en armes, sous forme d'algorithmes de ciblage conçus de manière à maximiser l'extraction, ces algorithmes sont alors retournés contre les sources humaines de ces données, sans qu'elles s'en doutent afin d'accroître leur engagement. Les mécanismes de ciblage ont un impact dans la vraie vie, parfois avec de graves conséquences. Par exemple, selon les Facebook Files¹⁸, M. Zuckerberg utilise ses algorithmes pour renforcer ou perturber le comportement de milliards de personnes. La colère est récompensée ou ignorée. Les reportages journalistiques deviennent plus fiables ou déjantés. Les éditeurs prospèrent ou dépérissent. Le discours politique devient plus laid ou plus modéré. Les gens vivent ou meurent.

Parfois, le brouillard se dissipe et révèle le dommage ultime : le pouvoir croissant des géants de la technologie prêts à utiliser leur contrôle sur les infrastructures essentielles d'information afin de concurrencer les législateur-trice-s démocratiquement élu-e-s pour la domination de la société. Au début de la pandémie, par exemple, Apple et Google¹⁹ ont refusé d'adapter leurs systèmes d'exploitation pour héberger des applications de recherche des contacts développées par les autorités de santé publique et soutenues par des élus. En février, Facebook a fermé plusieurs de ses pages en Australie comme marque de refus de négocier²⁰ avec le Parlement australien au sujet des redevances pour les contenus d'information.

C'est pourquoi, lorsqu'il s'agit du triomphe de la révolution du capitalisme de surveillance, ce sont les législateur-trice-s de toutes les démocraties libérales, en particulier des États-Unis, qui portent le plus lourd fardeau de responsabilité. Ils ont permis au capital privé de gouverner nos espaces d'information pendant deux décennies de croissance spectaculaire, sans aucune loi pour l'enraver.

Il y a cinquante ans, l'économiste conservateur Milton Friedman²¹ exhortait les cadres américains : « Il n'y a qu'une seule et unique responsabilité sociale de l'entreprise : utiliser ses ressources et s'engager dans des activités conçues pour augmenter ses profits tant qu'elles respectent les règles du jeu ». Même cette doctrine radicale n'envisageait pas la possibilité d'une absence de règles.

Parfois, le brouillard se dissipe et révèle le dommage ultime : le pouvoir croissant des géants de la technologie prêts à utiliser leur contrôle sur les infrastructures essentielles d'information afin de concurrencer les législateur-trice-s démocratiquement élu-e-s pour la domination de la société.

La contre-révolution de la démocratie

Les sociétés démocratiques déchirées par les inégalités économiques, la crise climatique, l'exclusion sociale, le racisme, les urgences de santé publique et l'affaiblissement des institutions ont un long chemin à parcourir avant d'atteindre la guérison. Nous ne pouvons pas résoudre tous nos problèmes en même temps, mais nous n'en résoudrons jamais aucun, à moins de nous rétablir le caractère sacré de l'intégrité de l'information et de la fiabilité des communications. Le fait d'abdiquer nos espaces d'information et de communication au capitalisme de surveillance est à l'origine de la métacrise de toute démocratie, car elle fait obstacle à la résolution de toutes les autres crises.

Ni Google, ni Facebook, ni aucune autre entreprise dans ce nouvel ordre économique n'avait comme objectif de détruire la société, pas plus que l'industrie des combustibles fossiles n'avait comme objectif de détruire la Terre. Par contre, comme pour le réchauffement climatique, les géants de la technologie et leurs compagnons de route sont prêts à traiter leurs effets destructeurs sur les personnes et la société comme étant des dommages collatéraux, le produit malheureux, mais inévitable, d'opérations économiques parfaitement légales qui ont produit certaines des entreprises les plus riches et les plus puissantes de l'histoire du capitalisme.

17. En ligne : <https://theintercept.com/2018/04/13/facebook-advertising-data-artificial-intelligence-ai/>

18. En ligne : <https://www.wsj.com/articles/the-facebook-files-11631713039>

19. En ligne : <https://www.politico.eu/article/google-apple-coronavirus-app-privacy-uk-france-germany/>

20. En ligne : <https://www.ft.com/content/cac1ff54-b976-4ae4-b81046c29ab26096>

21. En ligne : <https://www.nytimes.com/1970/09/13/archives/a-friedman-doctrine-the-social-responsibility-of-business-is-to.html>

Où en sommes-nous aujourd'hui? La démocratie est le seul ordre institutionnel doté de l'autorité et du pouvoir légitimes pour nous faire changer de trajectoire. Si l'idéal de l'autogouvernance humaine doit survivre au siècle numérique, alors toutes les solutions pointent vers une seule solution : une contre-révolution démocratique. Mais à la place des habituelles listes d'épicerie de solutions, les législateur-trice-s doivent procéder avec une compréhension claire de l'adversaire : une hiérarchie unique des causes économiques et de leurs dommages sociaux.

Nous ne pouvons pas nous débarrasser des dommages sociaux ultérieurs à moins de rendre illégaux leurs fondements économiques. Cela signifie que nous devons aller au-delà des moyens pris actuellement qui visent les conséquences, comme la modération des contenus et le contrôle des contenus illégaux. De tels remèdes ne traitent que les symptômes, sans contester la légitimité de l'extraction des données humaines, alors que celle-ci finance le contrôle privé des espaces d'information de la société. De la même manière, des solutions structurelles, telles que le démantèlement des géants de la technologie, peuvent être utiles dans certains cas, mais elles n'affectent pas les opérations économiques sous-jacentes du capitalisme de surveillance.

Les débats autour de la réglementation des géants de la technologie devraient plutôt se concentrer sur les fondements de l'économie de surveillance, c'est-à-dire l'extraction secrète de données humaines à partir de domaines de la vie qui étaient autrefois considérés privés.

Où en sommes-nous aujourd'hui?

La démocratie est le seul ordre institutionnel doté de l'autorité et du pouvoir légitimes pour nous faire changer de trajectoire.

Les solutions centrées sur la réglementation de l'extraction sont neutres. Elles ne menacent pas la liberté d'expression. Au contraire, elles libèrent le discours social et les flux de l'information de la sélection artificielle d'opérations commerciales qui visent à maximiser le profit et favorisent la corruption de l'information au détriment de son intégrité. Elles restaurent le caractère sacré des communications sociales et de l'expression individuelle.

Sans extraction secrète, il n'y a pas de concentration illégitime de connaissances sur les personnes. S'il n'y a pas de concentration des connaissances, il ne peut y avoir d'algorithmes de ciblage. Sans ciblage, des entreprises ne peuvent plus contrôler et gérer les flux de l'information et le discours social, ni façonner le comportement humain pour favoriser leurs intérêts. La réglementation de l'extraction éliminerait les dividendes de la surveillance et donc les incitatifs financiers.

Alors que les démocraties libérales ont commencé à relever le défi de réglementer les espaces d'information d'aujourd'hui, détenus par des intérêts privés, nous avons besoin de législateur-trice-s prêts à s'engager dans une réflexion unique autour de questions bien plus fondamentales. Comment devons-nous structurer et gouverner l'information, la connectivité et la communication dans un siècle numérique démocratique? Quelles nouvelles chartes des droits, quels nouveaux cadres législatifs et quelles nouvelles institutions sont requis pour garantir que la collecte et l'utilisation des données servent les besoins véritables des individus et de la société? Quelles mesures protégeront les citoyens contre un pouvoir non redevable sur l'information, qu'il soit exercé par des entreprises privées ou par des gouvernements?

Les démocraties libérales devraient prendre les choses en main, car elles ont le pouvoir et la légitimité pour le faire. Mais elles doivent savoir que leurs alliés et collaborateurs incluent les peuples de toutes les sociétés qui luttent contre un futur dystopique.

L'entreprise qu'est Facebook peut changer de nom ou de dirigeant-e-s, mais elle ne changera pas volontairement son modèle économique.

Est-ce que l'appel à réglementer Facebook dissuadera les législateur-trice-s de procéder à une remise en cause plus approfondie? Ou provoquera-t-il un sentiment d'urgence accru? Allons-nous enfin rejeter les vieilles réponses et nous libérer pour poser les nouvelles questions, en commençant par celle-ci : que faut-il faire pour que la démocratie survive au capitalisme de surveillance?

Allons-nous enfin rejeter les vieilles réponses et nous libérer pour poser les nouvelles questions, en commençant par celle-ci : que faut-il faire pour que la démocratie survive au capitalisme de surveillance?

Lexique du capitalisme de surveillance

Martine Éloy, militante au comité surveillance des populations, IA et droits humains de la LDL et membre du CA de 2002 à 2022

Les données prédictives

Les *données prédictives* sont les données du *surplus comportemental* qui permettent au GAFAM (Google, Apple, Facebook, Amazon et Microsoft) de prédire nos comportements.

Droits épistémiques

Le développement du capitalisme de surveillance rend impératif de définir un nouveau droit – un droit qui garantit à chaque personne la souveraineté sur son expérience personnelle. C'est ce que nous nommons les *droits épistémiques*, qui pourraient se résumer ainsi, « je connais et je décide qui connaît mon expérience personnelle ».

Par le biais des mécanismes utilisés à notre insu pour capturer, produire et analyser les données, et pour, par la suite, influencer nos comportements, le capitalisme de surveillance porte atteinte à notre *agentivité*. L'*agentivité* représente notre capacité d'avoir un pouvoir sur notre expérience en tant qu'être humain, pouvoir que nous étions auparavant les seuls à détenir.

Dividuels

Ce terme fait référence à l'image de nous-même projetée par nos données biométriques, par exemple, celles mobilisées par les services douaniers. Comme l'explique Gilles Deleuze, ces données ne sont que l'ombre de nous-mêmes, des *dividuels*, c'est-à-dire une traduction partielle de notre réalité sous la forme du nombre.

Externalités du capitalisme de surveillance

Une externalité est une conséquence imprévue et inconnue d'une action. Par exemple, la production d'automobiles a contribué à la crise climatique. La crise climatique est une externalité de la production automobile. Dans le domaine du numérique, Google nous permet d'avoir accès rapidement à une quantité énorme d'informations, mais ceci produit des externalités, telles que la modification des comportements, l'addiction, la désinformation, la perte de la capacité de jugement moral indépendant. Les externalités du capitalisme de surveillance sont synonymes, en quelque sorte, d'effets collatéraux.

Gouvernementalité algorithmique

Selon Antoinette Rouvroy et Thomas Berns, ce serait un type de rationalité (a)normative et (a)politique reposant sur la récolte, l'agrégation et l'analyse automatisée de données en quantités massives de manière à modéliser, anticiper et affecter à l'avance les comportements possibles.

Marchandises fictionnelles

Ce concept, développé par Karl Polanyi, économiste de la première moitié du XXe siècle, souligne le fait que la nature qui nous entoure (la forêt, les rivières, l'air, etc.) n'est pas en elle-même une marchandise, mais qu'elle est devenue *marchandise* par l'effet du capitalisme. Shoshana Zuboff reprend ce terme en le référant aux comportements humains, qui ne sont pas des marchandises en soi, mais qui le sont devenus par l'effet du capitalisme de surveillance (parfois aussi nommé *capitalisme algorithmique*).

Pouvoir instrumentarien

Le *pouvoir instrumentarien* fait référence au pouvoir que les entreprises du capitalisme de surveillance ont de façonner nos comportements. C'est une nouvelle forme de pouvoir qui s'inscrit dans nos vies et dans la société.

Surplus comportemental

Au début, les compagnies collectaient des données personnelles. En les collectant, elles obtenaient, sans le savoir, toutes sortes d'autres informations qu'elles n'avaient pas cherchées. C'était un *surplus*. Puis, certain-e-s ont pensé qu'il était possible d'utiliser ce *surplus* à des fins utiles. Aujourd'hui, les données personnelles ne représentent qu'une infime partie, et la moins importante des informations que les compagnies détiennent sur nous. Chaque empreinte que nous laissons dans le monde numérique, chaque trace que nous laissons de notre activité en ligne comme – nos expressions faciales, nos comportements, nos goûts, notre orientation sexuelle, etc. – est extraite et analysée pour prédire nos comportements. C'est ce qu'on nomme le *surplus comportemental*.

À la lumière du droit international des droits de la personne

Silviana Cocan, docteure en droit, chargée de cours et chercheuse postdoctorale, Faculté de droit, Udm et militante au comité surveillance des populations, IA et droits humains de la LDL

L'émergence du capitalisme de surveillance est étroitement liée aux progrès technologiques, notamment dans le domaine du numérique, qui n'ont pas été anticipés par le droit international des droits de la personne. Le cadre juridique international protège principalement le droit à la vie privée et avait vocation initialement à imposer à la charge des États des obligations internationales de protection, sans toutefois prendre en considération le rôle joué par les entreprises privées. Ainsi, l'article 12 de la *Déclaration universelle des droits de l'homme* (1948) et l'article 17 du *Pacte international relatif aux droits civils et politiques* (1966) soulignent l'interdiction des « immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance [et des] atteintes illégales à son honneur et à sa réputation ». Ces dispositions consacrent également le droit de toute personne à « la protection de la loi contre de telles immixtions ou de telles atteintes ».

Néanmoins, la protection de la vie privée et des données personnelles dans l'espace numérique exploité par des entreprises privées, qui échappent au contrôle étatique, soulèvent de nombreux enjeux. Le droit international des droits de la personne s'adresse en premier lieu aux États et à leurs organes, qui sont tenus de s'y conformer et de veiller à ce que des tiers ne portent pas atteinte aux droits et libertés garantis. Il est vrai que dans les Principes directeurs relatifs aux entreprises et aux droits de l'homme (2011), les Nations Unies avaient souligné que les entreprises étaient tenues de respecter les droits de la personne, de minimiser les incidences négatives de leurs activités et de prévoir de mesures de réparation ou de collaborer à leur mise en œuvre en cas d'atteintes aux droits de la personne. Or, le capitalisme de surveillance s'est développé en l'absence d'un cadre juridique contraignant et dans l'incertitude des obligations à la charge des entreprises opérant dans le domaine numérique.

Une nouvelle matière première

L'exploitation massive des données personnelles des utilisateurs a permis progressivement l'émergence d'un nouveau modèle de publicité ciblée en exploitant les informations de profils d'utilisateurs¹, d'une redéfinition du consentement libre et éclairé des consommateurs face à des

conditions générales d'utilisation complexes et d'un manque de transparence dans le traitement des données personnelles. La collecte de ces données sous couvert d'une utilisation gratuite et illimitée des services a permis la concrétisation d'un « nouvel ordre économique qui revendique l'expérience humaine comme matière première gratuite à des fins de pratiques commerciales dissimulées d'extraction, de prédiction et de vente² ».

Les Nations Unies se sont emparées de la question en envisageant le droit à la vie privée à l'ère du numérique dans un rapport du Haut-Commissariat aux droits de l'homme (2018)³. Il a été souligné que les technologies numériques, mises au point principalement par le secteur privé, en exploitant en permanence les données personnelles, « pénètrent progressivement dans le tissu social, culturel, économique et politique des sociétés modernes ». Le rapport mettait également en garde contre l'émergence de cet « environnement numérique intrusif dans lequel les États et les entreprises commerciales seront en mesure de surveiller, d'analyser, de prédire et même de manipuler le comportement des personnes à un degré sans précédent » (§ 1).

Or, le capitalisme de surveillance s'est développé en l'absence d'un cadre juridique contraignant et dans l'incertitude des obligations à la charge des entreprises opérant dans le domaine numérique.

En ce qui concerne la responsabilité des entreprises de respecter le droit à la vie privée, le rapport recommandait aux États de se doter d'une législation adéquate et de mettre en place des autorités indépendantes en charge de surveiller les pratiques des secteurs public et privé, tout en leur accordant un pouvoir d'enquête sur les atteintes, la possibilité de recevoir des plaintes des particuliers ou d'organisations et d'imposer des amendes et d'autres sanctions effectives en cas de traitement illégal des données à caractère personnel (§ 61, points b), d) et e)). Or, c'est précisément à l'égard de l'adoption

1. En ligne : <https://www.monde-diplomatique.fr/2019/01/ZUBOFF/59443>

2. En ligne : <https://www.lapresse.ca/societe/2020-12-06/notre-droit-au-temps-futur.php>

3. En ligne : <https://www.ohchr.org/fr/calls-for-input/reports/2018/report-right-privacy-digital-age>

de telles mesures que les États peinent à suivre le rythme effréné des innovations numériques et technologiques. Face aux lacunes du droit et à la lenteur des réformes législatives, les entreprises privées se trouvent investies d'un pouvoir démesuré, en l'absence d'une régulation stricte et d'un réel mécanisme de sanction en cas de violations des droits de la personne, dans un monde dématérialisé où la logique du profit, combinée à celle de la liberté numérique, ne connaissent aucune limite.

Dans une résolution adoptée le 7 octobre 2019, le Conseil des droits de l'homme des Nations Unies a réitéré les engagements des États et des entreprises en ce qui concerne le respect des droits de la personne dans le contexte de la collecte, du stockage, de l'utilisation, du partage et du traitement des données personnelles (§ 6 et § 8)⁴. Le plus récent rapport du Haut-Commissariat des Nations Unies aux droits de l'homme était consacré à l'« Incidence des nouvelles technologies sur la promotion et la protection des droits de l'homme dans le contexte des rassemblements, y compris des manifestations pacifiques » (2020)⁵. En effet, l'impact des nouvelles technologies dépasse le cadre de la protection de la vie privée en ayant aussi des répercussions sur le droit de réunion pacifique et la liberté de manifester, notamment lorsqu'il est question des systèmes de reconnaissance faciale exploités par les entreprises privées et qui sont utilisés pour surveiller les activités des acteurs de la société civile (§ 39). Ce sont ainsi les fondements de la démocratie et les principes de l'État de droit qui peuvent être impactés par l'exploitation des données personnelles, comme cela a pu être le cas avec la société Cambridge Analytica qui a procédé à la collecte des données personnelles des utilisateurs de Facebook et utilisées à des fins politiques pour influencer l'issue des élections⁶.

Face aux lacunes du droit et à la lenteur des réformes législatives, les entreprises privées se trouvent investies d'un pouvoir démesuré, en l'absence d'une régulation stricte et d'un réel mécanisme de sanction en cas de violations des droits de la personne, dans un monde dématérialisé où la logique du profit, combinée à celle de la liberté numérique, ne connaissent aucune limite.

De multiples défis

Même en l'absence d'un instrument juridique contraignant destiné à réguler le capitalisme de surveillance, les principes protecteurs du droit international des droits de la personne sont susceptibles de contraindre les entreprises privées à se conformer à des standards minimums en matière d'exploitation des données personnelles. Les défis persistants et les difficultés qui paraissent incontournables découlent principalement de l'exploitation des données personnelles dans un environnement dématérialisé. Dans ce cadre, l'identification d'un dommage demeure extrêmement complexe et l'engagement de la responsabilité des acteurs privés très largement hypothétique. Le décalage entre la rapidité des progrès technologiques et la lenteur de la réactualisation de l'encadrement juridique dans les ordres juridiques internes des États a entraîné l'émergence d'une économie de surveillance dans laquelle les données personnelles des utilisateurs sont la monnaie d'échange et la source infinie de profit pour les entreprises privées qui peuvent agir parfois en toute impunité. Si ces entreprises sont tenues de respecter les droits humains dans le cadre de leurs activités, de leur toute-puissance numérique découle l'incapacité des États à les contraindre au respect de leurs obligations en engageant leur responsabilité assortie de véritables sanctions. Ce constat sera vrai aussi longtemps que les cadres juridiques nationaux ne seront pas dotés de mesures législatives appropriées et que les autorités étatiques ne seront pas habilitées à exercer un véritable pouvoir de contrôle de nature à imposer des limites et à contraindre les entreprises privées à une utilisation des données personnelles conforme aux garanties qui s'attachent aux droits et libertés.

Les défis persistants et les difficultés qui paraissent incontournables découlent principalement de l'exploitation des données personnelles dans un environnement dématérialisé.

Vers un premier traité international

Le défi majeur réside dans la capacité des États à imposer, isolément, un encadrement juridique aux acteurs privés qui reposerait uniquement sur le droit interne, alors même que le multilatéralisme et la coopération globale semblent incontournables afin de répondre adéquatement à cette problématique. Si un traité international véritablement

(Suite à la page 25)

4. En ligne : <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/297/53/PDF/G1929753.pdf?OpenElement>

5. En ligne : <https://www.ohchr.org/fr/documents/thematic-reports/ahrc4424-impact-new-technologies-promotion-and-protection-human-rights>

6. En ligne : <https://ici.radio-canada.ca/nouvelle/1090159/facebook-cambridge-analytica-donnees-personnelles-election-politique-campagne-marketing-politique>

Une culture de surveillance

Stéphane Leman-Langlois, professeur titulaire, École de travail social et de criminologie, Université Laval et militant au comité surveillance des populations, IA et droits humains de la LDL

En 2010, quelques-uns de mes étudiants et moi avons demandé à plus de 600 personnes qui descendaient de nouveaux *métrobus* du Réseau de transport de la capitale s'ils avaient remarqué l'une des sept caméras installées à bord (en plus de deux microphones) durant leur voyage. Près de 40 % d'entre elles nous ont répondu que non, bien qu'un dôme de 20 cm de diamètre trône déjà à l'entrée, où il faut s'arrêter pour régler son déplacement. L'immense majorité des voyageurs interrogés n'y voyaient par ailleurs aucun inconvénient.

Cette indifférence généralisée s'explique par plusieurs facteurs, dont la simple réduction de la taille des caméras et leur intégration esthétique aux endroits où elles sont installées (couleur, matériau, forme). Elle a également souvent été expliquée par l'évolution des perceptions face à la surveillance en général, surtout due à l'omniprésence de stratégies et d'appareils, qui l'a banalisée. À voir les sondages, cette indifférence semble bien s'étendre à la plupart des nouvelles formes de surveillance, même si l'immense majorité d'entre nous se disent aussi préoccupés par la protection de leur vie privée. Cette contradiction s'amointrit sensiblement lorsqu'on constate que les répondants sont rarement suffisamment *préoccupés* pour prendre des mesures de protection de base (chiffrement, stratégies et logiciels d'anonymisation, appareils et applications sécurisés, etc.). Cela dit, il n'y a jamais eu de glorieux passé libre de surveillance, avec lequel le contraste serait évident. L'être humain est social et cherche à exister sous l'œil de ses semblables. Les résidents du petit village québécois d'antan, avec la proximité, les commérages et la curiosité, finissaient par tout savoir au sujet de tout le monde. Bref, nous étions déjà indifférents à ces formes de surveillance communautaires – omniprésentes, profondes et totales.

L'apparition d'une culture généralisée de surveillance

Objectivement, la différence est qu'aujourd'hui à la fois la collecte, la distribution et la conservation des données ne sont plus (uniquement) horizontales, entre pairs. Certains ont argumenté que la société de l'information a simplement pris la relève lors de la disparition des formes traditionnelles de surveillance. Quoi qu'il en soit, les informations collectées sont désormais bien davantage que de simples souvenirs et acquièrent une existence propre, sujettes à une foule d'usages secondaires, aspirées par de multiples entités non redevables, voire tout bonnement inconnues. C'est dans ce contexte qu'il

faut noter l'apparition récente et le développement fulgurant d'une industrie très prospère fondée sur un aspect ou un autre de ce flux intarissable de données personnelles. C'est l'aspect central du concept de capitalisme de surveillance, qu'il faut donc comprendre comme une émanation d'une culture généralisée de surveillance.

La plus solide fondation de cette culture est notre participation active et volontaire au système, à la fois pour nous offrir à la surveillance des autres, pour les surveiller ou pour réclamer qu'un tiers (gouvernemental ou privé) le fasse pour nous. Recueillir de l'information est la panacée qu'on oppose à toutes les formes de problèmes, de l'intimidation à l'extérieur de l'école à la qualité de l'air à l'intérieur, de la sécurité du logis à son chauffage, à notre santé, notre conduite et notre assurance automobile, la personnalité de nos intérêts amoureux, etc.

Quoi qu'il en soit, les informations collectées sont désormais bien davantage que de simples souvenirs et acquièrent une existence propre, sujettes à une foule d'usages secondaires, aspirées par de multiples entités non redevables, voire tout bonnement inconnues.

Paradoxalement, cette course à la surveillance entraîne sa disparition progressive. Non pas au sens où elle cesse d'exister, mais bien parce qu'elle est intégrée à chacune de nos activités, à un point tel qu'elle cesse peu à peu d'être une pratique autonome. Ceci, surtout parce qu'elle est réalisée à l'aide de dispositifs dont la fonction première est tout autre : le thermostat qui sait si quelqu'un est à la maison, notre application de réseautage qui nous permet de scruter la vie des autres, notre application GPS qui révèle notre position, etc.

Ceci génère bien sûr une foule de données sur nos comportements, et une nouvelle industrie multimilliardaire, au point qu'il tient désormais du lieu commun d'affirmer que *les données sont le nouveau pétrole*. L'État et ses agences ont bien sûr aussi noté ce développement alléchant et, des polices municipales exploitant Facebook aux révélations de Snowden, on a vu et revu qu'il est toujours plus efficace de détourner les données déjà produites par cet assemblage disparate que de développer et d'opérer des systèmes de surveillance dédiés.

Une perte de valeur éventuelle

Il faut toutefois noter que, contrairement à la plupart des ressources naturelles exploitables, dont la quantité diminue à mesure de leur extraction, la quantité d'information personnelle disponible à un usage industriel est vouée à une augmentation exponentielle. L'internet des objets, où pullulent les appareils *intelligents* produisant et échangeant des informations sur leur utilisateur, générera un flux toujours plus considérable d'information. La simple loi de l'offre prévoit donc une perte proportionnelle de sa valeur, sans compter qu'en moyenne chaque nouvel élément d'information est de moins en moins révélateur (au sens où il ajoute peu, voire rien, au modèle statistique actuariel déjà façonné). Notons de plus que la puissance des publicités ciblées vendues sur les plateformes numériques est en déclin accéléré. Les utilisateurs ne cliquent tout simplement plus dessus, et lorsqu'ils le font c'est par erreur ou par curiosité : elles génèrent donc de moins en moins de revenus¹. Bref, à court ou à moyen terme le *capitalisme de surveillance*, du moins tel que nous le connaissons aujourd'hui, se dirige vers le proverbial mur de brique. Avant de s'en réjouir, par contre, il faut bien comprendre que depuis 20 ans l'internet au complet est structuré pour et par ce système, et pourrait bien s'écrouler avec lui.

L'État et ses agences ont bien sûr aussi noté ce développement alléchant et, des polices municipales exploitant Facebook aux révélations de Snowden, on a vu et revu qu'il est toujours plus efficace de détourner les données déjà produites par cet assemblage disparate que de développer et d'opérer des systèmes de surveillance dédiés.

Une culture de surveillance pérenne?

Quoi qu'il en soit, notre culture de surveillance survivra aisément à la disparition ou à l'arrivée de modèles différents d'économie des données personnelles. Heureusement, elle non plus n'est pas aussi blindée, hégémonique qu'il n'y paraît. Elle a entre autres donné naissance à une culture de contre-surveillance : la conscience de la dissémination de renseignements à notre sujet inspire certains d'entre nous à prendre une série de mesures de contournement et de subversion, comme l'inscription de fausses données, la création de comptes multiples et autres stratégies visant à corrompre leur *double numérique* et à farcir d'erreurs les banques de données. La démocratisation des outils de surveillance a aussi multiplié nos capacités de *sous-veillance*,

comme dirait Steve Mann, avec lesquelles le citoyen réussit à faire pencher la balance un peu plus du côté de la redevabilité des institutions, notamment via la nouvelle visibilité de la police, qui travaille désormais sous les caméras du public. Enfin les Manning, Snowden et autres sonneurs d'alerte sont rapidement, inéluctablement et irrémédiablement diffusés dans l'ensemble de la planète. D'un point de vue citoyen, notre culture de surveillance a simplement besoin d'une nouvelle impulsion qui redirigerait son attention globale plus solidement vers les complexes institutionnels publics, privés et hybrides. On devra également y faire germer la notion que ce système de surveillance est un large *réseau*, donc plus ou moins solide, plus ou moins opportuniste, plus ou moins capitaliste, libéral ou totalitaire, mais dont les citoyens eux-mêmes constitueront toujours l'immense majorité des nodes.

(Suite de la page 23)

contraignant serait plus approprié, il serait nécessaire que les négociations aboutissent tout d'abord et qu'il recueille un nombre suffisant de ratifications de la part des États qui s'engageraient à une mise en application effective au niveau national grâce à la modification de leur cadre législatif. Dans le cadre du Conseil de l'Europe, des négociations devraient commencer au mois de mai 2022 en vue d'aboutir à l'adoption d'un texte contraignant sur l'intelligence artificielle⁷. Il s'agirait du premier traité international, mais si le texte venait à être adopté, il pourrait réunir au maximum 46 États (à la suite de la récente exclusion de la Russie du Conseil de l'Europe qui sera effective en septembre 2022). Parallèlement, un projet de règlement sur l'intelligence artificielle⁸ a été proposé par la Commission dans le cadre de l'Union européenne en avril 2021. Il faudra suivre les développements de ce processus, qui pourrait aboutir à une législation harmonisée sur l'intelligence artificielle et qui serait immédiatement applicable dans les 26 États membres de l'Union. En ce qui concerne les Nations Unies, si des négociations n'ont pas encore été initiées en vue de l'adoption d'un texte contraignant, un moratoire a été demandé sur l'utilisation de certains systèmes d'intelligence artificielle⁹ face aux risques de violations graves des droits de la personne. Dans le cadre de l'UNESCO, la première norme mondiale sur l'éthique de l'intelligence artificielle a été adoptée par 193 États au mois de novembre 2021¹⁰. Bien qu'il ne s'agisse pas d'un texte ayant une force obligatoire, les États ont une responsabilité de principe dans la mise en œuvre des recommandations. Ainsi, pour l'instant, au niveau universel, des instruments de droit souple (*soft law*) définissent des principes qui ne sont pas juridiquement contraignants, mais qui pourraient servir de guide aux autorités nationales dans la détermination de mécanismes de protection et la réactualisation des législations.

7. En ligne : <https://justice.legibase.fr/actualites/veille-juridique/actualite-de-la-regulation-internationale-de-lintelligence-artificielle-123050>

8. En ligne : <https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX:52021PC0206>

9. En ligne : <https://news.un.org/fr/story/2021/09/1103762>

10. En ligne : <https://news.un.org/fr/story/2021/11/1109412>

1. Tim Hwang, *The Subprime Attention Crisis : Advertising and the Time Bomb at the Heart of the Internet*, FSG Originals, New York, 2020.

Réforme des lois de protection des renseignements personnels

Pas de quoi contrecarrer le modèle d'affaires des GAFAM

Anne Pineau, militante au comité surveillance des populations, IA et droits humains de la LDL

La protection des renseignements personnels (RP) fait partie intégrante du droit à la vie privée reconnu par les chartes des droits. Il assure le contrôle des individus sur leurs données et leur droit « de déterminer eux-mêmes à quel moment les renseignements les concernant sont communiqués, de quelle manière et dans quelle mesure¹ ».

Les lois de protection des RP adoptées dans les années 80 et 90 posent les principes de cette protection : consentement de la personne concernée (PC) à la cueillette de ses RP; minimisation de la collecte aux seuls RP nécessaires; respect des finalités et destruction des données après réalisations des fins; sécurisation et confidentialité des RP; accès de la PC à ses données.

Mais le développement fulgurant de l'informatique, des réseaux sociaux et de l'intelligence artificielle ont fait naître d'autres enjeux et rendu ces lois en partie obsolètes. Une sérieuse mise à jour s'imposait, particulièrement pour contrecarrer l'accumulation effrénée de données par les plateformes numériques (GAFAM), à des fins publicitaires, politiques ou autres.

La réponse du gouvernement québécois a consisté dans le dépôt du *Projet de loi 64* (PL 64)², modifiant tant la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (LAI)³ que la *Loi sur la protection des RP dans le secteur privé*⁴. Largement inspiré du *Règlement général sur la protection des données* (RGPD) du Parlement européen, le PL 64 apporte plusieurs correctifs comme celle de la notion de RP qui est élargie ; elle s'étend aux informations permettant d'identifier une personne physique, directement ou indirectement. Les exigences sont aussi resserrées en matière de consentement (qui doit être manifeste, libre, éclairé, donné à des fins spécifiques et distinctement pour chacune des fins); mais du même souffle

le PL 64 multiplie les cas où les RP pourront être utilisés ou transmis sans consentement.

De plus, tout produit ou service technologique disposant de paramètres de confidentialité devra, par défaut, assurer le plus haut niveau de confidentialité; mais cette obligation ne s'applique pas aux témoins de connexion (*cookies*). Lors de la collecte de RP, les fonctions d'identification, de localisation ou de profilage qu'une entreprise ou un organisme public (OP) utilise éventuellement devront être désactivées par défaut; ces fonctions devront donc être activées par la PC, si elle y consent. Ensuite, toute personne qui fait l'objet d'une décision « fondée exclusivement sur un traitement automatisé » doit être informée de ce fait, de même que des RP et des principaux facteurs utilisés pour rendre la décision; contrairement au RGPD, il ne sera pas possible de s'opposer au traitement entièrement automatisé d'une décision.

Un élément important à souligner est la perte du pouvoir de contrôle de la Commission d'accès à l'information (CAI) en matière de Recherche; la communication de RP à cette fin sera possible sur simple *Évaluation des facteurs relatifs à la vie privée* (EFVP), une sorte d'étude d'impact maison menée par l'entreprise ou l'organisme; on passe donc d'un régime d'autorisation (par un tiers indépendant) à un système d'autorégulation. Le tout pour la communication sans consentement de RP possiblement très sensible.

Du côté du secteur privé, les entreprises ou OP ont le droit de conserver et d'utiliser les RP, sans consentement, lorsque les fins pour lesquelles ils ont été recueillis sont accomplies, à condition de les anonymiser ; ce qui est contraire au principe de base de la destruction des RP après réalisation des fins. Cela est d'autant plus inadmissible que l'anonymisation est un procédé qui n'est pas infallible.

Les entreprises et OP ont aussi l'obligation d'aviser les personnes touchées par un bris de confidentialité lorsque l'incident présente un risque de préjudice sérieux; la personne n'a cependant pas à être avisée tant que cela serait susceptible d'entraver une enquête policière et comme ces enquêtes peuvent être longues, les victimes pourraient très bien être avisées du vol de leurs données longtemps après le fait.

1. R. c. Spencer, 2014 CSC 43, 2 RCS 212, par. 40.

2. Maintenant adopté sous le nom de chapitre 25 (Loi 25) des lois de 2021.

3. *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, chapitre A-2.1 (LAI)

4. *Loi sur la protection des renseignements personnels dans le secteur privé* (Loi privée), chapitre P-39.1

Notons une augmentation importante des sanctions pénales en cas de contravention à la loi par une entreprise (amende maximale de 25M\$ ou 4 % du chiffre d'affaires mondial.) La CAI se voit accorder un pouvoir de sanction administrative (montant maximal de sanction pour une entreprise pouvant atteindre 10M\$ ou 2 % du chiffre d'affaires mondial). L'entreprise pourra toutefois s'engager auprès de la CAI à prendre les mesures nécessaires pour remédier au manquement, auquel cas elle ne pourra faire l'objet d'une sanction administrative.

Ces dispositions entreront en vigueur graduellement d'ici 2024. Si on peut noter quelques avancées intéressantes, le PL 64 comporte aussi plusieurs reculs; et ces modifications législatives s'avèrent nettement insuffisantes pour répondre aux enjeux actuels.

Le PL 64 laisse en plan plusieurs questions. La biométrie, notamment l'utilisation de la reconnaissance faciale, est ignorée⁵. Pourtant un contrôle accru de cette technologie s'imposait au vu des affaires Clearview AI⁶ et du Centre commercial Place Ste-Foy⁷. La CAI faisait d'ailleurs valoir dans son mémoire sur le PL 64 que « la législation actuelle ne permet pas d'encadrer adéquatement certaines utilisations de cette technologie⁸ ».

Si la désactivation par défaut de certains outils de traçage doit être saluée, on peut toutefois craindre que l'inactivation de ces outils affecte délibérément le fonctionnement ou la qualité du service ou du produit technologique.

Par ailleurs, le traitement de données massives par intelligence artificielle soulève des enjeux sociétaux. L'édiction de règles de transparence et d'explication des modes de fonctionnement de ces systèmes est essentielle.

Les algorithmes de personnalisation peuvent conduire les individus à s'enfermer dans leurs certitudes et miner la capacité de mener des débats publics éclairés. Les chambres d'écho des réseaux sociaux peuvent, quant à elles, amoindrir la circulation de l'information et la diversité d'opinions et mener à de la manipulation. En outre, des algorithmes mal calibrés peuvent entretenir – voire aggraver – des pratiques discriminatoires. De nombreux cas prouvent que des vices de conception ou l'usage de données historiquement biaisées peuvent conduire l'algorithme à reproduire, voire aggraver, des attitudes et des comportements discriminatoires. La LDL réclamait une divulgation publique et proactive du mode de fonctionnement de ces systèmes et leur surveillance par audit indépendant. Le PL 64 ne répond pas à ces préoccupations.

Le PL 64 ne révolutionne rien. Il conforte un modèle d'affaires fondé sur l'extraction de données et l'accaparement des traces numériques que nous laissons derrière nous. En y mettant toutefois quelques formes, du côté du consentement. Pas de quoi limiter ou proscrire la logique d'accumulation de données comportementales ni rameuter les troupes de lobbyistes à l'emploi des GAFAM.

Nous sommes ici à des lieux de ce que Shoshana Zuboff appelle de ses vœux, à savoir, des « lois qui rejettent la légitimité fondamentale des déclarations du capitalisme de surveillance et qui mettent fin à ses opérations les plus primaires, y compris la restitution illégitime de l'expérience humaine sous forme de données comportementales⁹ ».

5. Sauf en ce qui concerne le préavis, à la CAI, de constitution d'une banque de données biométriques.

6. En ligne : <https://www.cai.gouv.qc.ca/la-commission-ordonne-clearview-ai-de-cesser-ses-pratiques-de-reconnaissance-faciale-non-conformes/>

7. En ligne : <https://www.journaldequebec.com/2020/10/31/ivanhoe-cambridge-a-abandonne-lidee>

8. En ligne : https://www.cai.gouv.qc.ca/documents/CAI_M_projet_loi_64_modernisation_PRP.pdf

9. Shoshana Zuboff, *L'âge du capitalisme de surveillance*, Zulma, 2020, p. 463.

Forces policières et capitalisme de surveillance

Dominique Peschard, militant au comité surveillance des populations, IA et droits humains et président de la LDL de 2010 à 2015

Dans les mois suivant les attentats du 11 septembre 2001, le Pentagone, à travers son agence de recherche *Defense Advanced Research Projects Agency* (DARPA), mettait sur pied le projet *Total Information Awareness* (TIA). Dirigé par l'Amiral à la retraite John Poindexter, le projet visait, ni plus ni moins, qu'à compiler toutes les informations disponibles sur chaque individu : achats, transactions financières, lectures, sites Web fréquentés, appels téléphoniques, réseau d'ami-e-s, activités, voyages, prescriptions médicales, etc. En reliant toutes ces informations, Poindexter prétendait pouvoir identifier le prochain terroriste et l'arrêter avant qu'il ne prenne l'avion.

Sécurité nationale et agences de renseignements

Le tollé qui a suivi la révélation et la dénonciation de ce programme par le New York Times a entraîné l'abolition du projet par le Congrès en 2002. Le projet n'était pas mort pour autant – il allait simplement être poursuivi secrètement par la *National Security Agency* (NSA). Et le développement du capitalisme de surveillance dans les deux décennies suivantes allait fournir aux agences les masses de données sur les populations dont rêvait Poindexter. En 2013, Edward Snowden dévoilait l'étendue de l'appareillage d'espionnage de la NSA et l'existence d'outils, comme XKeyscore qui permet à la NSA d'avoir accès à presque tout ce qu'un-e internaute fait sur Internet, et PRISM qui donne accès aux données de Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple.

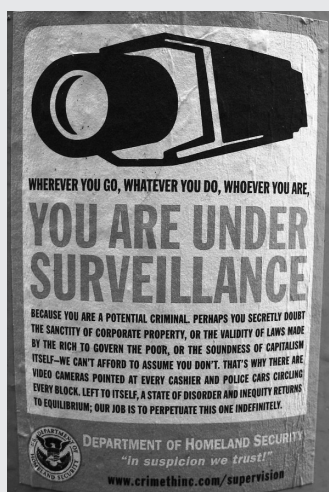
Rappelons que la NSA est le chef de file d'un consortium de partage de renseignements, les *Five Eyes*, formé des agences d'espionnage des États-Unis, de la Grande-Bretagne, de l'Australie, de la Nouvelle-Zélande et du Canada (le Centre de la sécurité des télécommunications).

Depuis l'adoption du PL C-59 en 2017, le Service canadien du renseignement de sécurité (SCRS) peut légalement recueillir des ensembles de données sur les Canadien-ne-s. Il suffit que le SCRS juge ces renseignements « utiles » et qu'il ait « des motifs raisonnables de croire » qu'ils sont « accessibles au public ». Un pouvoir défini de manière aussi vague ouvre la voie à la constitution de banques de données sur l'ensemble de la population. Et ce, alors que les services policiers et de renseignements ne cessent de prétendre que les informations personnelles perdent leur caractère privé à partir du moment où elles sont accessibles dans l'espace virtuel.

Forces policières et centres de surveillance

La mise sur pied de centres de surveillance ne se limite pas aux agences de renseignements et de sécurité nationale. Les forces policières se dotent de plus en plus de centres d'opération numérique qui analysent en temps réel toutes les informations disponibles pour diriger les interventions des policiers sur le terrain¹. Ces centres s'inspirent des *fusion*

1. En ligne : <https://breachmedia.ca/canadian-police-expanding-surveillance-powers-via-new-digital-operations-centres/>



Traduction de l'affiche créée par www.crimethinc.com/supervision

Où que vous alliez, quoi que vous fassiez, qui que vous soyez, vous êtes sous surveillance parce que vous êtes un criminel potentiel. Peut-être doutez-vous du caractère sacré de la propriété des entreprises, de la validité des lois élaborées par les riches pour gouverner les pauvres, ou du bien-fondé du capitalisme lui-même – nous ne pouvons pas nous permettre de supposer que vous ne doutez pas. C'est pourquoi il y a des caméras vidéo pointées sur chaque caissier et des voitures de police qui font le tour de chaque quartier. Laisse à lui-même, un état de désordre et d'inégalité revient à l'équilibre ; notre travail consiste à perpétuer celui-ci indéfiniment.

Crédit : *You are under surveillance*, TheeErin, CC BY-ND 2.0.



Crédit : André Querry

centres mis en place par le *Homeland Security* aux États-Unis après les attentats du 11 septembre 2001. Les informations traitées proviennent autant des banques de données des services de police, que d'images de caméras de surveillance publiques et privées, et d'informations extraites des réseaux sociaux par des logiciels conçus à cette fin. Notons que les banques de données des forces policières contiennent des données sur des citoyen-ne-s qui n'ont jamais été condamné-e-s pour un quelconque crime, y compris des données issues d'interpellations fondées sur le profilage racial, social ou politique.

Notons que les banques de données des forces policières contiennent des données sur des citoyen-ne-s qui n'ont jamais été condamné-e-s pour un quelconque crime, y compris des données issues d'interpellations fondées sur le profilage racial, social ou politique.

Systèmes de décisions automatisées et maintien de l'ordre prédictif

Les forces policières ont de plus en plus recours à des systèmes de décisions automatisées (SDA) pour exploiter les masses croissantes de données dont elles disposent. Des SDA sont utilisés, entre autres, pour cibler les lieux où des délits sont susceptibles de se produire, ou les individus susceptibles d'en commettre. Ces systèmes sont particulièrement problématiques lorsqu'ils incorporent la petite criminalité et les incivilités dans leurs modèles. Ce genre de délit sans victime, comme la consommation d'alcool par des mineurs, est plus susceptible d'être commis dans des espaces publics de quartiers défavorisés où les personnes ne jouissent pas

d'espaces privés pour socialiser. En ciblant ces quartiers, on arrête des personnes pour des infractions qui passent inaperçues dans des quartiers plus favorisés. Le SDA est alimenté de données qui renforcent un biais répressif envers certaines populations. Comme le dit Cathy O'Neil, dans son livre sur les biais des algorithmes, « Le résultat, c'est que nous criminalisons la pauvreté, tout en étant convaincu que nos outils sont non seulement scientifiques, mais également justes² ». Les quartiers pauvres sont également ceux où on retrouve une plus grande proportion de personnes racisées, ce qui alimente également les biais racistes des SDA et des interventions policières.

Le système de décisions automatisées (SDA) est alimenté de données qui renforcent un biais répressif envers certaines populations.

Le rôle des entreprises privées

Les logiciels de SDA nécessaires pour interpréter ces masses de données sont fournis par des compagnies comme IBM, Motorola, Palantir, qui ont des liens avec l'armée et les agences de renseignements et d'espionnage. Des compagnies, comme Stingray, fabriquent des équipements qui permettent aux forces policières d'intercepter les communications de téléphones cellulaires afin d'identifier l'utilisateur et même d'accéder au contenu de la communication. Le logiciel Pegasus de la compagnie israélienne NSO permet même de prendre le contrôle d'un téléphone. D'autres entreprises comme Clearview AI et Amazon fournissent même les données de surveillance aux forces policières. Clearview AI a collecté des milliards de photos sur Internet et offre aux forces policières de relier l'image d'une personne à tous les sites où elle apparaît sur le Net. Le Commissaire à la vie privée du Canada a déclaré illégales les actions de Clearview AI au Canada ainsi que l'utilisation de ses services par la Gendarmerie royale du Canada (GRC).

La compagnie Amazon est emblématique du maillage entre le capitalisme de surveillance et les forces policières. Amazon héberge dans son nuage plusieurs programmes de surveillance du *U.S. Department of Homeland Security*. La compagnie a une relation incestueuse avec les forces policières et les agences de renseignement, incluant le partage d'information sur ses utilisateur-trice-s et des contrats gouvernementaux confidentiels³.

Aux États-Unis, le système *Ring* d'Amazon est en voie de constituer un vaste système de surveillance de l'espace public par les forces policières. Les sonnettes *Ring* sont dotées de caméras qui scrutent en permanence l'espace public devant le

2. Cathy O'Neil et Cédric Villani, *Algorithmes, La bombe à retardement*. Les Arenes Ed, 2018.

3. ACLU, *Sidewalk : The Next Frontier of Amazon's Surveillance Infrastructure*. En ligne : <https://www.aclu.org/news/privacy-technology/sidewalk-the-next-frontier-of-amazons-surveillance-infrastructure/>

domicile. L'utilisateur d'une sonnette *Ring* accepte par défaut qu'Amazon rende les images de sa sonnette accessibles aux services de police — pour s'y soustraire l'utilisateur doit avoir recours à une procédure de désinscription (opting out), ce que beaucoup de personnes ne font pas. Plusieurs millions de ces sonnettes ont déjà été installées aux États-Unis et environ 2 000 services policiers ont déjà conclu des ententes avec Amazon pour avoir accès à ces caméras⁴ — le tout sans mandat judiciaire! Bien que *Ring* n'utilise pas la reconnaissance faciale, Amazon a développé cette technologie et l'a déjà vendue à des forces policières.

Avec le projet *Sidewalk*⁵, Amazon pousse l'intégration des données issues des appareils « intelligents » encore plus loin⁶. Avec *Sidewalk*, chaque appareil consacre une petite partie de sa bande passante et devient un pont dans un réseau de communication parallèle relié aux serveurs d'Amazon. Des compagnies, par exemple de vêtements connectés, peuvent choisir de devenir des partenaires d'Amazon et de rendre leurs dispositifs compatibles avec *Sidewalk*. Selon l'*American Civil Liberties Union* (ACLU), les documents d'Amazon indiquent que la politique d'utilisation des données sera la même avec *Sidewalk* qu'avec *Ring*. Pour l'ACLU, ce système est un véritable cauchemar pour les droits et libertés.

Bien que le système *Ring* n'utilise pas la reconnaissance faciale, Amazon a développé cette technologie et l'a déjà vendue à des forces policières.

Le manque de transparence

Tous ces développements se font dans un contexte d'absence de transparence des forces policières et de débats publics. Lorsque confrontées à des demandes portant sur leurs pratiques et sur les outils qu'elles utilisent, le réflexe premier des forces policières est de refuser de répondre sous prétexte qu'elles n'ont pas à dévoiler leurs méthodes d'enquête, ou de mentir, comme l'a fait initialement la GRC à propos de son utilisation de Clearview AI.

Que savons-nous des outils informatiques utilisés par les forces policières pour définir leurs priorités d'intervention, organiser leurs patrouilles, et que font-ils avec les données recueillies lors d'interpellations, effectuées sans fondement légal? Quels impacts ces outils ont-ils sur les différentes formes de profilage pratiquées par les corps de police comme le Service de police de la Ville de Montréal?

4. En ligne : <https://www.theguardian.com/commentisfree/2021/may/18/amazon-ring-largest-civilian-surveillance-network-us>

5. Ne pas confondre avec le projet de quartier intelligent *Sidewalk Labs* de Google.

6. ACLU, *Sidewalk : The Next Frontier of Amazon's Surveillance Infrastructure*. En ligne : <https://www.aclu.org/news/privacy-technology/sidewalk-the-next-frontier-of-amazons-surveillance-infrastructure/>

Les pratiques des forces policières et les outils qu'elles utilisent doivent respecter les droits reconnus dans les chartes. Ces pratiques et ces outils sont d'intérêt public et les forces policières ne doivent pas se soustraire à leur obligation de rendre des comptes en invoquant des arguments fallacieux.

Tous ces développements se font dans un contexte d'absence de transparence des forces policières et de débats publics.

Des pratiques à débattre et à encadrer

La masse de données que le capitalisme de surveillance a engendrée à des fins lucratives constitue une mine d'or pour les services de police et de sécurité nationale qui fonctionnent de plus en plus selon une logique de surveillance généralisée des populations et de maintien de l'ordre prédictif.

Ces pratiques vont à l'encontre du principe de présomption d'innocence selon lequel une personne ne peut faire l'objet de surveillance policière sans motifs. Elles contournent également l'exigence d'un mandat judiciaire pour les formes de surveillance intrusives. En ciblant les quartiers et les populations jugés à risque, elles renforcent les différentes formes de profilage policier discriminatoire.

Il n'est pas suffisant de savoir si les forces policières utilisent tel ou tel système de décision automatisé et à quelles fins. Les algorithmes doivent aussi être publics et soumis à un examen réglementaire indépendant permettant d'en repérer les failles et les biais. L'argument du secret commercial n'est pas recevable alors que l'utilisation de ces algorithmes soulève des enjeux de droits humains.

Les tribunaux et les organismes de protection de la vie privée ont statué à maintes reprises que la protection de la vie privée ne disparaît pas du moment qu'une personne se trouve dans l'espace public, qu'il soit physique ou virtuel⁷. Il faut cependant beaucoup plus que des décisions à la pièce, comme celle du Commissaire à la vie privée du Canada dans l'affaire Clearview AI, pour encadrer le travail policier dans ce nouvel environnement. Le cadre légal qui gouverne la police doit être mis à jour pour protéger la population contre une surveillance à grande échelle. La surveillance de masse doit être proscrite et des techniques particulièrement menaçantes, comme la reconnaissance faciale, doivent être interdites tant qu'il n'y aura pas eu de débat public sur leur utilisation.

Ces pratiques vont à l'encontre du principe de présomption d'innocence selon lequel une personne ne peut faire l'objet de surveillance policière sans motifs.

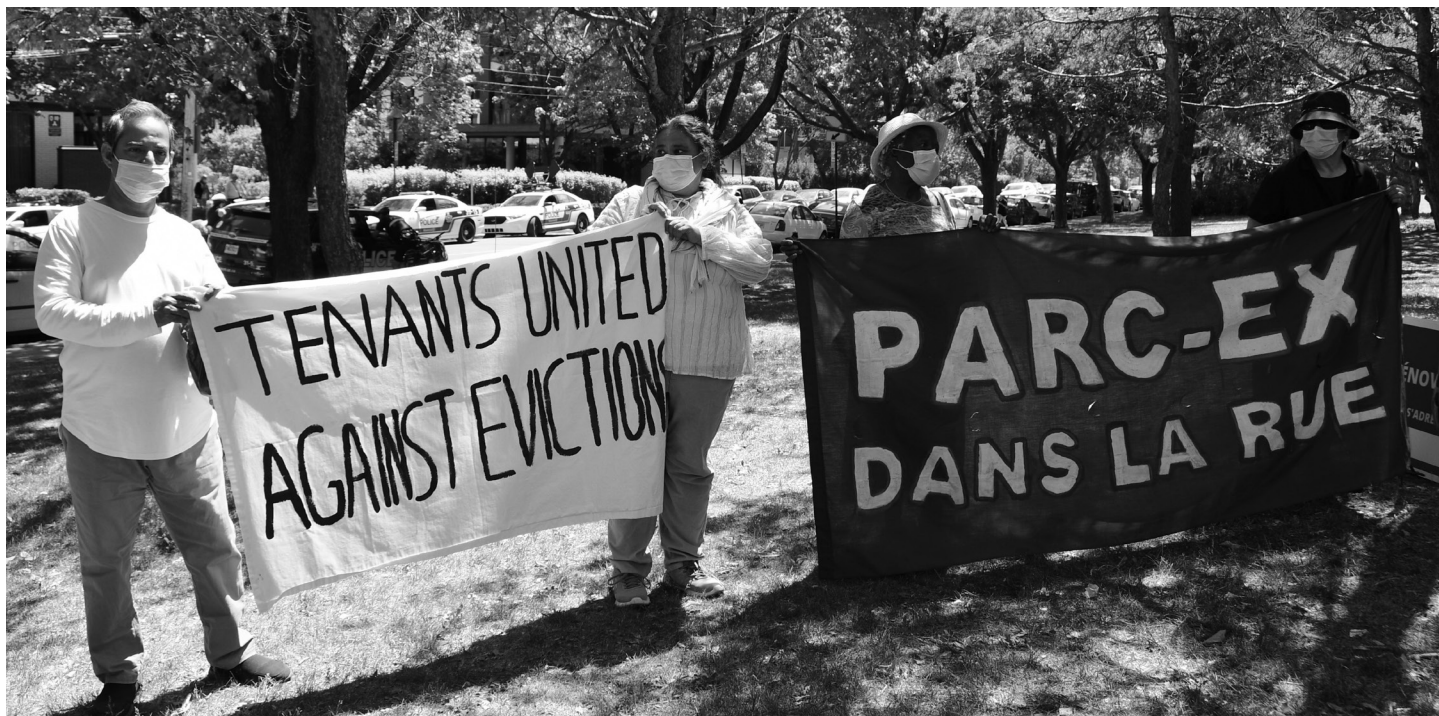
7. En ligne : <https://liguedesdroits.ca/droit-a-la-vie-privée-la-jurisprudence-de-la-cour-suprême/>

Le Big Data contre le droit à un chez-soi?

Le secteur de l'intelligence artificielle et l'embourgeoisement de Parc-Extension

Collectif de chercheur-euse-s et militant-e-s

Alessandra Renzi, Tamara Vukov, Emanuel Guay, Sepideh Shahamati, Yannick Baumann, Simone Chen, et Montserrat Emperador Badimon



Crédit : André Querry

Le secteur de l'intelligence artificielle (IA) occupe une place de plus en plus importante parmi les stratégies de développement économique à Montréal, notamment par le biais de partenariats entre les pouvoirs publics, le milieu de la recherche et des entreprises spécialisées dans les hautes technologies et les données massives (*big data*). Le gouvernement provincial a annoncé, en 2019, l'octroi de 80 millions de dollars sur cinq ans à l'Institut québécois de l'intelligence artificielle Mila, auquel s'ajoute un financement fédéral de 44 millions, par l'entremise de l'Institut canadien de recherches avancées¹. Les dernières années ont aussi été marquées par l'établissement, dans le quartier Marconi-Alexandra, de compagnies telles que Element AI, Microsoft et IVADO, ainsi que par l'ouverture du Campus MIL en septembre

2019 et la mise en chantier d'un Centre d'innovation en intelligence numérique. Ces deux établissements, associés à l'Université de Montréal, visent entre autres à soutenir l'écosystème de l'IA au Québec.

L'essor de Montréal comme un pôle international de l'IA est souvent présenté comme une excellente nouvelle, dont nous devrions tou-te-s nous réjouir. Des craintes ont toutefois été partagées par rapport aux risques que représente ce secteur, comme en témoigne la *Déclaration de Montréal pour un développement responsable de l'intelligence artificielle*. Cette déclaration, promue entre autres par le professeur Yoshua Bengio, compte parmi ses principes le bien-être, la solidarité, la participation démocratique, l'équité, l'inclusion de la diversité, la responsabilité et le développement soutenable².

1. En ligne : <https://www.lapresse.ca/affaires/economie/quebec/201901/29/01-5212755-montreal-inaugure-sa-cite-de-lintelligence-artificielle.php>

2. En ligne : <https://www.declarationmontreal-iaresponsable.com/la-declaration>.



Crédit : André Query

Nous sommes des chercheur-euse-s et des militant-e-s qui travaillent en étroite collaboration avec différentes initiatives communautaires à Parc-Extension. Ce quartier est adjacent aux nouvelles installations de l'Université de Montréal, il est situé à proximité de Marconi-Alexandra et il est caractérisé par un taux de pauvreté élevé, une proportion importante de sa population issue de l'immigration récente et un embourgeoisement qui s'accélère depuis quelques années. Nous souhaitons mettre en lumière ici l'impact du secteur de l'IA sur l'embourgeoisement de Parc-Extension, puis ses conséquences pour les locataires à faible revenu du quartier. Nous concluons notre article en proposant trois pistes de solution, soit une collaboration plus étroite entre le milieu de la recherche et les initiatives communautaires locales, l'élaboration d'une entente sur les avantages communautaires (*community benefits agreement*) entre le secteur de l'IA et les résident-e-s des quartiers concernés, ainsi qu'une plus grande transparence de la part de ce secteur et des pouvoirs publics.

Le secteur de l'IA et l'embourgeoisement de Parc-Extension

Les recherches que nous menons à Parc-Extension, en collaboration avec des organismes locaux, nous ont permis de constater que le secteur de l'IA et les nouvelles installations de l'Université de Montréal qui leur sont associées contribuent grandement à l'embourgeoisement de Parc-Extension, ce qui correspond à des tendances observées dans d'autres villes comme New York, Los Angeles et San Francisco³. L'arrivée d'entreprises de haute technologie et de nouveaux campus universitaires favorise une hausse importante de la valeur des propriétés dans les quartiers environnants et la venue de nouvelles résidentes et de nouveaux résidents plus fortunés, y compris des personnes qui travaillent pour ces entreprises et ces universités. Cela encourage les propriétaires à augmenter de façon radicale les loyers et à effectuer des rénovictions, qui consistent en l'éviction de locataires afin de rénover un logement et d'accueillir ensuite d'autres locataires avec des revenus plus élevés. Le rapport *MIL façons de se faire évincer : l'Université de Montréal et la gentrification à Parc-Extension*, paru en juin 2020, a mis en lumière la réorientation du marché locatif de Parc-Extension autour des jeunes professionnel-le-s et des étudiant-e-s, qui se manifeste notamment dans les loyers offerts et les stratégies publicitaires utilisées par les propriétaires et les promoteurs immobiliers⁴.

3. En ligne : <https://theconversation.com/universities-can-squeeze-out-low-income-residents-in-cities-like-montreal-131834>

4. Projet de cartographie anti-éeviction de Parc-Extension. *MIL façons de se faire évincer. L'Université de Montréal et la gentrification à Parc-Extension*. Montréal, 2020, p. 15-20.

Un rapport produit récemment par le *Digital Divides Project* et le Réseau de recherche-action communautaire de Parc-Extension (CBAR) examine l'impact du secteur de l'IA sur l'embourgeoisement de Parc-Extension, ainsi que les conséquences dévastatrices de ce processus pour les locataires à faible revenu⁵. Ces locataires sont de plus en plus souvent obligés de se reloger, après une éviction, dans des appartements trop petits pour le nombre de personnes qui les habitent, de couper dans des dépenses essentielles comme la nourriture ou les médicaments afin de pouvoir payer des loyers plus élevés qu'auparavant, ou encore de quitter le quartier, en rendant ainsi plus difficile leur accès à différents services et réseaux de soutien. Ces réseaux et ces services sont particulièrement importants pour les résident-e-s issu-e-s de l'immigration récente, puisqu'ils ont de plus fortes probabilités d'être allophones et d'avoir un statut précaire. La manière dont l'IA se développe actuellement nuit au respect de plusieurs principes contenus dans la *Déclaration de Montréal*, notamment l'équité et la solidarité.

La collecte de données, les ententes sur les avantages communautaires et la transparence du secteur de l'IA et des pouvoirs publics

Bien que les réalités exposées ici soient préoccupantes, nous pensons que des solutions peuvent être mises de l'avant pour assurer une meilleure prise en compte des besoins et des aspirations des locataires de Parc-Extension. Une première avenue à envisager est l'établissement de collaborations entre des personnes issues du milieu de la recherche et des initiatives communautaires, afin d'encourager des projets et des stratégies de collecte de données qui contribuent aux luttes des résident-e-s, ainsi qu'au travail des organismes locaux. Nous avons ainsi lancé, en novembre 2021, deux cartes interactives portant sur les évictions et les mobilisations pour le droit au logement à Parc-Extension, en partenariat avec le Comité d'action de Parc-Extension (CAPE). Ces cartes visent tant à montrer l'ampleur et les conséquences de la crise du logement dans le quartier qu'à promouvoir des initiatives menées par les locataires pour contrer cette crise⁶. Une deuxième avenue qui mérite notre attention est l'élaboration d'une entente sur les avantages communautaires, pour s'assurer que les résident-e-s de Parc-Extension bénéficient réellement de l'expansion du secteur de l'IA, avec des offres d'emploi ciblées et des investissements dans des projets locaux, notamment dans le domaine du logement social et communautaire. Une troisième avenue à envisager est l'adoption d'une approche plus transparente par le secteur de l'IA et les pouvoirs publics. Par exemple, des projets d'IA qui sont jugés nuisibles par les communautés concernées pourraient être l'objet d'un moratoire.

Ces trois avenues font partie d'un ensemble plus large de solutions qui permettraient au secteur de l'IA de reconnaître pleinement sa responsabilité sociale et d'en tirer les conséquences qui s'imposent. Les stratégies proposées ici doivent être menées en collaboration avec les résident-e-s, et les organismes de Parc-Extension, en respectant leur leadership et en encourageant leur participation tout au long du processus, notamment avec une compensation adéquate pour leur temps. Nous ne pouvons pas tolérer, en tant que société, un modèle d'innovation technologique qui externalise les coûts associés à son développement et qui affecte négativement les locataires à faible revenu, en niant ainsi leur contribution à la vie sociale et culturelle de nos quartiers et leur droit à la ville.

Une deuxième avenue qui mérite notre attention est l'élaboration d'une entente sur les avantages communautaires, pour s'assurer que les résident-e-s de Parc-Extension bénéficient réellement de l'expansion du secteur de l'IA, avec des offres d'emploi ciblées et des investissements dans des projets locaux, notamment dans le domaine du logement social et communautaire.

5. Digital Divides Project et Réseau de recherche-action communautaire de Parc-Extension. *The Impact of Montreal's AI Ecosystems on Parc-Extension: Housing, Environment and Access to Services*. Montréal, 2022.

6. Projet de cartographie anti-éviction de Parc-Extension. *Cartographie*. En ligne : <https://antievictionmontreal.org/fr/maps/>

La ville intelligente : Qu'ossa donne?

Lyne Nantel, chercheuse et autrice de l'*Avis sur l'utilisation de systèmes de décision automatisée par la ville de Montréal* du Conseil jeunesse de Montréal¹

Entrevue réalisée par Martine Éloy, militante au comité surveillance des populations, IA et droits humains de la LDL et membre du CA de 2002 à 2022 et **Dominique Peschard**, militant au comité surveillance des populations, IA et droits humains de la LDL et président de 2007 à 2015



Crédit : Arturo Castaneyra sur Unsplash

Qu'entend-on par ville intelligente?

L'expression « ville intelligente » (VI) est apparue au tournant des années 2000, elle visait à marquer un virage. Les villes allaient dorénavant s'appuyer sur les nouvelles technologies pour leur développement, pour assurer leurs services et l'ensemble de leur fonctionnement.

Dans les faits, une VI n'est rien de plus qu'une ville qui prend le tournant numérique, comme on le voit dans l'ensemble des sphères de la vie. Il n'y a donc pas un modèle, mais des modèles, certains où la technologie et le numérique sont d'abord des finalités et d'autres où le numérique est simplement un moyen parmi d'autre de développer les services urbains.

Toutefois, il faut noter que la ville intelligente, la *smart city*, a été largement promue comme une sorte de mot d'ordre qui allait favoriser des solutions et des innovations aux enjeux environnementaux, de mobilité, de gestion des ressources, etc. Dans ce modèle de développement urbain les entités privées jouent un rôle important en tant que fournisseurs de services technologiques. Ces entreprises ont intérêt à faire miroiter un *solutionnisme technologique* pour faire face aux défis que rencontrent les villes. Comme on le dit dans l'*Avis* :

Cette adhésion, cette confiance à l'endroit des technologies comme réponse à un problème fait écho à une idée répandue : le solutionnisme technologique. Cette notion traduit une tendance forte à convertir les problèmes sociaux complexes

1. L'*Avis* peut être consulté à : https://ville.montreal.qc.ca/pls/portal/docs/page/cons_jeunesse_fr/media/documents/Avis_SDA.pdf

en problèmes technologiques. Selon ce raisonnement, le développement continu de la science des données conduit à des outils de décision toujours plus performants, précis et efficaces.

Qu'entend-on par un système de décision automatisé (SDA)? Pouvez-vous donner des exemples de SDA dans le contexte d'une ville?

Un système de décision automatisé (SDA) est une notion de plus en plus utilisée qui renvoie à l'ensemble des données, des algorithmes et du traitement qui est fait dans le but d'aider, d'assister ou de remplacer la prise de décision humaine. C'est une notion plus précise que l'intelligence artificielle. Pour l'Avis au Conseil jeunesse de Montréal, nous avons retenu la définition de SDA du Conseil du trésor du Canada.

Au niveau des administrations publiques, les SDA sont de plus en plus exploités dans divers domaines: la justice, la police, les finances, les assurances, en éducation, assistance sociale; immigration... pour faire des prédictions, générer des scores ou des niveaux de risques. À l'échelle des villes, l'utilisation de SDA est variable en raison des compétences et du rôle des municipalités qui diffèrent d'un pays à l'autre.

Prenons l'exemple de systèmes automatisés de synchronisation des feux de circulation basés sur des capteurs de densité de la circulation. Ces systèmes peuvent améliorer la fluidité du trafic automobile, mais est-ce l'objectif visé? Veut-on investir seulement dans l'amélioration du trafic automobile ou dans des alternatives à l'automobile? L'implantation du numérique devrait à mon avis plutôt augmenter les options de mobilité pour l'ensemble des citoyens.nes sans exclure des personnes qui n'utilisent pas ces outils de l'offre de services publics.

La chercheuse Virginia Eubanks démontre comment des logiciels devant *faciliter* la gestion de ressources pour des personnes en situation d'itinérance peuvent avoir des conséquences négatives pour ces personnes. En effet, à partir de l'indice de vulnérabilité, l'outil d'aide à la décision peut exclure certaines personnes des programmes d'aide prioritaire. Par exemple, une personne qui quitte un établissement carcéral sera classée comme ayant eu un hébergement stable au cours des mois précédents, ce qui abaissera son indice de vulnérabilité et, par conséquent, réduira sa possibilité d'accéder aux ressources d'aide au logement. En fait, le recours au SDA dans ces cas sert à gérer un manque de ressource plutôt que de répondre aux besoins des bénéficiaires.

Les systèmes de réponse automatisés sont souvent présentés comme servant à améliorer le service. La numérisation de certains services risque toutefois de désavantager les personnes qui ne sont pas à l'aise avec ces systèmes ou qui ne possèdent pas les outils technologiques nécessaires pour communiquer en ligne.

Les services de polices sont aussi reconnus pour utiliser un type de logiciel qu'on appelle de *police prédictive*; l'objectif étant de cibler des lieux de manière préventive ou encore d'identifier des individus susceptibles d'avoir des liens avec la criminalité. Jusqu'en 2020, la police de Chicago avait une liste d'individus classés en fonction du niveau de risque qu'ils étaient supposés représenter.

[...] une personne qui quitte un établissement carcéral sera classée comme ayant eu un hébergement stable au cours des mois précédents, ce qui abaissera son indice de vulnérabilité et, par conséquent, réduira sa possibilité d'accéder aux ressources d'aide au logement.

Quels sont les domaines où l'utilisation de SDA pose le plus de danger? Quels sont-ils?

En fait lorsque la décision risque d'avoir un impact sur les droits et libertés des individus et des collectivités, c'est là qu'il y a un danger. Les outils de *police prédictive* présentent de grands risques de discrimination et de profilage racial puisque ces outils utilisent des données de police qui sont déjà biaisées, quand on sait que les personnes racisées sont victimes de profilage et sont plus souvent visées par les interpellations policières.

Il y a aussi des enjeux de vie privée. Prenez les lecteurs automatisés de plaques d'immatriculation qu'utilise le projet pilote de stationnement intelligent de l'Agence de mobilité durable de Montréal. Un traitement croisé de données pourrait permettre de prédire le lieu de travail d'une personne ou encore le lieu de culte qu'elle fréquente. La question est de savoir qui a accès à ces données ou qui peut avoir accès à ces données.

Quand on pense à ville intelligente, on pense au projet Sidewalk Lab de Toronto. Quel était ce projet et pourquoi a-t-il été rejeté?

J'ai évoqué l'intérêt des entreprises privées en tant que fournisseurs de services technologiques pour qui les villes constituent des bancs d'essais intéressants. Les villes manquent souvent de ressources pour améliorer la qualité de leur service et cherchent à augmenter leur attractivité, surtout auprès des entreprises numériques.

Le projet *Quayside Toronto* est emblématique de cette idée de la ville comme laboratoire pour le numérique. Lancé en 2017, *Sidewalk Labs*, l'une des branches d'Alphabet-Google, et l'agence de développement urbain *Waterfront Toronto* se sont

associés pour construire un quartier hyperconnecté et géré en temps-réel où capteurs, données et algorithmes assureraient la gestion de l'énergie, du transport, des déchets... Dans un tel projet, la captation de données est continue. L'opposition au projet a été assez grande¹ et les citoyens et citoyennes réclamaient des réponses quant à la protection et l'utilisation des données. L'absence de réponse et de transparence a fait que ce projet n'a jamais reçu l'acceptabilité sociale pour aller de l'avant et le projet a été abandonné en 2020. En plus de soulever des questionnements importants concernant les partenariats public-privés et les droits de la personne, cet exemple démontre l'importance de concevoir les projets selon des principes démocratiques, participatifs et délibératifs. Il faut que les gens soient informés et ils doivent pouvoir se prononcer, s'exprimer et s'opposer à de tels projets s'ils jugent que ceux-ci ne répondent pas à l'intérêt général et ne respectent pas leurs droits.

Y a-t-il des SDA déjà en opération à Montréal? Y a-t-il des projets en gestation?

C'est la grande question. Est-ce que le Service de Police de la Ville de Montréal (SPVM) utilise des logiciels de police prédictive ou de reconnaissance faciale? La réponse n'est pas claire. On sait que l'accès à des logiciels d'essai est facile. Même si le SPVM n'a pas officiellement fait l'acquisition de ces logiciels, un enquêteur se serait-il servi sur une base individuelle de la reconnaissance faciale pour une enquête?

Comme je vous dis, il est difficile de savoir exactement ce qui se développe, car souvent on innove et on ne pense aux conséquences qu'après coup. On ne se soucie pas d'être transparent, d'expliquer la finalité du projet et de le soumettre au débat public.

Le projet des abribus intelligents débuté en 2018 dans le Laboratoire à ciel ouvert de la vie intelligente (Lab-Vi), impliquant Vidéotron, ETS, le quartier de l'innovation, l'entreprise Ericsson, est un bon exemple. Ces abribus dotés de capteurs biométriques sont présentés comme permettant d'améliorer le service en calculant s'il y a trop de gens qui attendent l'autobus à certains moments. Mais ce même projet inclut aussi des capteurs permettant d'évaluer leurs émotions. Pourquoi? En quoi la reconnaissance des émotions améliore le service public? Quand on lit sur le projet, on apprend que les capteurs permettront aussi de mesurer l'intérêt démontré par les usagers à la vue d'une publicité affichée dans l'abribus, dans le but d'envoyer des publicités ciblées directement sur leurs téléphones mobiles. On peut comprendre l'intérêt de l'entreprise privée pour ce genre de projet, mais les usagers-ères ont-ils consenti à être épié-e-s de la sorte?

1. Une campagne contre le projet *Sidewalks* a été menée notamment par l'Association canadienne des libertés civiles (ACLU) qui avait déposé une poursuite en 2019 contre *Waterfront Toronto*.
En ligne : <https://ccla.org/major-cases-and-reports/torontos-smart-city/#response>

Quels mécanismes et balises devraient être mis en place avant d'implanter des SDA dans les services de la ville?

Parmi la liste des recommandations, il y a la tenue d'un registre des SDA ainsi que des données qui sont collectées dans les espaces publics urbains. Il faut s'avoir ce qui est collecté et à quelles fins. Cette transparence est essentielle.

La transparence ne suffit pas, car on peut être transparent mais ne pas avoir mis en place les mécanismes nécessaires pour évaluer correctement l'impact, la fiabilité et l'efficacité des outils technologiques. Un comité indépendant et représentatif responsable de faire une évaluation et de la rendre publique serait déjà une protection supplémentaire pour les citoyens. Ce n'est pas facile pour tout le monde de connaître les impacts de telle ou telle technologie et de savoir si leurs données sont suffisamment protégées.

On collecte de plus en plus de données. Il faut prendre le temps de réfléchir aux problèmes qu'on souhaite résoudre par l'utilisation de technologies et mieux évaluer les impacts que cela pourrait avoir sur les droits. Il faut développer le réflexe de minimiser la collecte de données aux situations où celle-ci a une réelle utilité.

Enfin, on doit adopter une position ferme et claire pour un moratoire sur l'utilisation de la reconnaissance faciale comme l'ont fait d'autres villes, notamment certaines villes américaines.

La transparence ne suffit pas, car on peut être transparent mais ne pas avoir mis en place les mécanismes nécessaires pour évaluer correctement l'impact, la fiabilité et l'efficacité des outils technologiques.



La dissolution de la société dans le capitalisme de surveillance

Groupe de recherche sur l'information et la surveillance au quotidien (GRISQ)

Jacob Boivin, doctorant en communication, UQÀM, chercheur au GRISQ et

Laurence Grondin-Robillard, doctorante en communication, UQÀM, chercheuse et coordonnatrice au GRISQ

La notion de capitalisme de surveillance telle qu'analysée par la sociologue Shoshana Zuboff¹ met au jour des sociétés contemporaines soumises au joug de la circulation de l'information comme seul horizon. Dès lors que nos expériences subjectives quotidiennes sont source de production de données et que l'accroissement, le traitement et l'exploitation de ces dernières sont au cœur de l'accumulation du capital, la totalité du réel se retrouve gouvernée par la surveillance numérique. Les GAFAM² procèdent ainsi à une réduction informationnelle de nos existences menée avec une indifférence radicale pour leurs contenus, pour autant qu'elles génèrent de la donnée. Si cela participe à une oblitération totale de la question du consentement et de la vie privée³, une problématique tout aussi fondamentale transparaît en arrière-plan : une dissolution de la société, du moins tel qu'on l'entend. En ce sens, il est envisageable de traduire la totalité du réel en information : nul besoin de l'orienter politiquement et collectivement, l'agrégation fluidifiée des profils numériques suffit à remplacer le lourd défi du politique.

La dissolution de la société

Les études sur la surveillance ont tendance à faire prévaloir une critique d'inspiration libérale. D'une part, cette dernière est nécessaire, notamment sous l'optique de la transparence des mécanismes algorithmiques et de leurs enjeux de vie privée. D'autre part, elle participe généralement à maintenir la focale sur la figure de l'individu plutôt que sur celle du collectif ou de la société. Pourtant, l'un des plus grands défis du capitalisme de surveillance est bien de contribuer à ce qu'on pourrait appeler une dissolution de la société. Nous faisons ici écho à la disparition tendancielle d'une forme de totalité de référence en rapport à laquelle nous pouvons collectivement définir l'horizon de l'action individuelle par le biais d'une médiation politique : d'un vivre-ensemble. (Ainsi, la société

est-elle de plus en plus représentée comme un système autonome émancipé de la vie politique.) Dans le capitalisme de surveillance, une telle mise en commun est tout simplement remplacée par une médiation technique générant au passage des données numériques. Nous pouvons d'ailleurs penser aux logiques actuarielles qui perdent tout horizon collectif à travers la segmentation individuelle qu'offre l'analyse numérique des comportements. Par exemple, l'analyse des comportements routiers via les systèmes connectés des voitures permet d'ajuster les primes d'assurance au cas par cas plutôt que d'en problématiser la source.

La représentation identitaire par les nombres

Puisque les données numériques constituent le vecteur principal de capitalisation, n'est retenue du réel que sa transcription sous forme de données et de profils numériques. Il s'agit d'un ensemble d'informations chiffrées abstraites qui servent de représentation identitaire (on songe à notre double numérique ou profil d'utilisateur). Pensons aux données biométriques mobilisées par les services douaniers : ces doubles ne sont que l'ombre de nous-mêmes, des dividiuels pour reprendre le terme de Gilles Deleuze, c'est-à-dire une traduction partielle de notre réalité sous la forme du nombre.

Une perte de sens

En effet, les données numériques participent d'une compréhension a-significative des subjectivités, elles traduisent l'action, mais pas la signification de celle-ci. Par exemple, les profils générés par les algorithmes de prédictions policières n'indiquent que la récurrence d'un crime en un certain lieu et non pas les causes psychosociales de sa reproduction. À partir de ce principe de nature signalétique (restreint au niveau de l'action elle-même) plutôt que significative (la finalité et le contexte de l'action) de la donnée numérique, il est envisageable d'extrapoler sur le devenir d'une société fondée sur une captation et une rentabilisation systémique des données : ce à quoi œuvre la surveillance.

1. Shoshana Zuboff, *The age of surveillance capitalism. The fight for a human future at the new frontier of power*, New York, Public Affairs, 2019.

2. Google, Amazon, Facebook, Apple, Microsoft.

3. Un rapport d'Amnistie Internationale soulignait d'ailleurs en 2019 que le modèle d'affaire des GAFAM (particulièrement Facebook et Google) porte atteinte aux droits humains. En ligne : <https://www.amnesty.org/en/latest/news/2019/11/google-facebook-surveillance-privacy/>



Crédit : André Query

Une gouvernamentalité algorithmique

Cet horizon prend alors la forme de ce que les juristes et philosophes Antoinette Rouvroy et Thomas Berns nomment une gouvernamentalité algorithmique : un type de rationalité (a)normative et (a)politique reposant sur la récolte, l'agrégation et l'analyse automatisée de données en quantités massives de manière à modéliser, anticiper et affecter par avance les comportements possibles⁴. Les recommandations algorithmiques et l'hyperplasticité des offres de consommation qui les accompagnent en donnent un exemple. Ainsi, non seulement les subjectivités ne sont interpellées que par leur double numérique, mais elles sont tendanciellement guidées par des opérations algorithmiques réalisées avec vélocité (en deçà du temps de conscience humaine) et à leur insu. Cela se traduit selon Zuboff par une transition vers un pouvoir qualifié d'instrumentariste⁵. Il ne vise pas l'imposition idéologique par la force, mais l'orientation subtile des comportements par des mécanismes de marché fondés sur une compréhension signalétique du social. Ce dernier ne renvoie plus à une mise en commun qui dépasse les individus, mais plutôt à l'agrégation des actions individuelles sous une forme objectivée. Le contexte, les finalités et les relations en sont alors évincés. En conséquence, la nécessité de la société comme un ensemble de valeurs communes s'évapore. Nul besoin de faire l'épreuve pénible d'un vivre-ensemble s'il est possible de simplement agencer les multiples individualités par le biais de leurs profils numériques. Une simple gestion algocratique suffit, d'autant plus qu'elle est souhaitée, car elle est au fondement d'un processus de valorisation structurant l'économie contemporaine.

Nul besoin de faire l'épreuve pénible d'un vivre-ensemble s'il est possible de simplement agencer les multiples individualités par le biais de leurs profils numériques.

Un exemple de cette dissolution d'un idéal de société symbolique au profil d'une économétrie sans friction transparait dans le projet de physique sociale qu'ambitionne de faire advenir l'informaticien Alex « Sandy » Pentland⁶. Sous prétexte qu'un ensemble d'informations s'échangent notamment à des niveaux non perceptibles pour la conscience humaine (langage corporel, sensations, préjugés, etc.), la médiation technologique (capteurs, algorithmes) serait seule à même de capter la subjectivité objectivement. On s'adresserait en effet directement aux gens plutôt qu'à leurs croyances. Ainsi, avec une surveillance généralisée constituée sous la forme d'un grand système, il serait possible d'aiguiller la société adéquatement et sans les biais de la conscience. Comme le souligne Pentland :

La combinaison de ce système nerveux en évolution avec des modèles de physique sociale mènera bientôt à la capacité d'orienter nos sociétés et l'ensemble de la culture⁷. [notre traduction]

4. A. Rouvroy et T. Berns, *Gouvernamentalité algorithmique et perspectives d'émancipation. Le disparates comme condition d'individuation par la relation?*, Réseaux, 2013, vol. 177, no 1 p. 173.

5. S. Zuboff, *op. cit.*, p. 376-377.

6. A. Pentland, *Social physics : How good ideas spread the lessons from a new science*, New York, Penguin books, 2013.

7. A. Pentland, *Honest signals. How they shape our worlds*, Cambridge, MA, MIT Press, 2008, p. 98.

L'objectification du réel

Or, ces modèles fondés sur la collecte massive de données opèrent sur un registre procédural et non substantiel (symbolique). Il ne capte pas un contenu, un référent symbolique, mais plutôt une récurrence ou un lien de corrélation. Comme le proclamait déjà en 2008 Chris Anderson en plaçant la fin de la théorie : « Qui sait pourquoi les gens font ce qu'ils font. Le fait est qu'ils le font et qu'on peut le suivre et le mesurer avec une fidélité sans précédent. Avec suffisamment de données, les chiffres parlent d'eux-mêmes ».

Ainsi, cette objectification du réel à laquelle participent la surveillance généralisée et son modèle économique concomitant identifié par Zuboff transparaît aujourd'hui un peu partout dans la société. Que ce soit par les transactions à haute fréquence⁸ au cœur des échanges financiers, de la quantification de soi par le biais de tout un ensemble d'outils numériques personnels munis de capteurs, des recommandations algorithmiques des plateformes ou de la e-santé qui se met en place, les normes sociétales correspondant au capitalisme de surveillance ne s'adressent plus à des citoyen-ne-s. Dès lors, la critique libérale, bien que nécessaire, glisse malheureusement sur la question primordiale du modèle de société que suggère le tout numérique du capitalisme de surveillance.

Or, ces modèles fondés sur la collecte massive de données opèrent sur un registre procédural et non substantiel (symbolique). Il ne capte pas un contenu, un référent symbolique, mais plutôt une récurrence ou un lien de corrélation.

La praxis comme condition de liberté fondamentale?

La société sans friction que souhaite articuler la surveillance généralisée revient à proposer une société sans politique. Ce dernier se définit pourtant précisément par la mise en relief de la friction sociale comme socle d'une discussion collective autour des horizons normatifs visés. Le danger ici est qu'un social réticulé ayant délesté la société elle-même en tant que totalité ne peut faire la critique de l'horizon de cette dernière. Comment le pourrait-on si cet horizon n'est pas institué en amont, mais se dévoile toujours seulement dans un éternel présent exclusivement médié par la technologie et orienté au gré des logiques de marchés? Cette dissolution de la société dans une masse de données numériques nous apparaît donc inquiétante.

En effet, à la lueur des grandes tendances polarisatrices actuelles et des difficultés majeures à faire rupture avec des modèles de sociétés nocifs (notamment en termes d'inégalités sociales, de genre et de classe autant que d'écologie), réaffirmer des horizons de sociétés alternatifs fondés sur des droits et des responsabilités revus et corrigés pour le numérique semble plus que jamais une urgence. La question de la liberté peut ainsi être interprétée comme celle d'une capacité nécessaire pour une démocratie digne de ce nom de toujours être en mesure de reconsidérer la forme instituée de la société. À la lueur de la dissolution de cette dernière que nous avons retracée en tant qu'enjeu du capitalisme de surveillance, cette opération apparaît tendanciellement fuyante et toute à redéfinir pour un 21^e siècle numérique.

8. Ce sont des transactions financières réalisées à des échelles de millisecondes par le biais d'algorithmes.



Le capitalisme de surveillance *like* la fracture numérique

Centre de documentation en éducation des adultes et condition féminine (CDÉACF)

Lise Chovino, responsable de la formation et de l'accompagnement en technologies de l'information et des communications (TIC) et Catherine St-Arnaud Babin, bibliothécaire de liaison

Il est de plus en plus complexe de se défendre contre les pratiques invasives du capitalisme de surveillance fondées sur la collecte des données, surtout quand on prend en compte les inégalités systémiques et structurelles qui creusent la fracture numérique.

Inégalité des chances face au numérique

La fracture numérique différencie les personnes qui ont accès aux TIC de celles qui ne peuvent ou ne savent pas les utiliser. Cette fracture est notamment matérielle, financière et géographique. Elle repose aussi sur les connaissances et la confiance nécessaires pour être autonome dans le monde numérique.

Pour être un-e internaute, certes, il peut suffire d'avoir accès à un appareil connecté à Internet. Cependant, pour être un-e internaute aguerri-e et autonome, il vaut mieux savoir bien lire, posséder son propre appareil, avoir une connexion haute vitesse et, surtout, avoir confiance en ses capacités de résolution de problèmes numériques. Or, ce sont des conditions qui sont rencontrées chez moins de gens qu'on ne le croie.

Au Québec, l'enjeu de la littératie et de l'alphabétisation demeure crucial pour de nombreuses personnes. Des enquêtes sont régulièrement menées à ce sujet, tel que le Programme pour l'évaluation internationale des compétences des adultes (PEICA) ou des études de la Fondation pour l'alphabétisation. Or, un faible niveau de littératie entraîne souvent un faible niveau de littératie numérique. Pour naviguer en ligne, il faut pouvoir lire et trier l'information présentée dans le corps du texte, les encadrés, les menus, les images et les icônes. Pouvoir donner un sens aux consignes et des avertissements, c'est loin d'être acquis pour tout le monde.

Et puis, encore faut-il avoir les moyens de se payer un appareil connecté et une bonne connexion Internet. La localisation géographique a d'ailleurs un énorme impact sur la qualité et le coût du service, comme le démontre la dernière enquête *NETendances* par région¹. Plus on est loin, moins le service est bon et plus il est cher.



Crédit : ev sur Unsplash

Il faut également noter que les études mentionnées plus haut n'incluent même pas une analyse intersectionnelle qui nous permettrait de comprendre comment certaines parties de la population peuvent être davantage vulnérables aux conséquences de la fracture numérique, même dans les grands centres urbains. Le CDÉACF a exposé une de ces réalités dans la capsule vidéo *Les inégalités numériques sont une violence faite aux femmes* produite pour la *Campagne 2021 des 12 jours contre les violences faites aux femmes*².

De plus, la cyberadministration creuse à elle seule un grand fossé au sein de la population. Le grand virage numérique du gouvernement entraîne une dépendance structurelle aux TIC afin d'avoir accès aux services, causant un stress lié à l'obligation d'utiliser ces outils. Alors que les projets de formation à la littératie numérique sont ponctuels ou sous-financés, beaucoup d'internautes ont appris sur le tas, prises entre incertitude et crainte de commettre une bêtise irréparable. Cette insécurité est un grand cadeau pour le capitalisme de surveillance : plus les internautes sont hésitant-e-s ou inexpérimenté-e-e, moins ils ou elles se prémunissent contre les tactiques de collectes de données. C'est un gain sans effort pour Google, Apple, Facebook, Amazon et Microsoft (GAFAM).

1. En ligne : <https://api.transformation-numerique.ulaval.ca/storage/473/netendances-2020-00-portrait-ensemble-du-quebec.pdf>

2. En ligne : <https://www.facebook.com/watch/?v=921932688420882>

Or, un faible niveau de littératie entraîne souvent un faible niveau de littératie numérique. Pour naviguer en ligne, il faut pouvoir lire et trier l'information présentée dans le corps du texte, les encadrés, les menus, les images et les icônes.

Dire non, mais à quoi?

Comment savoir qu'on a le choix d'une option ou d'une autre? Comment savoir *si* on a le choix? Comment protéger ses données personnelles en toute sérénité et accorder un consentement éclairé en matière de partage de ses informations personnelles?

Il est difficile de comprendre avec précision toutes les subtilités de la déconnexion et des options de confidentialité. Les politiques de confidentialité sont longues et souvent rédigées dans un jargon juridique peu intelligible. Sans compter les options de consentement offrant de faux choix tels que : « voulez-vous enregistrer votre mot de passe? *oui* ou *plus tard* », l'ajout de mises à jour régulières qui changent les paramètres de confidentialité (exemple : Facebook qui remet par défaut les publications en mode public), ou les options de partage de données activées automatiquement. Ces pratiques faussées imposent aux utilisatrices et aux utilisateurs une vigilance quasi continue et peut les mener à céder face à l'insistance. Untel *accepte* de rester connecté, car peu familier avec les TIC, il a peur de mal faire. Une telle finit par cliquer sur *oui* pour sauvegarder son mot de passe parce que fatiguée de voir continuellement la fenêtre *plus tard* s'afficher. C'est le genre de choix qu'on nous offre.

Il faut également considérer la dangerosité de ces pratiques pour des publics déjà vulnérabilisés. L'exemple des femmes vivant de la violence conjugale est éloquent. Dans ce contexte, les pratiques du capitalisme de surveillance ont non seulement un impact sur la confidentialité des informations personnelles de ces femmes, mais aussi des conséquences directes sur leur sécurité. Pensons, entre autres, aux algorithmes de recommandation de contacts sur les réseaux sociaux, au partage non sollicité de l'adresse des maisons d'hébergement sur les cartes en ligne et aux publicités ciblées envoyées à l'entourage selon les activités en ligne. Les conséquences de ces bris de confidentialité peuvent être sans retour.

[...] les pratiques du capitalisme de surveillance ont non seulement un impact sur la confidentialité des informations personnelles de ces femmes [victimes de violence conjugale], mais aussi des conséquences directes sur leur sécurité.

Fardeau individuel ou action collective

Bien que la population générale ait besoin de sensibilisation, de formation et de soutien au sujet des TIC, il est capital de créer un cadre politique et commercial permettant de s'épanouir avec ces technologies et de les choisir sciemment. Malgré leur bonne volonté, les personnes qui parviennent à se former se confrontent au rythme d'évolution des TIC et des pratiques de confidentialité et de sécurité. Le fardeau individuel est pratiquement insoutenable, car il faut sans cesse réviser ses connaissances des paramètres de chaque outil. Sans parler des barrières structurelles et systémiques ayant un impact direct sur la possibilité d'acquérir les outils et les savoirs technologiques nécessaires à son autonomie.

D'ailleurs, une perspective plus globale sur les aspects éthiques entourant les pratiques du capitalisme numérique permet de constater que les décisions prises par les GAFAM et par les pouvoirs publics ont aussi un impact sur la marge de manœuvre des individus. Malgré les failles actuelles et toujours non résolues présentées plus haut, il semble se dessiner une volonté institutionnelle et économique d'entreprendre au plus vite un nouveau virage numérique qui systématise le recours à la collecte massive de données et à l'intelligence artificielle. Pour obtenir ces données, nous voyons les bailleurs de fonds orienter le financement des projets et embrasser cette voie sous couvert de célébrer les données ouvertes. Cependant, encore une fois, qui saura faire la part des choses entre le partage d'informations et la protection de la confidentialité des données personnelles? Dans ce contexte, reporter entièrement le fardeau de la protection de ces données sur les utilisatrices et les utilisateurs a peu de chances d'aboutir à une véritable souveraineté sur nos données, en plus de renforcer l'isolement et les risques encourus par les populations déjà vulnérabilisées. Sans changement structurel et systémique, les initiatives individuelles sont donc mises en échec au gré des mises à jour. Cela revient, en somme, à jouer exactement le jeu du capitalisme de surveillance.

Cependant, encore une fois, qui saura faire la part des choses entre le partage d'informations et la protection de la confidentialité des données personnelles?

Capitalisme de surveillance et monopolisation

Quelles réponses, quelles ripostes?

Pierre Henrichon, auteur de *Big Data. Faut-il avoir peur de son nombre?*

Le 20 octobre 2020, le procureur général des États-Unis et les procureurs généraux de 11 états (Arkansas, Floride, Georgie, Indiana, Kentucky, Louisiane, Mississippi, Missouri, Montana, Caroline du Sud, Texas) saisissaient la Cour fédérale du District de Columbia d'accusations portées contre Google alléguant des pratiques monopolistiques illégales de la part de la société-phare géante de la Silicon Valley¹.

Le 9 décembre 2020, la *Federal Trade Commission* (FTC) du gouvernement des États-Unis déposait une plainte à l'endroit de Facebook, alléguant des pratiques contraires aux lois antitrust.

Entre 2011 et 2013, la FTC avait mené enquête sur le rôle de Google au sein des marchés de la recherche Internet et de la publicité en ligne. Alors que le personnel juridique de la Commission recommandait le dépôt de poursuites, l'administration en décida autrement. En fait, il faut remonter à mai 1998 pour retracer le plus récent procès contre un géant du Big Tech s'appuyant sur les dispositifs juridiques antitrust des États-Unis, et dont le jugement fit l'objet d'un appel réussi².

Et je me limite aux enquêtes et mises en accusation diligentées aux États-Unis. Elles sont légion en France, en Grande-Bretagne, en Inde et ailleurs.

Alors que les poursuites intentées en vertu des lois antitrust sont les bienvenues, elles ne seront pas suffisantes pour mettre un terme à ce qu'il est convenu d'appeler le *capitalisme de surveillance* d'autant plus que les tribunaux américains, depuis plus de 40 ans maintenant, sont devenus bienveillants à l'égard des monopoles^{3,4}.

Un modèle d'affaires vorace en données

On le sait clairement maintenant : le modèle d'affaires des géants du numérique repose sur la collecte massive, et souvent incontrôlée, des données en vue de modeler nos comportements et même nos émotions. Comme le souligne Shoshana Zuboff, « Les marchés qui font le commerce de l'avenir humain devraient être illégaux (ils entraînent des conséquences néfastes, dangereuses et antidémocratiques, et des préjudices intolérables dans une société démocratique) tout comme le commerce d'organes humains et d'êtres humains sont illégaux⁵ ». Bien que des réglementations aient été adoptées au fil des ans⁶, elles n'atteignent pas le cœur du modèle d'affaires des Facebook de ce monde.

La socialisation des données

Dans mon essai⁷, j'ai proposé un régime de socialisation des données par lequel les données captées par des acteurs comme les Google, Apple, Facebook, Amazon et Microsoft (GAFAM) seraient mises en commun et proposées à des utilisateurs, sous condition de finalités socialement acceptées, qui pourraient alors les agréger et les traiter. Cela présentait l'avantage d'ouvrir l'accès à toutes ces données à des fins de recherche en santé publique, en intelligence artificielle, etc. Et cela n'interdisait pas non plus aux GAFAM de mener à bien leurs travaux... sous surveillance d'une agence de réglementation d'utilisation des données.

Bien que des réglementations aient été adoptées au fil des ans, elles n'atteignent pas le cœur du modèle d'affaires des Facebook de ce monde.

1. Les tribunaux ont renvoyé les procureurs faire leurs devoirs. Cela montre bien les limites de l'approche légaliste qui s'appuie sur les lois antitrust.

2. *United States v. Microsoft Corporation*, 253 F.3d 34 (D.C. Cir. 2001)

3. Voir : Lina M. Kahn, *Amazon's Antitrust Paradox*, The Yale Law Journal, no 126, p. 720 (2017)

4. *Judge Throws Out 2 Antitrust Cases Against Facebook*, New York Times, 28 juin 2021. Notons que la FTC et les procureurs du fédéral ont décidé de revenir à la charge.

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

6. Parmi ces réglementations, le *Règlement général sur la protection des données* de l'Union européenne.

7. P. Henrichon, *Big Data. Faut-il avoir peur de son nombre?*, Écosociété, 2020.

D'autres modèles de socialisation – volontaire cette fois – ont depuis fait l'objet de travaux et de propositions. Au Canada, la notion de *fiducie de données* a été avancée⁸. On en donnait la définition suivante : *Une fiducie de données est un organisme formé pour gérer des données pour le compte de ses membres. Ces derniers mettent en commun leurs données et conviennent expressément des conditions afférentes à leur partage.*⁹ Les finalités de telles fiducies visaient surtout l'innovation et la commercialisation des résultats.

L'intérêt général avant tout

Un autre modèle, peut-être plus prometteur, est celui du *Data altruisme*¹⁰ par lequel toutes les parties prenantes – contributeurs de données et utilisateurs – sont liées par des ententes encadrées en vue de partager des données à des fins identifiées comme étant en concordance avec l'intérêt général. Cette approche a déjà reçu l'aval des autorités européennes et sera probablement mise à l'épreuve au cours des prochaines années.

Mais de tels régimes, aussi innovateurs et généreux soient-ils, ne mettent pas en péril la captation tous azimuts des données pratiquée par les principaux acteurs monopolistiques de l'économie numérique. Aussi, nos efforts visant le démantèlement de ces monopoles, la socialisation générale des données et la réglementation plus serrée de la commercialisation des données ne doivent-ils pas s'affaiblir.

Pourquoi combattre les monopoles dans l'économie du Big Data¹²

- Produits de qualité moindre se traduisant par moins de protection des données personnelles, ce qui est l'équivalent d'une hausse de prix.
- Concentration de la collecte, du stockage et du traitement des données, dont des données personnelles.
- Profilage psychographique plus étendu, plus précis et plus révélateur.
- Dataveillance plus étendue et approfondie augmentant ainsi les risques de surveillance par l'État et de sécurité.
- Ciblage publicitaire, idéologique et politique plus précis, plus convaincant et plus susceptible de piloter les comportements.
- Importants transferts de richesses vers les monopoles provenant de tierces parties : fournisseurs, développeurs d'applications, annonceurs, consommateurs.
- Imposition de barrières à l'entrée à des applications et plateformes pouvant concurrencer celles de l'entreprise occupant une position dominante.
- Risques de manipulation de l'opinion publique à la faveur d'un profilage psychographique plus étendu¹³. Corruption des processus démocratiques.
- Risques de perte d'autonomie individuelle par un pilotage toujours plus intrusif des comportements.
- Risques de propagation de préjugés et de censure.
- Risques accrus de vols massifs de données.
- Contrôle de services considérés essentiels dans nos sociétés (communications sur médias sociaux, messageries, recherche sur le Web)¹⁴.
- Risques accrus d'opacité en matière de collecte, de traitement et d'utilisation des données.

8. Voir : Innovation, Sciences et Développement économique Canada, *Rapport des Tables de stratégies économiques du Canada : Industries numériques*. En ligne : <https://www.ic.gc.ca/eic/site/098.nsf/fra/00024.html> et aussi Conseil canadien des normes, *Feuille de route du Collectif canadien de normalisation en matière de gouvernance des données*.

En ligne : https://www.scc.ca/fr/system/files/publications/SCC_Data_Gov_Roadmap_FR.pdf

9. *Rapport des Tables de stratégies économiques du Canada*, op cit., p. 13 (version PDF).

10. Human Technology Foundation, *Le Data altruisme : une initiative européenne. Les données au service de l'intérêt général*.

En ligne : <https://www.mccarthy.ca/fr/a-propos/nouvelles-et-annoncements/human-technology-foundation-rapport-data-altruisme>

12. Maurice, E. Stucke, *Here Are All the Reasons It's a Bad Idea to Let a Few Tech Companies Monopolize Our Data*, Harvard Business Review, 27 mars 2018.

13. « On ne mène pas une campagne électorale sur la base de faits, mais bien sur les émotions... Il faut exploiter les peurs, même inconscientes des gens. » Affirmations faites par un dirigeant de la firme Cambridge Analytica, qui utilise le profilage psychographique, lors d'une conversation filmée clandestinement par des journalistes de Channel 4 en Grande-Bretagne et diffusée le 19 mars 2018 sur la chaîne. On peut visionner le tout ici : <https://www.channel4.com/news/cambridge-analytica-revealed-trumps-election-consultants-filmed-saying-they-use-bribes-and-sex-workers-to-entrap-politicians-investigation>

14. Kashmir Hill, *I Tried to Live Without the Tech Giants. It Was Impossible*, New York Times, 31 juillet 2020.

Nouvelles perspectives

Renforcement de la vie privée et éthique du design numérique

Michelle Albert-Rochette, candidate à la maîtrise en droit, Université Laval

Marie-Pier Jolicoeur, candidate au doctorat en droit du design numérique, Université Laval

Shoshana Zuboff dénonce, dans son ouvrage *The Age of Surveillance Capitalism*, un modèle économique basé sur l'extraction de nos données personnelles¹. Dans cette nouvelle forme de capitalisme, la professeure Zuboff expose que l'on cherche, de toutes les manières possibles et pour des motifs économiques, à ce que les personnes passent le plus de temps possible en ligne afin de générer toujours plus de données². La collecte et le traitement d'une quantité massive de données permettent ultimement aux grandes entreprises de mieux prédire et contrôler le comportement des personnes³. Les outils technologiques et les médias sociaux que nous utilisons quotidiennement sont ainsi mis au service de l'*addiction by design*⁴, soit l'objectif de créer une propension à utiliser continuellement ces technologies. L'objet de ce court article n'est pas de proposer des pistes de solution révolutionnaires au modèle décrit par la professeure Zuboff, mais plutôt d'ouvrir les lectrices et lecteurs à de nouvelles perspectives. Nous décrirons donc certaines initiatives qui visent à créer un environnement numérique davantage respectueux de la vie privée et des vulnérabilités humaines. Nous présentons d'abord, dans une perspective critique, quelques propositions juridiques. Ensuite, nous proposons un court examen du thème de l'éthique du numérique.

Aperçu du projet de loi 64

Le projet de loi 64⁵ (PL 64), adopté le 21 septembre 2021, a modifié la loi québécoise de protection des renseignements personnels⁶ (RP) dans le secteur privé. Un de ses objectifs est d'accroître le contrôle qu'ont les personnes sur leurs

données. Les modifications introduites par PL 64 s'intéressent notamment aux pratiques de profilage en imposant de nouvelles obligations aux entreprises, qui devront désormais avertir les personnes et les informer des moyens dont elles disposent pour *activer* les fonctions de profilage⁷, comme la publicité ciblée. Le PL 64 a aussi introduit des exigences à l'obtention du consentement pour la collecte, l'utilisation ou la communication de RP⁸. Le but est de mieux informer les personnes pour les protéger en leur permettant de faire des choix éclairés. Ces modifications paraissent positives, mais on peut douter de leur utilité : même si le consentement est renforcé par l'introduction de nouvelles normes, ce mécanisme demeure ancré dans une vision individualiste de la vie privée peu adaptée au fonctionnement du capitalisme de surveillance.

En effet, à l'ère du numérique, il est peu praticable de refuser son consentement. On peut par exemple penser à la nécessité d'accepter les politiques de confidentialité de Facebook pour accéder à différents services et pour entretenir des liens sociaux⁹. Le mécanisme de consentement individuel occulte par ailleurs les effets systémiques liés au traitement des données. Au moment de consentir, on peut difficilement imaginer ce que ses données peuvent révéler sur soi lorsqu'elles sont croisées avec des milliards d'autres¹⁰. On ne peut non plus appréhender le pouvoir que confère aux entreprises le cumul de données d'apparence anodine¹¹. Et même si un consentement était réellement libre et éclairé, ce choix individuel a des effets collectifs puisqu'il permet d'inférer des informations sur les autres : « *[b]y consenting [...] a user becomes a conduit for gathering information about her entire social network, whether or not they have consented*¹² ».

1. S. Zuboff, *The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power*, PublicAffairs, New York, 2019.

2. *Id.*

3. N. Richards et W. Hartzog, *A Duty of Loyalty for Privacy Law*, 2021, 99 Wash. U. L. Rev. 961, p. 18.

4. N.D. Schüll, *Addiction by design*, Princeton University Press, 2012.

5. *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (Loi modernisant la loi sur le privé)*.

6. *Loi sur la protection des renseignements personnels dans le secteur privé*.

7. *Loi modernisant la loi sur le privé*, art. 8.1.

8. *Id.*, art. 14.

9. Jack M. Balkin, *The Fiduciary Model of Privac*, 2020, 134:1 HLRF 11, p. 13.

10. J. A.T. Fairfield et C. Engel, *Privacy as a Public Goo*, 2015, 65:3 Duke L.J. 385, p. 390.

11. S. Delacroix et N. D. Lawrence, *Bottom-up data Trusts: disturbing the 'one size fits all' approach to data governance*, 2019, 9:4 Int. Data Priv. Law 236, p. 237.

12. J. A.T. Fairfield et C. Engel, *supra* note 10, p. 410.

Le mécanisme de consentement individuel occulte par ailleurs les effets systémiques liés au traitement des données.

Vers des solutions collectives

Face à ces limites, des autrices et auteurs ont envisagé des solutions qui s'écartent de la perspective dominante de contrôle individuel des données, parmi lesquelles figurent les fiducies de données¹³ – qui consistent en une mise en commun de données gérées par un tiers indépendant agissant pour le compte des personnes – et le devoir de loyauté (*duty of loyalty*¹⁴). Cette deuxième solution cherche à garantir que les entreprises qui collectent et traitent les données agissent conformément à la confiance que les personnes leur accordent. Un réseau social assujéti à une telle obligation devrait donc agir selon les attentes raisonnables des personnes relativement à l'utilisation de leurs données et à leur expérience en ligne¹⁵. Ainsi, l'utilisation des données à des fins de publicité contextuelle serait loyale, mais pas celle réalisée à des fins de publicité comportementale. Par exemple, une personne consultant un site de voyage sur un pays donné pourrait s'attendre à recevoir de la publicité en lien avec ce pays, mais il serait déloyal pour une entreprise de diffuser une publicité basée sur le traitement de nombreux types de données issues de sources variées¹⁶. En matière

d'expérience en ligne, le devoir de loyauté pourrait aussi inclure une exigence d'influence loyale¹⁷, où les entreprises ne pourraient pas concevoir un *design* visant à manipuler le comportement des personnes à l'encontre de leurs intérêts. L'imposition d'un tel devoir de loyauté aurait pour avantage de protéger les personnes indépendamment de leur niveau de compréhension des politiques de confidentialité¹⁸.

Pour une éthique du numérique

Dans un article de 2018 s'intéressant au capitalisme de surveillance et visant à mettre en lumière le processus par lequel l'IA parvient à collecter nos données personnelles, le professeur Pierre-Luc Déziel émettait certaines réserves sur la capacité de la législation canadienne à protéger à elle seule notre vie privée :

Au cours des dernières années, de nouveaux droits visant la protection de la vie privée informationnelle des personnes firent leur apparition : droit à l'explication, droit à la portabilité des données et le fameux droit à l'oubli. Ces droits [...] pourraient aider les personnes à mieux protéger leur vie privée dans les environnements numériques. Toutefois, je crois que, pour répondre aux défis soulevés [...], le droit à la vie privée ne peut agir seul, et que d'autres pans du droit peuvent et doivent être mobilisés¹⁹.

13. Ex : S. Delacroix et N. D. Lawrence, *supra* note 11.

14. N. Richards et W. Hartzog, *A Duty of Loyalty for Privacy Law*, *supra* note 3.

15. N. Richards et W. Hartzog, *The Surprising Virtues of Data Loyalty*, 71 ELJ (à paraître 2022), p. 8.

16. Jack M. Balkin, *supra* note 10, p. 28.

17. N. Richards et W. Hartzog, *supra* note 3, p. 44.

18. N. Richards et W. Hartzog, *supra* note 15, p. 27.

19. P.-L. Déziel, *Les limites du droit à la vie privée à l'ère de l'intelligence artificielle : groupes algorithmiques, contrôle individuel et cycle de traitement de l'information*, 2018, 30:3 C.P.I. 827.



Pour compléter ce court article, il nous apparaît intéressant de nous ouvrir aux enjeux entourant l'éthique du numérique. Pour les programmeuses et programmeurs informatiques, réfléchir à ce qu'est un *bon code informatique* est fondamental²⁰, mais cette question ne se limite plus seulement à la création d'outils efficaces et performants. De nouveaux concepts comme celui de *Privacy by design*, *Safety by design* et *Éthique by design*, qui répondent à des questions morales et de *devoir-être* de l'objet technique²¹, ont vu le jour. La *PhD* Flora Fisher explique que la prolifération des termes *by design* dans les dernières décennies révèle l'existence de nouveaux concepts polysémiques obligeant à entamer une réflexion sur l'éthique virtuelle et sa puissance normative²². Très sommairement, l'idée serait, dans le cas de la vie privée, de tenir compte dès la phase de conception des systèmes informatiques, des exigences en matière de protection des données personnelles en les intégrant directement dans le produit, au lieu de les ajouter ultérieurement²³. On chercherait donc à limiter, *a priori*, la divulgation de données collectées²⁴. Pour Lawrence Lessig, professeur de droit à Harvard, le code informatique a une force équivalente à celle de la loi puisque le *design* du numérique impose de produire certains comportements. Ce code constitue également un levier important pour protéger

les droits de ces utilisatrices et utilisateurs²⁵. En somme, s'il l'on veut réellement avoir un impact pour améliorer les choses à long terme, c'est à l'architecture même du code informatique, au *design* du numérique, qu'il faudra s'intéresser, pour éviter que les solutions avancées soient de simples coups d'épée dans l'eau.

Très sommairement, l'idée serait, dans le cas de la vie privée, de tenir compte dès la phase de conception des systèmes informatiques, des exigences en matière de protection des données personnelles en les intégrant directement dans le produit, au lieu de les ajouter ultérieurement.

20. F. Fischer (2020). *Les normativités des technologies numériques : approche d'une éthique « by design »* (Doctoral dissertation, Compiègne), p. 189.

21. *Id.* p. 22.

22. *Id.*, résumé et p. 20.

23. *Id.*, p. 215

24. *Id.*

25. L. Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 1999, 113:2 Harv. L. Rev. 501.



Katasoho, partenaire de la Ligue des droits et libertés depuis 2007

Impressions, finition & façonnage au cœur du Plateau! Service complet de reliure et de finition : pliage, assemblage, brochage, brochage à cheval, numérotation, perforation, mise en tablette et reliure spirale et allemande sur place!

info@katasoho.com • www.katasoho.com • 514.961.5238

Depuis 15 ans, l'équipe de KataSOHO fait la conception graphique des publications de la Ligue des droits et libertés en plus d'en faire l'impression. Pour cet engagement indéfectible aux publications de la LDL et aux droits humains, mille mercis!

Mobilisations et médias sociaux : quelles opportunités et quels enjeux?

Anne-Sophie Letellier, candidate au doctorat en communications, UQÀM

Normand Landry, professeur, Université TÉLUQ, titulaire de la Chaire de recherche du Canada en éducation aux médias et droits humains

Les technologies numériques ont joué des rôles significatifs dans les mobilisations citoyennes des dernières décennies. À cet égard, elles sont couramment présentées comme des vecteurs de démocratisation des sociétés. Des répertoires numériques d'actions collectives se sont progressivement déployés au sein d'une société civile s'étant largement internationalisée. Ces technologies constituent désormais des architectures de militance qui favorisent l'organisation de la dissidence et de la militance politique, le partage d'information, la création collective de contenus et le contournement de la censure et des voies de communication officielles.

La dernière décennie a fait état d'une pluralité de situations où les technologies numériques ont joué un rôle majeur dans des mouvements démocratiques et contestataires. Les révolutions arabes, le mouvement anti-austérité *Occupy*, ainsi que les nombreuses mobilisations en ligne dans le cadre de luttes environnementales et autochtones (#IdleNoMore), féministes (#MeToo, #MoiAussi) et antiracistes (#BlackLivesMatter) en sont des exemples frappants.

Ainsi, à mesure que se démocratisent et se distribuent les technologies numériques au sein des sociétés, des usages et des pratiques politiques numériques se développent et se propagent. Costanza-Chock¹ qualifie d'*affordance* les caractéristiques de design qui invitent les utilisateur-trice-s à poser certaines actions (partager, commenter, interagir avec du contenu, former des groupes, créer des événements, entretenir des communications privées, etc.) sur une interface donnée. Ces *affordances* masquent néanmoins des mécanismes de collecte de données excessivement efficaces, subtils, et à la base d'un modèle économique hautement profitable où s'entrecroisent des intérêts commerciaux et étatiques.

Les *affordances* d'une mobilisation... et de la désinformation

Des discours critiques à l'endroit des technologies numériques présentent les plateformes, les sites et les services numériques mis à la disposition du grand public comme des

lieux où s'exerce une surveillance grandement facilitée et amplifiée par un modèle économique de monétisation des données personnelles, qualifié par Shoshana Zuboff (2019) de capitalisme de surveillance. Si les conséquences les plus évidentes du capitalisme de surveillance ont longtemps été réduites à une publicité trop ciblée, les risques associés à la collecte systématique et ubiquitaire des données personnelles sont désormais collectifs et touchent à l'organisation des sociétés démocratiques.

Notamment, en 2018, le scandale de Cambridge Analytica a mis en lumière comment les mécanismes du microciblage publicitaire pouvaient également être mobilisés dans un contexte électoral afin d'exposer des électeur-trice-s indécis-e-s ciblé-e-s à des campagnes de désinformation². Plus récemment, en 2021, Frances Haugen³ a dévoilé des documents révélant que les algorithmes de classification de contenus utilisés par la plateforme de réseau social avaient contribué significativement à exacerber des troubles alimentaires chez des adolescentes, ainsi qu'à amplifier la portée de discours haineux facilitant, entre autres, le génocide des Rohingyas au Myanmar⁴. Dans ces deux cas, les documents fuités démontrent que la rentabilité financière de compagnies transnationales – largement attribuable au modèle d'affaires inhérent au capitalisme de surveillance – est, comme l'a souligné Haugen, ordinairement explicitement priorisée face aux enjeux éthiques, sociaux et politiques qui découlent de leurs pratiques.

[...] les algorithmes de classification de contenus utilisés par la plateforme de réseau social avaient contribué significativement à [...] amplifier la portée de discours haineux facilitant, entre autres, le génocide des Rohingyas au Myanmar.

1. S. Costanza-Chock, *Design justice: Community-led practices to build the worlds we need*, The MIT Press, 2020.

2. C. J. Bennett, D. Lyon, *Data-driven elections: implications and challenges for democratic societies*, Internet Policy Review, 2019, 8(4).

3. Haugen est une ancienne employée chez Facebook. Elle était chargée de diriger un groupe de travail contre la désinformation dans le cadre des élections américaines de 2020.

4. En ligne : <https://www.courrierinternational.com/dessin/genocide-des-rohingyas-le-mea-culpa-de-facebook>

De la surveillance étatique à la montée des logiciels espions

En 2013, les révélations du lanceur d'alerte Edward Snowden ont exposé l'ampleur des pratiques de surveillance des États sur leurs citoyens. Elles ont également démontré comment, à travers un accès direct aux infrastructures physiques des réseaux – pensons au programme PRISM – ou encore à travers des ordres des tribunaux, les agences de renseignement et de sécurité américaines étaient en mesure de gagner l'accès aux données personnelles recueillies par les plus grandes entreprises du secteur du numérique.

Si ces pratiques ont été largement critiquées, elles s'inscrivent néanmoins dans une tendance forte des États à surveiller les communications de leurs citoyens. Dans les pays occidentaux, la légitimation de ces pratiques de surveillance s'articule généralement à travers la promotion d'un *accès légal* à des données et communications personnelles et par un argumentaire présentant le bien-fondé des initiatives gouvernementales cherchant à introduire des portes dérobées dans les systèmes de chiffrement utilisés par leurs citoyens⁵. Si ces positions sont défendues sous le couvert de la lutte au terrorisme et à la criminalité, de nombreux cas documentés ont mis en lumière un manque d'encadrement juridique et des pratiques injustifiables de surveillance de journalistes⁶ et de militant-e-s⁷.

Ces pratiques de surveillance étatique sont également alimentées par le marché en pleine expansion des logiciels espions. Ces logiciels sont officiellement développés avec cette même intention affichée publiquement de lutter contre la criminalité et le terrorisme. Lorsqu'installés sur des appareils, ces logiciels permettent de surveiller en temps réel l'ensemble des déplacements et des activités en ligne de leurs cibles. Les groupes de défense des droits humains s'évertuent depuis quelques années à documenter et à attirer l'attention sur les dérives associées à ces logiciels. Ces derniers sont couramment utilisés par des régimes autoritaires afin de surveiller des journalistes, des avocat-e-s et des militant-e-s. À terme, ces usages conduisent à des arrestations illégales et à des meurtres extrajudiciaires⁸.

Si ces positions sont défendues sous le couvert de la lutte au terrorisme et à la criminalité, de nombreux cas documentés ont mis en lumière un manque d'encadrement juridique et des pratiques injustifiables de surveillance de journalistes⁹ et de militant-e-s¹⁰.

En ce sens, l'utilisation ubiquitaire des technologies numériques, doublée des modèles d'affaires basés sur la collecte de données, crée un terrain fertile pour les pratiques de surveillance étatique. Plusieurs rapports, dont ceux du Rapporteur spécial des Nations Unies sur la liberté d'expression¹¹, abondent dans cette direction et associent directement ces pratiques de surveillance à des atteintes portées à plusieurs droits et libertés fondamentales, dont la liberté d'expression.

En somme, les *affordances* des technologies numériques offrent simultanément des opportunités inédites à l'organisation de mouvements sociaux démocratiques et une capacité de surveillance décuplée. Ces pratiques de surveillance font converger les intérêts des entreprises investissant le champ du numérique avec ceux des États qui régulent leurs activités ou qui constituent de potentiels *clients* pour leurs services de surveillance.

La prise en considération de ces enjeux ne vise pas la désertion des réseaux sociaux, ou une déconnexion aux technologies numériques. À un niveau tactique, elle invite plutôt à une éducation critique¹² face aux fonctionnalités de ces plateformes dans le but de déjouer – du moins partiellement – les mécanismes de collecte de données ainsi que les risques associés aux capacités de surveillance accrues des États et des compagnies privées. D'une perspective plus stratégique, cette situation appelle à d'urgentes réformes législatives et à une réglementation plus serrée des acteurs du numérique, visant notamment à accroître leur imputabilité sur la question de la désinformation et de la protection des données personnelles.

5. L. Gill, T. Israel et C. Parsons, *Shining a light on the encryption debate: A Canadian field guide*, 2018.

6. En ligne : <https://www.lapresse.ca/actualites/justice-et-affaires-criminelles/201610/30/01-5036027-patrick-lagace-vise-par-24-mandats-de-surveillance-policiere.php>

7. A. Choudry, *Activists and the surveillance state: Learning from repression*, Between the Lines, 2018.

8. B. Marczak, J. Scott-Railton, S. McKune, B. Abdul Razzak et R. Deibert, *HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to operations in 45 countries*, 2018.

9. *Op.cit.*, note 6.

10. A. Choudry, *Activists and the surveillance state: Learning from repression*, Between the Lines, 2018.

11. D. Kaye, *Report on the Adverse Effect of the Surveillance Industry on Freedom of Expression*, OHCHR, 2019. En ligne : <https://www.ohchr.org/en/calls-for-input/reports/2019/report-adverse-effect-surveillance-industry-freedom-expression>

12. N. Landry, A. M. Pilote et A. M. Brunelle, *L'éducation aux médias en tant que pratique militante : luttes et résistances au sein des espaces médiatiques et de gouvernance*, 2017.

Consultations publiques sur l'intelligence artificielle

Quelle place pour le droit de dire non à l'intelligence artificielle?

Entrevue avec **Fatima Gabriela Salazar Gomez**

par **Lynda Khelil**, responsable de la mobilisation à la Ligue des droits et libertés

Fatima Gabriela Salazar Gomez a été coordonnatrice à l'Agora Lab et chargée à la mobilisation pour une consultation internationale organisée en 2020 par l'Organisation des Nations Unies pour l'éducation, la science et la culture (UNESCO), *Dialogue International sur l'Éthique de l'IA* et une consultation pancanadienne organisée en 2021 par le gouvernement du Canada, *Dialogue ouvert : l'IA au Canada*. Elle est actuellement chargée de projet à Hoodstock, une organisation basée à Montréal-Nord qui œuvre pour la justice sociale et l'élimination des inégalités systémiques.

LDL : Peux-tu nous parler de la consultation publique sur l'IA du gouvernement du Canada en 2021? Quels étaient les objectifs et quels constats as-tu faits?

En mai 2019, le ministre fédéral de l'Innovation, des Sciences et de l'Industrie a créé un *Conseil consultatif en matière d'intelligence artificielle*¹. Ce dernier a ensuite mis sur pied en janvier 2020 un *Groupe de travail sur la sensibilisation du public*² dont le mandat est « de concevoir des stratégies régionales afin de sensibiliser le public à l'IA, de favoriser la confiance du public envers l'IA et de le renseigner sur la technologie, ses utilisations possibles et les risques qui y sont associés³ ».

Le groupe de travail a tenu en avril et mai 2021 une consultation publique pancanadienne, *Dialogue ouvert : l'IA au Canada*, sous la forme d'ateliers virtuels. J'ai participé à l'organisation de cette consultation dans le cadre de mon travail à Agora Lab, un des partenaires de la consultation. Mes collègues et moi, devons proposer des *cas d'usage*, c'est-à-dire des scénarios qui mettent de l'avant des utilisations de l'IA dans des situations précises tirées de la réalité, dans les domaines notamment de la santé, de l'éducation, de la justice ou de l'environnement. Lorsque nous avons soumis nos propositions, le gouvernement nous a clairement indiqué que nos cas d'usage démontraient trop les aspects négatifs de l'IA. Or, il nous semblait essentiel de discuter de ces aspects qui sont parfois plus difficiles à identifier pour la population et moins abordés. On nous a également rappelé que la

consultation portait sur ce qu'on appelle le *trustworthy*. Il ne fallait donc pas que le côté négatif de certains usages de l'IA ressorte trop.

J'ai constaté que la consultation ne visait pas tant à montrer ce qui se fait en matière d'IA et à discuter des dangers et atteintes potentielles aux droits, mais plutôt à faire de la sensibilisation du public. C'est d'ailleurs le mandat principal du Groupe de travail. Selon moi, il s'agissait pour le gouvernement de *tâter le terrain* pour évaluer jusqu'où certains droits humains pourraient être bafoués sans que ça suscite de fortes réactions. Les autorités utilisent souvent les consultations publiques pour savoir ce que la population pense pour ensuite ajuster leurs discours.

Dans ce cas-ci, le discours sous-jacent du gouvernement est, selon moi, qu'il y aura développement de l'IA, qu'on le veuille ou non. Je n'ai pas eu l'impression que le gouvernement valorise le droit de la population de dire non à l'implantation de l'IA dans certains domaines ou pour certaines utilisations. C'est même plutôt le contraire.

J'ai aussi pu faire le constat d'une forme de contrôle. Au départ, le gouvernement n'avait pas l'intention de rendre public le rapport de la consultation. Pour mes collègues et moi, ça ne faisait aucun sens qu'on fasse une consultation publique et que les données ne soient pas rendues publiques. On a donc demandé qu'il le soit. Ça m'est apparu être une forme d'utilisation de l'opinion et de la parole citoyenne à des fins politiques. Je pense que si, par exemple, toutes les personnes qui avaient participé avaient dit qu'elles étaient contre certains usages de l'IA, le gouvernement aurait été pris avec ça, d'où son intention initiale de ne pas publier le rapport. À ce jour, le rapport n'est pas encore public. J'espère qu'il le sera bientôt.

1. En ligne : <https://ised-isde.canada.ca/site/conseil-consultatif-intelligence-artificielle/fr>

2. En ligne : <https://ised-isde.canada.ca/site/conseil-consultatif-intelligence-artificielle/fr/groupe-travail-sensibilisation-public-mandat>

3. En ligne : <https://ised-isde.canada.ca/site/conseil-consultatif-intelligence-artificielle/fr/rapport-annuel-2019-2020>

Tu as utilisé l'expression *trustworthy*. Qu'est-ce que ça veut dire?

L'expression *trustworthy* AI qui est utilisée par les gouvernements signifie *une IA digne de confiance*. La consultation publique était orientée dans cette perspective. On veut nous inciter à avoir confiance dans des systèmes d'IA, bien qu'ils comportent des biais discriminatoires avérés et peuvent avoir dans certains documents des conséquences importantes sur l'exercice de nos droits et libertés. Ce ne sont pas uniquement les algorithmes qui sont biaisés, ce sont les données elles-mêmes qui le sont. Le déficit historique de données sur certaines personnes, populations et communautés induit des biais dans les algorithmes d'IA.

En tant que femme, racisée, issue de l'immigration, j'ai déjà de la difficulté à avoir confiance en nos propres institutions, donc comment penser que je pourrai avoir confiance d'emblée dans un système que je ne comprends pas, qui possède peu de données sur ma communauté et dont les algorithmes présentent des biais intrinsèques.

L'expression *une IA digne de confiance* opère donc selon moi une manipulation par le discours. On ne veut pas qu'il y ait trop de mots négatifs associés à l'IA. *Trustworthy*, c'est une expression positive. Mais ce que ça sous-tend, c'est que nous n'avons pas une IA digne de confiance actuellement ou que nous n'avons pas une IA qui suscite la confiance de la population. Mais le dire ainsi, c'est négatif d'un point de vue de relations publiques.

Dans ce cas-ci, le discours sous-jacent du gouvernement est, selon moi, qu'il y aura développement de l'IA, qu'on le veuille ou non. Je n'ai pas eu l'impression que le gouvernement valorise le droit de la population de dire non à l'implantation de l'IA dans certains domaines ou pour certaines utilisations. C'est même plutôt le contraire.

En quoi l'approche de sensibilisation du public sur l'IA est problématique selon toi? Et est-ce que la population a la possibilité de remettre en question certains usages de l'IA?

Quand on fait de la sensibilisation, ça sous-entend selon moi qu'on n'est pas là pour faire de l'éducation. Or, faire de l'éducation sur l'IA, c'est expliquer, présenter des choix et développer un esprit critique par rapport aux systèmes d'IA. Je pense qu'il faut faire de l'éducation à l'IA pour que la population comprenne mieux ce que c'est et puisse identifier les enjeux de droits qui sont en présents. Une population plus informée sera en mesure de participer au débat public sur l'IA et de se prononcer et se mobiliser sur les développements de l'IA dans certains domaines qu'elle ne voudrait pas par exemple. Mon rêve, c'est qu'on puisse faire des ateliers d'éducation aux enjeux liés à l'IA dans des espaces communs, par exemple les bibliothèques, pour que les gens soient outillés lorsqu'ils, elles sont invité-e-s à participer à des consultations publiques.

Actuellement, on est dans un paradigme où la discussion publique est orientée autour de la question « Comment atténuer les conséquences et les biais de l'IA? » avec la prémisse qu'il est bénéfique de développer et d'implanter largement des systèmes d'IA. Alors même qu'il n'y a pas d'encadrement robuste et que les lois ne sont pas adaptées au développement rapide de l'IA. Les autorités ont déjà pris la décision de développer des systèmes d'IA dans de nombreux domaines. La population n'est pas consultée et n'a pas de prise pour s'opposer à l'implantation de systèmes d'IA dans certains domaines et être entendue. Or, quand on sait que certaines utilisations de l'IA vont avoir des conséquences concrètes sur la vie des gens, par exemple dans le domaine de la justice, de l'immigration ou de l'emploi, on devrait pouvoir se poser la question « Veut-on véritablement de systèmes d'IA pour soutenir ou automatiser des prises de décisions dans ces domaines? ». C'est une question légitime et fondamentale à mon avis, d'autant plus dans un contexte pandémique où on a réalisé que nous sommes des êtres fondamentalement sociaux et que nos rapports aux autres, notre trajectoire de vie et comment on vit, ça a des impacts sur nos prises de décisions.

Pour une lucidité collective vis-à-vis des GAFAM

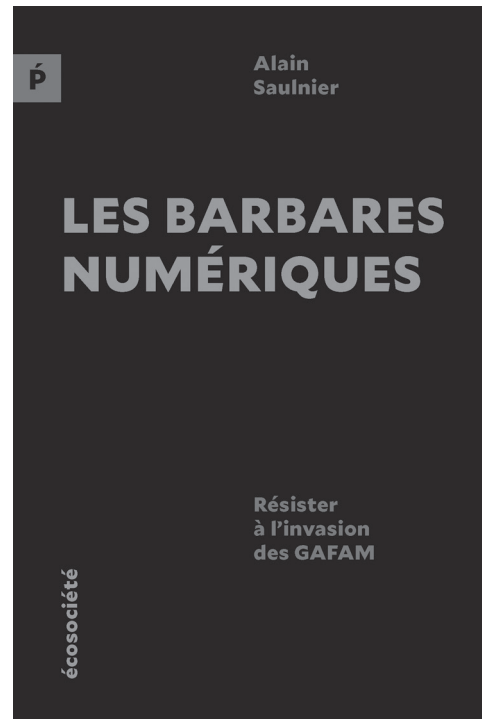
Delphine Gauthier-Boiteau, avocate criminaliste et candidate à la maîtrise en droit et société à l'UQÀM

Tandis que les Google, Apple, Facebook (Meta), Amazon et Microsoft (GAFAM¹) aimeraient se passer de toute réglementation et de cadre juridique et qu'ils défient constamment l'autorité des États, Alain Saulnier nous incite ici à prendre part à une mobilisation et une action collective pour faire face à ces entreprises privées. Dans ce plaidoyer pour le bien commun et la responsabilisation des instances concernées, l'auteur nous force à comprendre le caractère transversal de la menace que représentent ces géants.

Cet essai fouillé et percutant rend compréhensibles plusieurs des enjeux soulevés par la prolifération et l'accroissement des géants numériques, et il illustre la mesure de l'influence de ceux-ci sur les différentes sphères de notre société qu'ils traversent. Plus particulièrement, Alain Saulnier y appelle à une prise de conscience et à une mobilisation collective vis-à-vis des GAFAM, lesquelles s'avèrent nécessaires pour forcer une responsabilisation et une prise d'action concrète des structures gouvernementales. Force est de constater que sans l'implication de ces organisations, il paraît illusoire de penser rétablir le rapport de pouvoir foncièrement inégal qui caractérise notre relation avec ces géants.

Il importe donc notamment que nos gouvernant-e-s actualisent les conditions réglementaires dans lesquelles nous permettons à ces entreprises d'évoluer, ce qui implique *a priori* de reconnaître ces géants numériques pour ce qu'ils sont, c'est-à-dire une menace transversale et face à laquelle nous nous trouvons en situation de dépendance (laquelle n'a pu que s'accroître et se cristalliser par la pandémie de la COVID-19).

D'abord, le libéralisme et le laisser-faire qui caractérisent la posture de plusieurs États (sinon tous) à travers le monde permettent à ces superpuissances de cumuler une richesse inégalée dans l'Histoire, tout en bénéficiant d'évitement fiscal et de taux d'imposition dérisoires. L'auteur illustre ainsi comment ces géants en viennent à représenter une menace au rôle et à la définition de l'État, alors que la mondialisation numérique emporte une interdépendance économique, culturelle et sociale à la fois inégalée et inégalitaire (sur le plan de la souveraineté des États qui peut en découler).



En outre, l'impérialisme américain véhiculé par le biais de ces plateformes numériques porte aussi atteinte à notre spécificité et à notre patrimoine culturel, tandis que les artistes et le contenu culturel francophones et/ou issus des Premières Nations ou métis occupent une place bien réduite dans l'espace culturel et parmi l'offre de contenu mise de l'avant par ces géants.

L'auteur illustre ainsi comment ces géants en viennent à représenter une menace au rôle et à la définition de l'État, alors que la mondialisation numérique emporte une interdépendance économique, culturelle et sociale à la fois inégalée et inégalitaire (sur le plan de la souveraineté des États qui peut en découler).

1. L'acronyme GAFAM renvoie à Google-Apple-Facebook-Amazon-Microsoft, mais l'auteur renvoie dans cet ouvrage à plusieurs autres plateformes, notamment à YouTube, Netflix, Alphabet, Disney +, etc.

Tout cela s'accompagne de la difficulté des médias traditionnels à offrir des plateformes ou une offre de contenus comparables, notamment en raison du retard à agir qu'accuse le Conseil de la radiodiffusion et des télécommunications (CRTC), du caractère vétuste de *Loi sur la radiodiffusion* et de la *Loi sur les droits d'auteur*, qui se révèle dépassé par l'avènement des dites plateformes². Alors que d'une part, ces nouveaux médias peuvent agir sans grande contrainte, d'autre part, les médias traditionnels (notamment locaux et/ou publics) ne peuvent que pâtir de cet indubitable laisser-faire. Par ailleurs, il va sans dire que l'importance d'agir est redoublée, tandis que la désinformation et la propagation de fausses nouvelles par ces plateformes n'ont jamais été aussi visibles que dans le contexte de la pandémie que nous traversons. Pour l'auteur, il importe de repenser la forme des médias et de recentrer la mission de ces derniers qui doivent « se démarquer de la désinformation » ambiante, notamment par des pratiques de gouvernance transparentes et l'indépendance journalistique.

Ensuite, contrairement à ce que l'on pourrait penser, plateforme numérique ou virtuelle ne rime pas avec faible empreinte écologique et à ce titre les GAFAM (tant les installations que les structures sur lesquelles ils reposent) représentent une véritable catastrophe sur le plan écologique alors qu'internet est en voie de devenir la première source mondiale de pollution et que le numérique consomme pas moins de 10 à 15% de l'électricité mondiale.

Et enfin, si les enjeux de surveillance, de collecte et de monétisation des données personnelles des utilisatrices et utilisateurs des plateformes participent à un capitalisme de surveillance³ qui devrait tous nous inquiéter, il appert, au passage, pertinent de mentionner que les personnes judiciairisées (notamment en matières criminelle et carcérale, mais pas uniquement) sont dorénavant exposées à un système judiciaire qui mobilise de plus en plus, et à différents niveaux, ces plateformes et les outils qui en découlent ou qui s'y rapportent⁴.

Le déséquilibre de pouvoir à l'œuvre ne pourra être rétabli que si les gouvernements et les gouvernant-e-s mettent un terme à leur complaisance, adaptent leurs pratiques et réagissent promptement aux développements de ces géants. Seules une action concertée et la mobilisation d'acteurs sur le plan international permettront d'opposer une résistance efficace à ces forces hégémoniques.

Ce plaidoyer pour le bien commun et la mobilisation des instances concernées permet également de saisir l'ampleur de la menace actuelle, mais aussi de celle qui se profile à l'horizon. Alors qu'Amazon s'infiltrer maintenant dans nos universités, qu'il contracte avec le gouvernement du Québec et que les partis politiques ont recours à nos données personnelles (fournies par ces plateformes) pour influencer les élections, il devient tous les jours un peu plus urgent d'opposer une résistance à ces géants numériques pour lesquels, comme le dit Saulnier, l'univers est à conquérir et les frontières n'existent pas.

Seules une action concertée et la mobilisation d'acteurs sur le plan international permettront d'opposer une résistance efficace à ces forces hégémoniques.

Trop peu de personnes semblent saisir l'ampleur des maux et travers suscités par ces plateformes et leur influence grandissante. Cela laisse à penser que notre relation le plus souvent volontaire et de consommation vis-à-vis des services que nous offrent ces entreprises (et qui nous lient à celles-ci) peut expliquer qu'une forme de dissonance cognitive émerge de ce rapport. La contribution à la fois déconcertante et nécessaire proposée par cet ouvrage nous incitera, il faut l'espérer, à rompre de telles attaches.

2. À la suite de l'élection fédérale de 2021, le Gouvernement du Canada a repris l'engagement de faire adopter une *Loi modifiant la Loi sur la diffusion et d'autres conséquences*.

3. Shoshana Zuboff, *L'âge du capitalisme de surveillance*, Honfleur, Zulma Essais, 2019.

4. On peut penser à l'emploi de la visioconférence par les tribunaux judiciaires qui est beaucoup plus largement répandu depuis la pandémie, mais aussi aux liens qui existent entre différents outils qui émanent de la collecte de données personnelles et la justice actuarielle (Bernard E. Harcourt, *Against prediction : profiling, policing and punishing in an actuarial age*, The University of Chicago Press, 2007)



Profilage racial

Retour sur la *crise* au Service de police de la Ville de Québec

Maxim Fortin, coordonnateur de la Ligue des droits et libertés – Section Québec et politologue

Mélina Chasles, stagiaire à la Ligue des droits et libertés – Section Québec et organisatrice communautaire



Crédit : Scott Rodgerson sur Unsplash

Le profilage racial est l'une des formes de racisme systémique les plus fréquentes et constitue en soi une violation de droits. Pire, lorsqu'une interpellation policière tourne mal, ce profilage est souvent accompagné de violences et de brutalités qui mettent en danger la liberté, la sécurité et même la vie des personnes racisées. Nous avons pu le constater avec le cas de George Floyd aux États-Unis et avec celui de Fredy Villanueva au Québec. Depuis plusieurs décennies déjà, des voix s'élèvent partout dans le monde pour dénoncer cette forme de racisme. À l'automne 2021, un cas de profilage racial et de brutalité policière dans la Ville de Québec a relancé le débat et provoqué une polémique qui a fait de cette question un enjeu désormais central dans le dossier du vivre-ensemble.

Le 28 novembre 2021, des policiers du Groupe de relations et d'intervention policière auprès de la population (GRIPP) interpellent des jeunes afro-descendants sur la Grande Allée à Québec, à la sortie des bars. Les agents interviennent dans ce qui apparaît être une dispute entre fêtards éméchés, mais, rapidement, la tension monte d'un cran : les jeunes sentent alors qu'ils sont l'objet d'une attention démesurée de la part des forces de l'ordre. Un jeune homme et une jeune femme sont violemment interpellé-e-s. Le jeune homme est immobilisé au sol et un policier lui envoie de la neige au visage... La jeune femme est elle aussi maîtrisée et immobilisée. Le jeune homme a subi des blessures. Les images de l'arrestation montrant des agents largement supérieurs en nombre rudoyant des jeunes racisé-e-s et utilisant des



techniques rappelant celles qui ont causé le décès de George Floyd par arrêt respiratoire ne passent pas : leur publication sur les réseaux sociaux déclenche une salve de dénonciations. Rapidement, le nouveau maire Bruno Marchand fait part de sa volonté de faire la lumière sur cette histoire. L'affaire prend même une dimension nationale alors que le journaliste Antoine Robitaille¹, l'humoriste Eddie King² et le député fédéral Joel Lightbound³ expriment publiquement leurs préoccupations quant à ce dossier. Cinq policiers impliqués dans les événements sont suspendus et une enquête interne est déclenchée.

La diffusion des images et la dénonciation des actions du Service de police de la Ville de Québec (SPVQ) ont un effet inattendu. De nouvelles images sont alors rendues publiques, montrant cette fois-ci des agents du SPVQ brutalisant des personnes blanches dans des contextes où le suspect ne représente pas une menace directe. Le 30 novembre 2021, une nouvelle vidéo est publiée sur les réseaux sociaux. On peut cette fois-ci y voir des agents du SPVQ, membres de l'escouade GRIPP, malmener et blesser un client d'un restaurant du secteur Sainte-Foy lors de son arrestation⁴. Une autre vidéo est publiée pendant la semaine. Celle-ci montre un client d'un bar du centre-ville se faire projeter contre un mur⁵. Deux autres vidéos, moins médiatisées, témoignent quant à elles du niveau d'hostilité et d'agressivité des agents du SPVQ à l'égard des citoyen-ne-s lorsqu'ils sont contrariés. C'est donc la diffusion des vidéos de ces arrestations violentes qui mettent en lumière une problématique qui s'ajoute et se lie à celle du profilage racial : la brutalité policière flagrante du SPVQ et plus particulièrement de l'escouade GRIPP.

Pour la reconnaissance du profilage racial

Dans la foulée des événements, le collectif d'organisations à l'origine de la fresque publique *La vie des noir-e-s compte/ Black Lives Matter Qc*⁶, réalisée à l'été 2021, lance un appel à la mobilisation. La Ligue des droits et libertés – Section Québec, le Collectif 1629 et des groupes de la communauté afro-descendante de Québec organisent une marche le 4 décembre. Cette marche *Contre le profilage racial et la brutalité policière* réclame notamment la reconnaissance du profilage racial et des engagements fermes pour y mettre un terme. Le 5 décembre, le gouvernement du Québec annonce qu'une *Formation pour contrer le racisme et le profilage racial et social* sera mise en place pour l'ensemble des corps policiers de la province.

La Ville de Québec, visiblement ébranlée par cette histoire, annonce de nouvelles mesures pour rétablir la confiance envers son service de police. Un *Plan de développement pour de meilleures pratiques policières* est annoncé le 9 décembre. Le SPVQ s'associe à la Chaire de recherche sur l'intégration et la gestion des diversités en emploi (CRIDE) de l'Université Laval afin d'améliorer ses *compétences culturelles* et se pencher sur la question des *possibles biais inconscients*⁷. Elle annonce aussi l'embauche d'un examinateur externe en la personne de Mario Bilodeau. La Ville se montre aussi ouverte à la création d'un registre des interpellations et à une révision du mandat de l'unité GRIPP⁸.

Documenter les interpellations

La poussière est retombée au courant de l'hiver sans que les principales doléances des groupes et personnes racisées dans le dossier du profilage racial n'aient été satisfaites ou réellement entendues. La Ville de Québec et le SPVQ continuent de nier l'existence du profilage racial, sur la base d'un manque de données probantes permettant de le démontrer. Au même moment, la Ville de Québec refuse de produire des données sur l'ethnicité, l'origine ou la couleur de peau des personnes interpellées. Dans le cadre de la *Semaine d'actions contre le racisme* de mars 2022, les groupes antiracistes de Québec ont lancé une nouvelle mobilisation. Deux des trois revendications de cette mobilisation s'adressent directement à la Ville de Québec. Si la reconnaissance du racisme systémique par le gouvernement québécois fait toujours partie du programme, l'accent, cette année, a été mis sur la demande de documenter les interpellations faites par

1. En ligne : <https://www.journaldequebec.com/2021/11/30/il-sappelle-pacifique-1>

2. En ligne : <https://www.journaldemontreal.com/2021/11/29/arrestation-musclee-de-pacifique-eddy-king-annule-des-spectacles-a-quebec>

3. En ligne : <https://www.journaldequebec.com/2021/12/01/arrestations-musclees-a-quebec-une-enquete-externe-serait-mieux-selon-lightbound>

4. En ligne : <https://ici.radio-canada.ca/nouvelle/1844000/enquete-independante-spvq-protolino-police-quebec-intervention-arrestation>

5. En ligne : <https://ici.radio-canada.ca/nouvelle/1844406/quatrieme-video-spvq-crise-interventions-musclees-district-saint-joseph>

6. En ligne : <https://www.journaldequebec.com/2021/08/16/black-lives-matter-une-fresque-inauguree-dans-une-rue-de-quebec>

7. En ligne : <https://www.ledevoir.com/societe/653046/le-spvq-se-penchera-sur-ses-possibles-biais-inconscients>

8. *Ibid.*



le SPVQ en utilisant la méthodologie développée par l'équipe de recherche dirigée par les chercheurs Victor Armony, Mariam Houssaoui et Massimiliano Mulone. Précisons que c'est grâce à cette méthodologie qu'il a été démontré que, durant les dernières années, les personnes racisées ont été 2 à 3 fois⁹ plus interpellées à Montréal et à Repentigny¹⁰. La troisième et dernière revendication concerne la tenue d'une nouvelle consultation des groupes de la diversité ethnique et culturelle. Une marche a lieu le 27 mars.

La poussière est retombée au courant de l'hiver sans que les principales doléances des groupes et personnes racisées dans le dossier du profilage racial n'aient été satisfaites ou réellement entendues.

Quelques semaines avant, la Ville de Québec avait convoqué en comité plénier le SPVQ afin qu'il réponde aux questions des élu-e-s sur son travail. Loin d'avoir à se défendre ou à se justifier, le SPVQ a bénéficié de trois heures d'encensement par des membres du conseil municipal. La Ligue des droits et libertés – Section Québec et l'organisme communautaire Droit de cité¹¹ ont d'ailleurs dénoncé haut et fort cet exercice de promotion.

« Les élu-e-s de la Ville de Québec semblent préférer ignorer le sujet du profilage racial dans leurs questions posées au directeur du SPVQ. Bien que le comité plénier portait principalement sur le plan d'action mis en place à la suite des arrestations de l'automne dernier, plus de la moitié des questions posées concernait des sujets ayant pu être abordés à d'autres moments – les plaintes sur le bruit dans les rues, par exemple¹² ».

Néanmoins, certains acteurs politiques intéressés par le dossier continuent de faire pression afin d'instaurer des politiques publiques respectueuses des droits humains des personnes racisées. Le député solidaire Sol Zanetti a organisé une assemblée publique en mars sur la question du profilage racial. Plusieurs acteurs et groupes du mouvement antiraciste ont participé à la rencontre. La conseillère municipale Jackie Smith (Transition Québec), seule élue à aborder le profilage lors du comité plénier, a déposé le 21 mars dernier une proposition afin qu'une étude sur l'ethnicité, l'origine et la couleur de peau des personnes interpellées par la police soit réalisée à Québec et que cette étude utilise la méthodologie Armony¹³. Or, sa proposition ne fut ni appuyée par le comité exécutif ni par aucune autre personne élue du Conseil municipal; elle a donc été rejetée le 4 avril.

Néanmoins, certains acteurs politiques intéressés par le dossier continuent de faire pression afin d'instaurer des politiques publiques respectueuses des droits humains des personnes racisées.

La mobilisation pour faire pression

Que conclure de la *crise* au SPVQ et des mobilisations récentes contre le profilage racial? Premièrement, soulignons le manque de volonté politique de la Ville de Québec et de ses élu-e-s. Bien que sensibles à la question du racisme, les élu-e-s du Conseil municipal semblent sous-estimer la réalité du profilage racial et le degré de méfiance/défiante qu'il suscite au sein des populations racisées. Deuxièmement, la Ville de Québec semble ne pas vouloir s'opposer à ce que le SPVQ nie l'existence du profilage racial, tout en refusant de produire les données qui attesteraient de son ampleur. Troisièmement, les mobilisations contre le profilage racial ont fait en sorte que les communautés afro-descendantes de Québec sont plus mobilisées, qu'une perspective sociopolitique centrée sur la défense collective des droits et libertés émerge au sein des groupes racisés et que nous pouvons désormais construire un rapport de force avec les autorités afin de maintenir et d'accentuer la pression.

9. En ligne : https://spvm.qc.ca/upload/Rapport_Armony-Hassaoui-Mulone.pdf
En ligne : <https://cridaq.ugam.ca/wp-content/uploads/2021/09/Rapport-Armony-Hassaoui-Mulone-SPVR.pdf>

10. À Montréal, les personnes noires, autochtones et arabes avaient respectivement 4,2 fois, 4,6 fois et 2 fois plus de chances d'être interpellées que les personnes blanches, selon le rapport. À Repentigny, les personnes noires avaient 2,5 à 3 fois plus de chance d'être interpellées que les personnes blanches.

11. En ligne : <https://www.lesoleil.com/2022/03/06/un-exercice-dautopromotion-qui-fait-fi-des-abus-policiers-a-legard-de-certaines-citoyenes-52d4d2b93ef3d464a4126c543c931e42>

12. En ligne : <http://liguedesdroitsqc.org/2022/03/comite-plenier-des-fleurs-pour-le-spvq-et-des-elue-s-qui-tournent-autour-du-pot/>

13. En ligne : <https://www.carrefourdequebec.com/2022/03/jackie-smith-veut-documenter-le-profilage-racial-a-quebec/>

Les ficelles du capitalisme de surveillance

Cynthia Morinville, PhD, militante au comité environnement



Crédit : André Querry

L'importance du capitalisme de surveillance en émergence a été soulignée par l'hebdomadaire britannique *The Economist* qui titrait en 2017 « *Data is the new oil* » – les données sont le nouveau pétrole. Si la publication libérale saluait le potentiel de croissance et de productivité d'une économie basée sur les données, leur parallèle vaut aussi pour le côté moins reluisant de l'or noir. Si le pétrole nous a précipités dans une crise sociale et environnementale, les données risquent de nous y enfoncer.

Ce système économique a évidemment une empreinte écologique. Mais au-delà de l'impact environnemental d'une consommation effrénée encouragée par le capitalisme, quelle est l'empreinte écologique du capitalisme de surveillance? Quelles infrastructures soutiennent cette économie?

Le capitalisme de surveillance repose d'abord sur l'exploitation de mégadonnées, souvent mieux connues sous l'appellation *Big Data*. Pour que ce système d'exploitation fonctionne, ces données doivent circuler et elles doivent être assemblées en banques à partir desquelles des analyses peuvent être tirées. L'internet est une condition nécessaire à l'émergence

d'un capitalisme de surveillance, mais ce sont les récents développements de connectivité accélérée qui ont permis de réaliser le véritable potentiel des données massives.

Il est difficile de concevoir l'infrastructure physique d'une technologie accessible par un simple balayage de doigts sur un téléphone portable. Pourtant l'internet, malgré une accessibilité sans fil pour la vaste majorité des utilisateurs contemporains, repose bel et bien sur une infrastructure physique et matérielle. L'ampleur de ces infrastructures est telle qu'il est difficile d'en imaginer la magnitude. Le *Big Data* requiert une quantité de données gigantesque se déversant en torrent effréné. Un réseau immense de filage et de fibre optique connecte le routeur de chaque utilisateur au monde numérique permettant ainsi la copie et rediffusion de données connues sous l'appellation de *packets* à un intervalle de quelques millisecondes. Ces *packets* forment une série de relais qui permet à l'information de voyager sur des routes bien établies à travers le globe¹. À cela s'ajoutent des centres

1. Pour une exploration fascinante de l'envers de l'internet voir Andrew, Blum, 2012, May. *Tubes: A Journey to the Center of the Internet*. New York : Ecco.

Le monde de l'environnement

de données, des tours et des antennes. Cette infrastructure dépasse même les frontières de notre atmosphère alors que les constellations de microsattellites se multiplient.

L'expansion de la sphère de connectivité

Le capitalisme de surveillance ne se nourrit pas seulement du volume des données, mais aussi de leur type et de leur qualité. On cherche donc constamment à extraire des informations toujours plus précises sur nos habitudes quotidiennes. Des données plus variées demandent aussi plus de connectivité. En terme absolu, on assiste à ce qu'on pourrait appeler une expansion de la sphère de notre connectivité. Bien sûr, les bases de données sont nourries par notre utilisation de la téléphonie mobile et ses nombreuses applications. Elles le sont également par l'intermédiaire d'une collection de cartes de points et de privilège présentées chez les détaillants qui cartographient méticuleusement nos habitudes d'achat. La liste de nos points de connexion s'agrandit rapidement pour inclure certains modèles de voiture, les poignées de porte opérationnelles à distance, les électroménagers dits intelligents nous permettant de cuisiner à partir du bureau ou encore un réfrigérateur nous rappelant d'acheter du lait. L'internet des objets promet de connecter une panoplie d'outils du quotidien à l'internet et offre des gains en efficacité en échange d'un flux ininterrompu de données.

Pour réaliser ce monde connecté, il faut produire des appareils supportant la connectivité. En plus de l'empreinte écologique liée à la production d'électroménagers traditionnels, la connectivité de ces nouveaux produits à l'internet requiert de grandes quantités de matériaux et minéraux dits critiques, allant du lithium au cobalt en passant par les terres rares². En terme simple, plus de connectivité va de pair avec plus de production et d'extraction.

Ces données sont stockées dans des centres de données ayant non seulement une empreinte écologique notable à la production, mais aussi une importante empreinte énergétique à l'utilisation.

Toutefois, l'empreinte écologique du capitalisme de surveillance ne se limite pas à la production d'appareils technologiques. En effet, l'utilisation de ces technologies a aussi un impact environnemental. Le capitalisme de surveillance repose sur le stockage massif de données qui nécessite un volume grandissant de serveurs. Selon la firme allemande Statista, spécialisée en données concernant les marchés et la consommation, à la fin de 2021, 79 zetabytes³ de données avaient été générées mondialement. On s'attend à ce que ce volume, qui atteignait à peine 2 zetabytes en 2010, surpasse les 180 zetabytes en 2025. Ces données sont stockées dans des centres de données ayant non seulement une empreinte écologique notable à la production, mais aussi une importante empreinte énergétique à l'utilisation.

L'*International Energy Agency* estime que les centres de données et leurs réseaux de transmission étaient responsables d'approximativement 2 % de la consommation mondiale d'électricité en 2020. Cette grande consommation énergétique a poussé les entreprises du secteur des technologies de l'information et des communications à augmenter, au cours des dernières années, leur efficacité énergétique et leur consommation d'énergies renouvelables. Bien que les géants du web aient fait des gains importants en efficacité énergétique, leur consommation d'énergie en terme absolue continue d'augmenter. Le dernier rapport⁴ publié par Google chiffre cette consommation pour 2016 à 6,5 térawatts heures (TWh), 5 ans plus tard, en 2021, cette consommation atteignait 15,4 TWh. Au niveau mondial, alors que le trafic internet a triplé entre 2015 et 2020, la consommation d'énergie attribuée aux centres de données est restée plus ou moins stable et se chiffrait en 2020 à près de 200 TWh, selon l'*International Energy Agency*⁵. Ce plafonnement malgré les gains énergétiques s'explique entre autres par un effet rebond, appelé le paradoxe de Jevons, selon lequel les gains en efficacité sont annulés par une plus grande utilisation des technologies. Par exemple, alors que l'autonomie des batteries de nos téléphones portables s'est nettement améliorée au cours des dernières années, nous passons beaucoup plus de temps connecté au téléphone mobile en 2022 qu'on ne le faisait il y a à peine 5 ans. De ce fait, notre consommation d'énergie reliée à la téléphonie portable ne baisse pas ou augmente même.

2. Anthony Y. Ku, 2018. Anticipating critical materials implications from the Internet of Things (IOT): Potential stress on future supply chains from emerging data storage technologies. *Sustainable Materials and Technologies*, 15, p. 27-32. Le terme « terres rares » désigne un ensemble de 17 éléments du tableau périodique reconnus pour leurs propriétés magnétique et conductrice. Les gisements de terres rares coïncident souvent avec ceux d'autres éléments plus dangereux tels que l'uranium, le thorium, l'arsenic, le fluor et divers métaux lourds pouvant rendre leur extraction particulièrement dommageable pour l'environnement.

3. Un zetabyte est égal à 1 000 000 000 000 gigabites (GB), mille milliards de GB, ou 10¹² GB.

4. En ligne : <https://www.gstatic.com/gumdrop/sustainability/google-2021-environmental-report.pdf>

5. En ligne : <https://www.itu.int/en/ITU-T/climatechange/Documents/ITU%20AI4EE%20-%20George%20KAMIYA.pdf>

Le monde de l'environnement



Crédit : André Querry

Le développement de cet univers connecté a aussi un impact important sur la production de déchets. Le progrès technologique accélère l'obsolescence de ces technologies et raccourcit le cycle de vie de nos appareils. L'adoption du 5G, par exemple, promet de rendre caduques non seulement tous les appareils compatibles uniquement avec le 4G – ce qui inclut la majorité des téléphones portables que nous utilisons présentement – mais aussi toute l'infrastructure de ce réseau incluant les tours, les antennes et les transmetteurs. Notons que le volume de déchets électroniques produit mondialement en 2019 était déjà estimé à 53,6 millions de tonnes. Juxtaposés, ces déchets formeraient une mosaïque plus grande que l'île de Manhattan. En termes de volume, ils seraient équivalents à près de 5 300 Tour Eiffel⁶!

Le développement de cet univers connecté a aussi un impact important sur la production de déchets. Le progrès technologique accélère l'obsolescence de ces technologies et raccourcit le cycle de vie de nos appareils.

Les changements technologiques sont tels que le réseau 5G ne pourra passer par la même grille de connexion que son prédécesseur. Qu'advient-il alors de l'infrastructure actuelle? Dans certains endroits, comme les grands centres urbains où l'espace est un enjeu, elle sera remplacée, mais elle sera sans doute aussi laissée en place dans d'autres endroits où son démantèlement serait moins rentable. Dans ces endroits où le recyclage ne saurait générer de nouvelles opportunités économiques, elle deviendra l'artéfact d'une ère révolue un peu comme les stations radars du réseau d'alerte avancé (aussi appelé réseau DEW) qui parsème le territoire nordique de l'Alaska à l'Islande en passant par le Canada et le Groenland. Construites dans les années 1950, ces stations avaient nécessité plus de 30 000 tonnes de matériel acheminées par bateaux et avions afin de construire une ligne de défense visant à détecter les bombardiers soviétiques. Aujourd'hui, ce legs d'une autre époque et cette conception de la surveillance sont principalement laissés à une désintégration millénaire au gré des éléments et cela nous rappelle que la durée de vie courte de nos technologies ne raccourcit pas leur pérennité lorsqu'elles atteignent la fin de vie.

Alors qu'on nous promet des gains en efficacité et durabilité, la facture environnementale des technologies de l'information qui soutiennent le capitalisme de surveillance est appelée à grossir de pair avec la croissance de ce modèle économique.

6. Ces équivalences sont tirées du Global E-Waste Monitor 2017, et ajustées avec les données mise à jour en 2019.

La défense des droits humains, la voie vers une société juste et inclusive

Comme organisation phare de la société québécoise, la Ligue des droits et libertés agit sur plusieurs fronts, selon le principe de l'interdépendance des droits, pour assurer l'avancement des droits pour tous et toutes.

Nos actions en 2021-2022

NOS PUBLICATIONS

- Brochure *Pour une reprise en main collective de notre régime de santé*
- Revues Droits et libertés
Droits et handicaps / Droits de l'enfant

NOS LUTTES

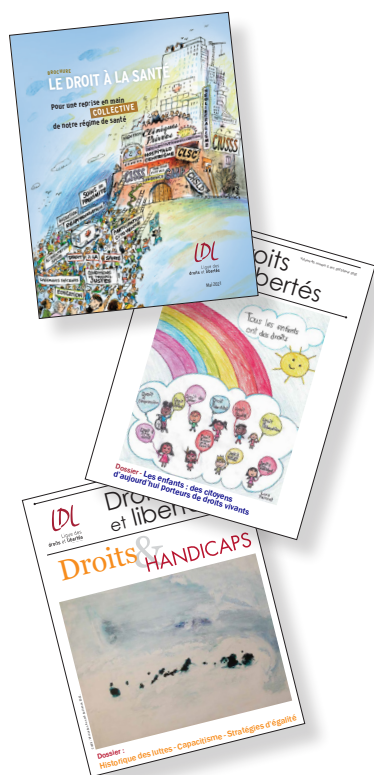
- Droit à la santé
- Droits économiques, sociaux et culturels incluant le droit au logement
- Droits humains et COVID-19 incluant la déclaration pour la levée de l'état d'urgence sanitaire
- Droit de manifester
- Droits des peuples autochtones
- Enjeux carcéraux et droits des personnes incarcérées
- Environnement et droits humains
- Pratiques policières
- Racisme systémique, exclusion sociale et laïcité de l'État
- Surveillance des populations et intelligence artificielle

NOS ÉVÉNEMENTS

- Série de deux visioconférences, *Le colonialisme médical au Québec*
- Visioconférence et lancement de la revue, *Droits et handicaps*
- Visioconférence sur les *Mesures d'exception : quels impacts sur l'état de droit?* dans le cadre des 20 ans depuis les attentats du 11 septembre 2001
- Visioconférence *Où en est le Québec dans sa lutte contre l'islamophobie?* Dans le cadre du 5e anniversaire de l'attentat de la Grande Mosquée de Québec
- Visioconférence *Quelle participation citoyenne des jeunes? À l'école, la ville et l'espace public* dans le cadre de la revue sur les droits de l'enfant

NOS MÉMOIRES

- Consultations particulières et auditions publiques sur la levée de l'état d'urgence sanitaire (PL 28)
- Consultation sur l'utilisation de la reconnaissance faciale, notamment par les services policiers



NOUVEAU SITE WEB
www.droitdemanifester.ca

LDL
Ligue des
droits et libertés

Visitez liguedesdroits.ca

pour devenir membre, faire un don

ou vous abonner à nos publications!



Ligue des
droits et libertés

Le capitalisme de surveillance : menaces à la démocratie et aux droits!

Appréhender le capitalisme de surveillance et les enjeux qui en découlent avec l'approche de l'interdépendance des droits, qui reconnaît que la réalisation d'un droit est intimement liée à celle des autres droits, ne peut que déclencher la sonnette d'alarme chez les militant-e-s pour la défense des droits humains.

En consacrant un dossier sur le capitalisme de surveillance, le comité éditorial de la revue souhaite dévoiler les angles morts du capitalisme de surveillance, sensibiliser aux rapides et profondes transformations qui s'opèrent ainsi qu'aux menaces que cela représente tant pour la démocratie que pour les droits humains.

Ce dossier vise à susciter des débats publics dans la population, loin des chambres d'écho, sur ces enjeux qui nous concernent toutes et tous.

Avec l'appui financier de :



FONDATION LÉO-CORMIER
pour l'éducation aux droits et libertés

LDL – Siège social

469, rue Jean-Talon ouest, #105
Montréal, QC H3N 1R4
Téléphone : 514 849-7717, #3221
Télécopieur : 514 878-1060
info@liguedesdroits.ca
liguedesdroits.ca

LDL – Section Québec

190-B, rue Dorchester, #70
Québec, QC G1K 5Y9
Téléphone : 418 522-4506
Cellulaire : 581 984-4506
info@liguedesdroitsqc.org
liguedesdroitsqc.org