10110
11001 BIG DATA
01101 SURVEILLANCE

SURVEILLANCE STUDIES CENTRE

Queen's UNIVERSITY

AU-DELÀ DE LA SURVEILLANCE DES MÉGADONNÉES

Liberté et équité

Rapport pour tous les Canadiens et Canadiennes

May 18, 2022

TABLE DES MATIÈRES

Remerciements
Résumé

Introduction

Problèmes persistants
- Déséquilibre informationnel
- Surveillance croisée
- Instruments inadéquats
- Groupes exposés

Défis à relever
- Partenariats public-privé
- Capitalisme de surveillance
- Technosolutionnisme
- Tri social

Et maintenant? Recommandations
- Protéger la vie privée et instaurer une justice des données
- Accroître la collaboration
- Sensibiliser le public et la population

Conclusion

REMERCIEMENTS

Ce rapport a été rédigé par David Lyon. Les membres de l'équipe de recherche sur la surveillance des mégadonnées et d'autres personnes ont mené des recherches et rédigé des articles et des livres au cours des sept années du projet. Des partenaires ont également grandement contribué aux travaux de recherches. Les publications ont été lues et résumées par Sachil Singh, dont le document de recherche a servi à structurer et éclairer le rapport, lequel a également bénéficié des commentaires de l'équipe de la haute direction – composée de Kirstie Ball, Colin Bennett, Stéphane Leman-Langlois, David Murakami Wood et Valerie Steeves – et de plusieurs autres personnes, notamment Mark Andrejevic, Adrian Kelly, Sachil Singh et Emily Smith. Le projet de recherche sur la surveillance des mégadonnées remercie le Conseil de recherches en sciences humaines du Canada de lui avoir accordé une subvention de partenariat. Un grand merci à toutes et à tous.

RÉSUMÉ

Introduction

Partout dans le monde, la surveillance augmente rapidement, particulièrement en période de pandémie de COVID-19. Le Canada fournit des exemples clairs, notamment l'accès aux données sur la santé publique par la police et l'utilisation des données de Telus pour l'analyse de la santé publique. La vie privée des citoyennes et des citoyens, mais aussi la liberté et l'équité sont en cause.

L'équipe de recherche sur la surveillance des mégadonnées a étudié les mégadonnées dans les domaines de la sécurité, du marketing et de la gouvernance. Par « surveillance », nous entendons tout moyen de découvrir la vie des gens pour mieux les gérer ou les influencer. Cette surveillance se produit dans le domaine du renseignement pour la sécurité nationale et des services de police; dans le domaine du marketing, qu'il s'agisse d'analyser les préférences des consommateurs ou d'amener les électeurs à voter pour un parti politique; ainsi que dans le domaine de la gouvernance, notamment dans les villes dites intelligentes, par le projet avorté « Sidewalk Labs » à Toronto ou par l'entremise d'appareils et d'outils intelligents comme Alexa. Notre quotidien est de plus en plus numérique, avec ses bons et ses mauvais côtés.

Problèmes persistants soulevés par la recherche

- **Déséquilibre informationnel:** Les citoyens et les consommateurs n'ont pratiquement aucune idée des données qui sont recueillies à leur sujet, sans parler des conséquences de devenir visibles, alors que les entreprises et les ministères recueillent d'énormes quantités de données sur les Canadiennes et les Canadiens, souvent pour les utiliser de façon non précisée.

- **Surveillance croisée:** Avant l'ère numérique, la surveillance était beaucoup plus simple. De nos jours, la surveillance est complexe, tant sur le plan organisationnel que technique. Peu d'entre nous avons une idée claire de ce qu'est l'analyse des données, et les exigences juridiques sont opaques et omettent souvent de traiter des détails de la surveillance. La pandémie contribue à rendre la situation encore plus complexe.

- **Instruments inadéquats:** Les règlements qui visent à contrôler l'évolution des technologies et des pratiques peinent à suivre le rythme beaucoup plus rapide de ces changements. Les réseaux sociaux, les entreprises de plateforme et les téléphones intelligents respectent peu de règles et ne se heurtent qu'à une faible résistance qui pourraient contribuer à façonner la technologie de manière plus appropriée.

- **Groupes exposés:** Tout le monde n'est pas touché de la même façon; certains groupes, comme les femmes, les Noirs et les autochtones, sont particulièrement vulnérables à la surveillance d'aujourd'hui. En temps de crise, comme lors d'une pandémie, leur situation est susceptible de s'aggraver.

"Notre monde post-pandémique nécessite des mesures réfléchies et décisives pour évaluer et affronter le monde émergent de la surveillance, omniprésent et souvent discriminatoire."

Voici les défis qui nous attendent:

- **Partenariats public-privé:** Les limites brouillées entre le gouvernement et les entreprises; l'application Alerte COVID en est un exemple. Cette surveillance relie des sphères autrefois distinctes, engendrant le besoin de politiques adéquates qui portent sur le lien entre ces deux entités.

- **Capitalisme de surveillance:** Le capitalisme de surveillance consiste à recueillir des données quotidiennes dans le but de les vendre. Les données peuvent être réutilisées à d'autres fins, notamment par le gouvernement et les services de police. Nous devons sensibiliser davantage les utilisateurs et trouver de nouveaux modes pour limiter la surveillance.

- **Technosolutionnisme:** De la même manière que lors des événements du 11 septembre, en réponse à la pandémie, des « solutions » technologiques ont été précipitées pour montrer que le gouvernement agit et que les entreprises offrent ce qu'elles prétendent être des outils numériques à jour pour répondre aux besoins.

- **Tri social:** La surveillance permet non seulement de « voir » les gens, mais aussi de les classer par groupes auxquels s'appliquent différents traitements. Cette pratique pose un risque de discrimination négative et d'injustice, plus particulièrement pour les personnes déjà vulnérables. Il est essentiel de reconnaître ces problèmes et de s'y attaquer.

Et maintenant? Recommandations:

- **Protéger la vie privée et instaurer une justice des données:** Si la protection de la vie privée est une bonne chose, elle ne suffit plus pour la société numérique actuelle. Les préjudices sociaux de la surveillance d'aujourd'hui soulignent la nécessité de nouveaux droits numériques et d'une justice en matière de données. La surveillance ne consiste pas seulement à recueillir des données personnelles, mais aussi à les analyser à l'aide d'algorithmes et à les utiliser en vue d'atteindre divers objectifs.

- **Accroître la collaboration:** La nécessité d'une collaboration active entre les chercheurs des sciences humaines et informatiques, les organismes de réglementation et la société civile est soulignée par l'urgence causée par les développements rapides et souvent non contrôlés de la surveillance dans la société numérique. De toute évidence, la participation de l'ensemble des citoyens et des consommateurs est une priorité.

- **Sensibiliser le public et la population:** La surveillance des mégadonnées touche chaque personne qui compose la société canadienne diversifiée d'aujourd'hui. Il incombe de prendre conscience de la situation et de la façon dont la surveillance affecte les choix et les chances au quotidien. L'information exacte, accessible et vulgarisée, qu'elle soit sous forme écrite, vidéo ou balado, est essentielle.

Conclusion:

Notre monde post-pandémique nécessite des mesures réfléchies et décisives pour évaluer et affronter le monde émergent de la surveillance, omniprésent et souvent discriminatoire. Les enjeux méritent d'être à l'avant-plan de l'éducation de chacun; de l'utilisation sécuritaire des téléphones intelligents aux systèmes informatiques responsables. Nous avons besoin de nouveaux modes d'évaluation et de réglementation des développements numériques. Une société plus libre et plus juste est un monde à l'échelle plus humaine.

AU-DELÀ DE LA SURVEILLANCE DES MÉGADONNÉES

Liberté et équité

Au XXIe siècle, la surveillance est rapidement devenue un élément central de la vie quotidienne contemporaine. Sa forte présence se fait ressentir dans les organisations de toutes sortes, qu'il s'agisse du maintien de l'ordre et de la sécurité, du suivi des travailleurs, d'analyses de santé publique ou de profilage généralisé par les entreprises propriétaires de plateformes. De nos jours, la surveillance bénéficie dépend de l'infrastructure numérique qui a permis la mise en place rapide et à grande échelle de systèmes d'informatique distribuée de toute taille, et de la participation active de millions de personnes qui, sciemment ou non, contribuent à sa croissance.

La surveillance des citoyens et des consommateurs par l'État et les entreprises ne cesse d'augmenter au Canada et dans le monde entier. La pandémie de COVID-19 a favorisé cette croissance. Outre le suivi autorisé des données personnelles à des fins épidémiologiques, les services de police de l'Ontario ont effectué des recherches dans les bases de données médicales sur la COVID-19 en lien avec les cas actifs[1] pendant plusieurs mois, jusqu'à ce que l'atteinte aux libertés civiles soit dénoncée, en 2020. Les personnes qui subissaient un test de dépistage de la COVID-19 n'avaient aucune idée que leurs données n'étaient mises à la disposition de la police ni des fins pour lesquelles ces données étaient utilisées. Les libertés tenues pour acquises étaient compromises.

Au niveau fédéral, il a été révélé en 2021 que l'entreprise de télécommunications Telus a vendu des données de localisation de téléphone mobile, établissant un lien entre des téléphones cellulaires et des cas actifs de COVID-19, à l'Agence de la santé publique du Canada, afin de suivre la trajectoire du virus de la COVID-19 et de vérifier si le confinement était respecté.[2] Bien qu'elles aient été anonymisées, de telles données peuvent être réidentifiées. Mais au-delà des enjeux de protection de la vie privée et de transparence, une telle surveillance de la population conduit non seulement à rendre les gens visibles, mais à les représenter et à les traiter de manière spécifique. Une plus grande discrimination contre certains groupes vulnérables peut s'en suivre, entraînant du même coup un enjeu d'équité.

Il y a quelques années à peine, le mot à la mode était « mégadonnées ». De nos jours, nous parlons plutôt de l'intelligence artificielle (IA) et de l'apprentissage machine, ainsi que de leur relation avec les technologies « intelligentes » et l'Internet des objets. Ces changements ne témoignent que partiellement des changements réels; après tout, l'IA nécessite encore d'énormes quantités de données. La recherche sur ces questions devient donc de plus en plus urgente, tant pour comprendre les réalités d'une société numérique que pour intervenir à l'aide de stratégies appropriées permettant de favoriser à la fois la liberté humaine et l'équité sociale. Les préoccupations classiques à l'égard de la protection de la vie privée et de la liberté sont maintenant liées à la priorité, tout aussi pressante, des droits et de la justice en matière de données comme objectifs pour les gouvernements et les entreprises.

Projet de recherche sur la surveillance des mégadonnées

En 2016, le Centre des études sur la surveillance de l'Université Queen's a lancé un projet de cinq ans, financé par le CRSH, sur la surveillance des mégadonnées et dont les travaux portaient sur trois domaines, soit la sécurité, le marketing et la gouvernance. La diversité des contextes soulève la question suivante : la surveillance est-elle le meilleur concept pour bien saisir ces différentes pratiques? Nous croyons que la surveillance d'aujourd'hui est mieux comprise au sens large, c'est-à-dire toute attention systématique, routinière et ciblée aux renseignements personnels qui vise à gérer, contrôler, protéger et influencer. Chaque domaine peut être envisagé comme un lieu clé pour l'exploitation des mégadonnées, c'est-à-dire la collecte, l'agrégation, l'analyse et l'utilisation à grande échelle des données par et sur des personnes et des choses, ainsi que sur des interactions entre ces personnes et ces choses, dans le but de générer des prédictions et d'obtenir des renseignements autrement inaccessibles.

Des développements déterminants ont été étudiés dans le cadre de la recherche sur la surveillance des mégadonnées, notamment les changements dans les services de renseignement et de police depuis l'affaire Snowden[3], l'utilisation des mégadonnées lors des élections politiques dans la foulée du scandale Cambridge Analytica[4], la croissance rapide des utilisations commerciales et marketing de l'analyse des données[5], et la hausse marquée d'entreprises de plateformes, de « villes intelligentes » et de la surveillance « intelligente » en général[6]. Dans chaque cas, nous souhaitions répondre à la question suivante : comment les mégadonnées sont-elles utilisées et quelles sont les incidences sur la politique publique, plus particulièrement la protection de la vie privée, la protection des données et au-delà? Cette question est vitale à une époque où la collecte, l'analyse et l'utilisation des données quotidiennes sont devenues la norme pour toutes les organisations, qu'elles soient commerciales, gouvernementales ou autres.

Au cours des dernières années, le champ d'application des mégadonnées s'est considérablement élargi, entraînant des changements constants et parfois turbulents, mais les enjeux communs dans chacun des domaines sont les suivants : d'une part, il y a la question de savoir à quels droits la surveillance accrue peut porter atteinte : la vie privée, l'autodétermination et le « droit à l'oubli ». D'autre part, il y a les enjeux éthiques, de discrimination et de justice qui, ensemble, constituent le « tri social ». La classification et la catégorisation automatisées de différents groupes produisent des résultats incohérents et parfois incontestablement injustes. Qui plus est, le pouvoir appartient clairement à ceux qui possèdent l'équipement sophistiqué nécessaire pour accumuler, stocker et interpréter les données.

Lorsque la pandémie mondiale de COVID-19 a éclaté, les membres de l'équipe ont porté leur attention sur la façon dont les mégadonnées sont utilisées dans la gestion d'une crise de santé publique. En raison de l'intérêt et de l'enthousiasme déjà présents des gouvernements et des entreprises à l'égard de l'exploitation des mégadonnées, les défis posés par certaines réponses hâtives et technosolutionnistes à la pandémie ont précisé notre recherche. Les retards imposés à nos travaux par la pandémie nous ont naturellement menés à nous pencher aussi sur la surveillance appliquée à la santé publique[7].

Un inventaire minutieux et exhaustif de l'ensemble de nos travaux[8] montre que notre recherche sur la surveillance des mégadonnées révèle la prédominance croissante du numérique dans le quotidien des citoyens et les quantités énormes de renseignements qui en sont tirés. La complexité des enjeux qui se recoupent dans chaque sphère s'est précisée encore davantage. Les principaux thèmes découlant de nos travaux de recherche sont le déséquilibre informationnel, qui touche particulièrement les électeurs; la surveillance croisée, qui est complexe et abstraite pour beaucoup, de citoyens et d'exploitants; les instruments inadéquats et le manque de transparence; ainsi que les groupes exposés; notamment leur vulnérabilité et leur manipulation.

Dans les pages qui suivent, nous étudions plus en détail ces principaux thèmes, nous présentons les principaux défis et, enfin, nous proposons des pistes de solution appropriées.

PROBLÈMES PERSISTANTS

Cette section du rapport porte sur les « problèmes persistants » entourant la surveillance et les données, comme le révèle notre recherche. Bien entendu, aucun problème dans ce domaine n'est simplement « nouveau ». Il s'agit, pour la plupart, de vieux problèmes sous une nouvelle forme, qui nécessitent une attention urgente pour deux raisons : leurs effets sont ressentis plus intensément par les populations auparavant moins touchées, et les anciens remèdes ne suffisent plus. Par le passé, par exemple après la Seconde Guerre mondiale, les enjeux de surveillance portaient principalement sur les documents papier, les communications téléphoniques et l'utilisation d'appareils photo à pellicule. L'informatique en était à ses débuts et n'était toujours pas associée aux technologies de communication. Les technologies numériques actuelles entraînent des bouleversements sans précédent dans le monde de la surveillance, permettant une surveillance omniprésente 24 heures sur 24, 7 jours sur 7, dans toutes les institutions gouvernementales, administratives et commerciales. Le quotidien en est profondément changé, parfois pour de bonnes raisons. En revanche, les conséquences négatives sont ressenties plus profondément par les personnes déjà désavantagées.

Déséquilibre informationnel

Le déséquilibre informationnel ou l'asymétrie d'information se produit lorsque des citoyens ou des consommateurs ne sont pas informés de la manière dont leurs données sont utilisées par les ministères gouvernementaux ou les grandes entreprises. En termes simples, les grandes organisations recueillent une quantité énorme de renseignements sur les citoyens ordinaires, les consommateurs, les travailleurs, les étudiants, les enfants et ainsi de suite. Qui plus est, les capacités croissantes de traitement de données de ces entités leur confèrent un avantage incommensurable.

Au Canada, comme dans d'autres pays démocratiques, les organismes de sécurité doivent rendre des comptes aux citoyens qu'ils ont le mandat de protéger. C'est le cas entre autres du le Centre de la sécurité des télécommunications (CST) et des services de police. Or, les enquêtes sur ces organismes s'avèrent particulièrement difficiles. Par exemple, pour simplement découvrir comment le CST utilise les mégadonnées, il faut procéder par demande d'accès à l'information[9]. Pourtant, les citoyens sont tenus dans l'ignorance au sujet de ces organismes, ils souffrent clairement des conséquences d'un déséquilibre informationnel. Les citoyens bénéficieraient d'une plus grande transparence, afin de forcer ces organismes à rendre démocratiquement des comptes. Les citoyens méritent d'être rassurés sur le fait qu'ils ne font pas l'objet d'une surveillance inutile ou illégale.

Le déséquilibre informationnel peut aussi être clairement observé dans le cas du scandale de Cambridge Analytica, où des profils psychographiques avaient été créés à partir de données extraites de Facebook, puis combinés à des données sur l'ensemble des électeurs pour tenter d'influencer les élections. Ces citoyens n'avaient aucune idée que le « questionnaire de personnalité » sur Facebook auquel ils avaient accepté de participer serait utilisé de cette façon. Ils étaient doublement désavantagés par le déséquilibre informationnel en cause[10].

Les techniques utilisées pour rendre les jeunes plus transparents pour les entreprises constituent un autre exemple de déséquilibre informationnel en marketing. La poupée « Hello Barbie », par exemple, pouvait « discuter » avec des enfants à l'aide d'algorithmes « conçus pour encourager des modes particuliers de consommation »[11]. On ne peut pas s'attendre à ce que les enfants disposent des connaissances et des attentes adultes lorsqu'ils sont exposés à des communications en ligne, ce qui les rend encore plus vulnérables aux messages et à la manipulation. Comme l'observe Valerie Steeves, cette transparence des enfants « fait pencher la balance en faveur de l'entreprise »[12].

Aussi, au plus fort de la pandémie, les citoyens ordinaires n'avaient aucun moyen de savoir comment leurs données sur la santé étaient utilisées : Que faisait la police de l'Ontario avec les données de traçage des contacts liés à la COVID-19?[13] Des milliers de recherches non autorisées ont été effectuées dans le portail des « premiers intervenants » pour la COVID-19 à l'aide de codes postaux pour repérer des cas actifs. L'attention du public n'a pas non plus été accordée au ciblage de maisons ordinaires par des entités commerciales lorsque l'espace domestique a été conscrit pour l'emploi, le divertissement, l'éducation et le magasinage. Pourtant, de cette façon, le déséquilibre de l'information s'est une fois de plus accentué au cours de la pandémie.[14]

Nos recherches ont également servi d'information documentaire pour créer une série de courts métrages d'anticipation à court terme qui mettent en lumière les enjeux de surveillance contemporains. Le court métrage *Blaxites* illustre de façon spectaculaire cette asymétrie. Il raconte le quotidien d'une élève anxieuse qui accepte de porter un bracelet électronique, fourni par son médecin, pour faire le suivi de ses activités. Il montre comment l'interaction entre les bases de données médicales peut rendre certains patients plus vulnérables et les désavantager de manières inattendues.[15]

Surveillance croisée

La surveillance « croisée » se produit lorsque la surveillance s'étend au-delà de la simple observation ou du suivi, de sorte à devenir tordue, emmêlée, compliquée et amalgamée ou, en d'autres termes, complexe. Cette complexité constitue un deuxième facteur clé. Il en résulte que de moins en moins de personnes comprennent la surveillance, ce qui contribue également au déséquilibre informationnel à son sujet. La surveillance d'aujourd'hui est terriblement entremêlée. La complexité entoure non seulement les « cibles » de la surveillance (utilisateurs, citoyens), mais aussi les organismes qui *effectuent* la surveillance.

Les analystes de la sécurité sont de plus en plus souvent appelés à être des experts en mégadonnées. De même, les spécialistes du marketing ont du mal à suivre les chefs de file de l'analyse des données. Parallèlement, les exigences juridiques sont souvent opaques, car elles ont été créées et étoffées de manière décousue, souvent bien avant le développement de la complexité que l'on connaît aujourd'hui. Peu de ministères ou agences comme le CST, ou de spécialistes du marketing dans de nouveaux domaines, semblent chercher activement à s'assurer que leurs activités liées aux données sont appropriées.

Comme le fait remarquer Sachil Singh, « certains des principaux enjeux liés à cette approche sont que les fins de la mise en œuvre technologique ne sont pas définies, que les méthodes de mise en œuvre ne sont pas claires et que les résultats escomptés sont inconnus »[16]. De nombreux observateurs ont déjà contaté le décalage entre l'obsession d'adopter des pratiques fondées sur les données d'une part, et la volonté d'adopter des dispositions juridiques de l'autre[17]. D'après certains chercheurs, l'augmentation des pratiques de commercialisation manipulatrices pourrait être liée à la lutte pour l'influence dans une ère axée sur les données. Si c'est le cas, la liberté d'action des consommateurs continuera d'en souffrir[18].

L'intelligence artificielle entraîne souvent le déplacement du travailleur humain, ce qui témoigne de la nécessité d'une plus grande transparence algorithmique et de lignes directrices éthiques plus vastes, alors même que les machines s'autoprogramment de plus en plus. Malheureusement, peu de personnes, même chez les informaticiens, ont défini ce à quoi pourrait correspondre cette transparence. Les propositions évoquent l'assurance qu'il y ait toujours la présence d'un « humain dans la chaîne ». En revanche, divers organismes, dont les services de police, continuent de faire pression pour recourir davantage à l'analyse des données, malgré leurs capacités douteuses à les utiliser dans le cadre de leurs activités de renseignement policier[19]. Au CST rien n'indique que l'utilisation des nouvelles méthodes axées sur les données soit accompagnée d'un sentiment des obligations qui en découlent - comme la responsabilité envers le public et une réforme de sa culture du secret[20].

Sur un autre plan, au début de la pandémie, la création de nouvelles bases de données intégrées sur la santé publique en Ontario a été réalisée de manière précipitée, sans consultation adéquate ni transparence. Des modifications de la LAIPVP et de la LPRPS[21] ont été apportées rapidement dans le cadre d'un projet de loi omnibus. Ici aussi, la complexité de la surveillance croisée l'a rendue opaque. Comme le fait remarquer Teresa Scassa, ces modifications « seraient difficiles à comprendre ou à contextualiser pour un citoyen ordinaire qui n'est pas aidé; et certaines modifications sont franchement presque insaisissables »[22].

Instruments inadéquats

La vitesse à laquelle la surveillance évolue, alors que la dépendance aux technologies de plus en plus abstraites se poursuit, fait en sorte que les règlements et les lois régissant une telle surveillance sont de moins en moins adaptés aux conditions actuelles. La transition vers les mégadonnées, l'intelligence artificielle, l'apprentissage automatique et l'« intelligence » qui en résulte – par exemple, votre voiture qui recueille des données sur vos habitudes de conduite et qui peut même surveiller votre regard pour savoir si vous regardez la route[23] – n'avaient pas été anticipées par ceux qui ont adopté bon nombre des lois existantes pour restreindre la surveillance inappropriée ou excessive. Ces instruments ne sont souvent pas adaptés aux conditions actuelles. Ils sont inadéquats.

Par conséquent, la loi, la réglementation et la transparence n'évoluent pas en fonction des changements réels dans les pratiques de gestion des données qui surviennent à un rythme effréné. Ni l'équilibre démocratique du pouvoir entre l'État et les citoyens, ni les conditions relativement équitables tenues pour acquises par de nombreux consommateurs à l'égard des entreprises, ne peuvent être facilement maintenus dans le contexte actuel d'utilisation des données. Le contrat social entre l'État et les citoyens – et maintenant, peut-être, entre les entreprises et les consommateurs – s'il a réellement existé, est soumis à d'énormes pressions[24]. Le flou qui existe entre les secteurs public et privé, par exemple, s'est intensifié et est davantage exacerbé par des motifs pandémiques qui invitent à de plus amples analyses de données.

À titre d'exemple, pendant la pandémie, des données recueillies commercialement ont été utilisées à des fins de suivi du virus par la Santé publique. Comme nous l'avons noté dans l'introduction, la société de télécommunications Telus a vendu des données de localisation de 33 millions de Canadiens à l'Agence de la santé publique du Canada (ASPC). En février 2022, le Comité ETHI de la Chambre des communes a tenu des audiences pour en apprendre davantage sur la façon dont cette affaire s'est produite, pour découvrir qui l'a autorisée et pour en savoir plus sur la manière exacte dont les données ont été utilisées, sans parler de la question de savoir si les motifs de la légalité de ces données avaient été mis à l'épreuve. Après avoir indiqué que ce cette affaire comportait plusieurs aspects inappropriés, le Commissaire à la protection de la vie privée a conclu que *les deux* lois fédérales sur la protection des renseignements personnels devraient être « mises à jour simultanément » afin de reconnaître l'importance des interactions approfondies entre les données des secteurs public et privé[25].

Sur la question des entreprises de plateforme comme Facebook, l'un des principaux problèmes est leur habileté notoire à échapper aux contraintes juridiques et leur faible transparence concomitante[26]. Facebook insiste sur le fait qu'elle *possède* les données des utilisateurs, tout en exploitant un monopole. Or les instruments mis à notre disposition pour réduire le pouvoir de telles plateformes sont généralement très inadéquats. Le traitement des données et la protection des renseignements personnels relèvent du Commissaire à la protection de la vie privée, les aspects monopolistiques du Commissaire de la concurrence, et les possibilités de faire des réseaux sociaux un service public, du Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC)[27].

Une autre difficulté vient du fait que les lois et les règlements, sont souvent adoptés de bonne foi mais pour faire face à des situations de surveillance très ponctuelles, souvent qui se sont produites il y a des décennies, et qui ne trouvent plus d'application à l'ère des mégadonnées, de l'intelligence artificielle et des technologies dites « intelligentes ». Aujourd'hui, la tâche plus large qui s'impose est de déterminer ce qui est considéré comme des « renseignements personnels », une question à laquelle nous reviendrons un peu plus loin.

En plus des retards dans l'élaboration de nouvelles lois en matière de protection des renseignements personnels et de la vie privée, l'avalanche constante de nouvelles lois qui autorisent de plus en plus de surveillance souligne l'importance du travail des groupes de défense des droits[28].

Un problème secondaire est que la transparence des organismes de surveillance, bien que cet aspect ne soit pas en soi la « solution », est très faible. Les exigences en matière de transparence doivent refléter la réalité des époques axées sur les données, tout en gardant à l'esprit que *l'objectif de la transparence* est toujours d'assurer *la responsabilisation* de ceux qui poursuivent des activités de surveillance intelligente axée sur les données.

Groupes exposés

Bien que les trois « problèmes persistants » précédents touchent l'ensemble de la société, ils n'affectent pas chaque personne dans la même mesure ou de la même manière. Certains groupes sont plus exposés à la surveillance que d'autres, et cette vulnérabilité sociale peut être observée pour chacun des problèmes discutés précédemment. La surveillance s'immisce de plus en plus dans la sphère intime, ce qui rend ses cibles plus vulnérables à la manipulation.

Les peuples autochtones constituent un groupe pour qui le risque d'une surveillance disproportionnée est clairement démontré, surtout lorsqu'ils exercent leur droit de protester[29]. Les leaders individuels, les communautés et les mouvements font l'objet d'une surveillance additionnelle. Cindy Blackstock, par exemple, militante Gitskan pour la protection de l'enfance et professeure à l'Université McGill, a été surveillée par Affaires autochtones et du Nord et le ministère de la Justice entre 2009 et 2011. Les manifestations contre les pipelines ou la destruction des forêts font l'objet d'une surveillance policière intensive sous prétexte de « menaces à la sécurité nationale », ce qui rejoint les hypothèses coloniales sur la propriété des terres[30].

Les services de police en milieu urbain révèlent également que les personnes noires dans les villes canadiennes font l'objet d'un niveau de surveillance plus élevé que les autres[31]. De façon beaucoup moins spectaculaire, mais non moins grave, les femmes noires subissent également une surveillance négative dans les domaines des soins de santé et les domaines connexes, entraînant une *sous-représentation* en raison de « lacunes statistiques »[32]. Les inégalités et les iniquités en matière de surveillance médicale peuvent également désavantager les femmes au Canada à long terme et tout au long de leur vie[33].

La vulnérabilité sociale s'accroît au fur à mesure que la manipulation par la surveillance intime prend de l'ampleur. Ce thème chevauche les trois précédents et touche les citoyens, les consommateurs, les employés et de nombreux autres groupes. Peu de gens arrivent à suivre le rythme et l'ampleur de l'évolution de l'analyse et de l'utilisation des données, donnant lieu à une diminution de la protection, surtout pour les plus vulnérables. Il n'y a plus de solutions aux enjeux de consentement. Les plateformes deviennent de plus en plus abusives. Avant la pandémie, les personnes racialisées et les personnes socioéconomiquement défavorisées étaient les plus durement touchées, et cette réalité s'est aggravée depuis.

LES DÉFIS QUI NOUS ATTENDENT

Partenariats public-privé

Les conséquences de la collaboration entre les entreprises et les gouvernements dans la production et l'utilisation des modes de surveillance sont énormes et se multiplient. Comme en témoigne la série de travaux de Kirstie Ball et de Laureen Snider, *The Surveillance-Industrial Complex*, les entreprises et les gouvernements ont un long historique de collaboration dans des domaines allant de la sécurité et des services de police aux relations industrielles, en passant par le développement militaire et le marketing[34]. L'augmentation rapide des partenariats public-privé (PPP), encouragés par le néolibéralisme à partir des années 1990, a également fait intervenir la surveillance, par exemple dans le cadre du développement de la surveillance par caméra au Royaume-Uni, puis aux États-Unis et au Canada.

La collaboration entre l'État et les entités commerciales en matière de surveillance, qui est devenue de plus en plus visible depuis le début du siècle, apparaît clairement depuis les événements du 11 septembre. L'expansion des réseaux sociaux a donné accès à de nouveaux types de données, générées par les utilisateurs, qui ont rapidement été très prisées par les organismes de sécurité nationale et les services de police, une relation publique-privée qui continue de prospérer. La pandémie de COVID-19 a aggravé cet enjeu de plusieurs façons dans le monde entier, comme nous l'avons constaté, par exemple, avec les systèmes numériques de traçage des contacts et de preuves de vaccination.

Alors que les gouvernements en viennent à s'appuyer de plus en plus sur des formes de gestion à grand volume de données, le stockage et le traitement de ces données sont souvent refilés à des entreprises privées, de telle sorte que les ministères deviennent redevables à ces entreprises, dont les impératifs commerciaux peuvent être en contradiction avec la responsabilité publique et le contrôle démocratique.

En raison du complexe industriel de la surveillance au Canada, les relations entre l'État et les entreprises sont plus solides et encore plus tenues pour acquises que jamais auparavant[35]. Nous devons impérativement faire preuve de réalisme à ce sujet pour faire avancer la réglementation et le contrôle de la surveillance inutile, excessive et illégale. En d'autres termes, tout programme visant à réduire la surveillance requiert la participation du gouvernement et de l'industrie, ainsi que des institutions de recherche indépendantes et d'autres organismes et réseaux pertinents de la société civile.

Capitalisme de surveillance

L'essor du capitalisme de surveillance est essentiel à notre compréhension des principaux enjeux actuels de surveillance. Il consiste en la marchandisation des renseignements personnels de tous les jours à des fins de profits commerciaux. Toutefois, la complicité des consommateurs continue de jouer un rôle important. Le capitalisme de surveillance repose sur la participation volontaire de ses utilisateurs. Le point positif de cet enjeu est que ses effets pourraient être atténués par des utilisateurs informés et actifs.

La question du pouvoir est cruciale. Comme le soutient Jim Balsillie, les déséquilibres structurels du pouvoir sont exacerbés par le capitalisme de surveillance. L'ampleur

et l'efficacité de l'analyse des données, plus particulièrement l'utilisation de l'intelligence artificielle et la prise de décision algorithmique, exposent les citoyens et les consommateurs à l'identification, mais aussi aux relations de pouvoir dont l'objectif principal est d'influencer les comportements[36]. Ce fait a été reconnu par Daniel Therrien, commissaire fédéral à la protection de la vie privée, qui, dans son rapport annuel de 2021, met également en garde contre « la puissance croissante des géants de la technologie comme Facebook et Google [qui semblent] en savoir davantage à notre sujet que nous en savons nous-mêmes »[37].

La sensibilisation du public au capitalisme de surveillance a été considérablement renforcée par la publication du livre de Shoshana Zuboff en 2019, mais la conscience populaire de ses implications dans notre quotidien demeure faible (même si vous avez regardé le documentaire *Derrière nos écrans de fumée* [*The social Dilemma*][38]). Le problème majeur demeure les avantages apparents de convivialité et de confort qui découlent de l'utilisation de machines et d'appareils numériques pour la communication, les affaires, l'éducation, les soins de santé et ainsi de suite. Ces avantages apparents maintiennent l'attrait pour le réseau social tout en détournant l'attention de leurs effets socialement pernicieux.

Technosolutionnisme

Nous pouvons concevoir la commercialisation de l'apprentissage machine et de l'intelligence artificielle, sans oublier les données elles-mêmes, comme des technosolutions. Le technosolutionnisme[39] est souvent présenté comme un thème dans les partenariats public-privé dans lequel les entreprises technologiques font du lobbying auprès des gouvernements pour faire des affaires, et où les gouvernements adoptent des technologies pour montrer qu'ils « font quelque chose » pour s'attaquer aux problèmes sociaux et politiques. C'est peut-être cela qui explique pourquoi la Chambre de commerce de l'Ontario a intitulé ironiquement son rapport *In Data We Trust*[40], qui semble technosolutioniste, parce qu'elle veut clairement alerter les membres sur la nécessité de protéger la vie privée et de renforcer les lois relatives aux données.

Le technosolutionnisme a connu un élan remarquable après les événements du 11 septembre, alors que les sociétés technologiques en difficulté se faisaient concurrence pour obtenir des contrats gouvernementaux. Il a connu une impulsion encore plus grande pendant la pandémie mondiale de COVID-19. L'empressement dans la recherche de ces « solutions » a mené, dans de nombreux cas, à l'adoption de systèmes et de pratiques qui n'avaient pas été suffisamment testés, approuvés ou débattus démocratiquement. Divers enjeux comme les procédures démocratiques ou les droits de la personne sont donc mis de côté, surtout lorsqu'il est question de surveillance, bien souvent associée au pouvoir et au contrôle.

Cependant, le technosolutionnisme ne constitue pas le moyen approprié pour réaliser des progrès. Les activités des services de police et de sécurité et, maintenant, l'expérience de la pandémie nous laissent fortement croire que de telles interventions de surveillance précipitées et excessives pourraient tout simplement ne pas fonctionner comme on l'avait imaginé au départ. Nous ne savons pas du tout, par exemple, si l'application Alerte COVID de notification d'exposition Google/Apple, utilisée au Canada, a atteint l'un ou l'autre de ses objectifs vantés de réduction de la propagation du virus[41]. Bien entendu, le technosolutionnisme se manifeste dans de nombreux domaines autres que le traçage de contacts numériques et aussi dans de nombreux autres pays du monde[42].

La pandémie de COVID-19 a perpétué et rendu ces enjeux encore plus urgents. La croyance selon laquelle, lors d'une « crise » sociale et politique liée à la santé, les organismes publics devraient d'abord se tourner vers des remèdes technologiques, est très répandue. Tenant compte de l'empressement avec lequel de nombreuses innovations fondées sur les données ont été apportées, il est peu surprenant que beaucoup de ces enjeux aient été relégués au second plan. Au cours de la pandémie, certains groupes marginalisés ont non seulement été plus durement touchés mais, dans certains cas, leur situation a été aggravée par les « solutions » mises de l'avant.

Tri social

Le tri social est un aspect de la surveillance qui recoupe tous les volets et les thèmes de nos recherches. Comme le fait remarque Singh, citant le rapport du volet 3, « les dangers éthiques, discriminatoires et judiciaires du tri social sont au cœur de toutes ces affaires »[43]. Rappelons que le volet 3 concerne les questions de marketing en tant que mode de surveillance, par lequel la division classique des consommateurs en groupes au moyen d'une

"les lois sur la protection des renseignements personnels ne peuvent plus être considérées comme le seul moyen de faire face aux changements technologiques, alors que les pratiques en matière de données se multiplient. Il nous faut de nouveaux modèles de gouvernance des données, qui associent les problèmes techniques à des questions plus vastes, afin de mettre un frein aux inégalités générées par le tri social"

classification continue est à l'origine du mécanisme employé pour la publicité ciblée. Cette pratique est devenue beaucoup plus sophistiquée qu'à l'époque de la publication de l'ouvrage révolutionnaire d'Oscar Gandy, *The Panoptic Sort*[44], dans lequel il aborde le sujet de la création et de la perpétuation de l'inégalité.

En effet, nous constatons avec étonnement l'ampleur des changements qui se sont produits en moins d'une génération. Gandy traite des technologies de tri et d'inégalité envers les consommateurs, et aussi des transformations du capitalisme qui les accompagnent. Les quantités de données recueillies, traitées et distribuées sont devenues astronomiques, et elles sont maintenant utilisées non seulement par les entreprises, mais aussi par les organismes gouvernementaux et au profit de partenariats public-privé. Ce n'est pas tout, les appareils autonomes sont dotés d'une puissance sans précédent, basée sur l'intelligence artificielle avancée et l'apprentissage automatique. Chaque appareil améliore les fonctions de tri et de discrimination de la surveillance.

Ces progrès sur le plan du perfectionnement et de la puissance sont facilement observables dans d'autres domaines, bien souvent fondés sur des pratiques d'abord utilisées en marketing. Depuis les attentats du 11 septembre, une logique très similaire sous-tend les mesures de contrôle aux aéroports, lesquelles dépendent également de catégories codées pour trier les passagers. Si des données personnelles sont extraites, combinées et extrapolées pour créer des profils de consommateurs potentiels, une logique semblable permet de traiter des données pour repérer et isoler des groupes et des personnes dont le profil correspond à ceux de terroristes potentiels[45]. Comme le montre la recherche sur la surveillance des mégadonnées, de telles pratiques sont reproduites et intensifiées – par exemple, comme l'illustre Stéphane Leman-Langlois à l'aide des technologies neuronales – dans le domaine du renseignement de sécurité d'aujourd'hui[46].

Au-delà de cet aspect, les processus de tri sont également très présents dans la manière dont les caractéristiques du marketing et de la sécurité réapparaissent dans le domaine de la gouvernance. Les villes intelligentes, par exemple, sont présentées comme la tendance apparemment attrayante de la vie et de l'organisation urbaines de demain. Une fois de plus, nous sommes témoins des ambiguïtés de la surveillance contemporaine. Qui ne voudrait pas de villes plus écologiques avec des transports intelligents, un réseau Internet rapide et des bâtiments à température contrôlée? Pourtant, comme le note David Murakami Wood, cette même intelligence en fait une « société de surveillance omniprésente fondée sur les données »[47].

La notion même de consentement est éliminée dans un contexte où – comme pour le projet de ville intelligente avorté à Toronto, Sidewalk Labs – des capteurs et des caméras recueillent continuellement des données dans toutes les situations imaginables. Les inégalités et les injustices qui affligent actuellement les villes d'aujourd'hui sont reproduites dans un environnement dépendant des données, où les modes d'utilisation des données sont à peine remis en question. Ces pratiques sont des formes technologiquement renforcées de tri social, dans un milieu où la participation du public à la prise de décisions est réduite au minimum.

Cela signifie, entre autres, que les lois sur la protection des renseignements personnels ne peuvent plus être considérées comme le seul moyen de faire face aux changements technologiques, alors que les pratiques en matière de données se multiplient. Il nous faut de nouveaux modèles de gouvernance des données, qui associent les problèmes techniques à des questions plus vastes, afin de mettre un frein aux inégalités générées par le tri social. Il s'agira par le fait même de faire respecter nos droits en matière de données et la justice des données. Le capitalisme de surveillance, ou « capitalisme de plateforme » doit être soumis à des limites cohérentes afin que les préjudices liés à la vie privée et au désavantage social puissent être réglés. Les données sur les consommateurs peuvent en fait entraîner des prix plus élevés et des choix plus limités pour les Canadiens. L'objectif devrait être d'assurer le *bien-être des consommateurs* si nous voulons une concurrence véritablement loyale[48].

ET MAINTENANT?

Les problèmes persistants que nous avons identifiés comme des enjeux urgents, qui nécessitent une attention du public, sont *le déséquilibre informationnel*, *la surveillance croisée*, *les instruments inadéquats et les groupes exposés*. Ces derniers doivent être pris en compte dans le contexte des défis majeurs des partenariats *public-privé*, *du capitalisme de surveillance*, *du technosolutionnisme et du tri social*. Pour la recherche en cours, tous ces thèmes rendent toujours plus pressant le besoin d'enquêtes multidisciplinaires, mais aussi la nécessité d'élargir le champ de préoccupation et d'accroître considérablement la sensibilisation du public.

Nos recherches montrent, de manière frappante, que la croissance de la surveillance des mégadonnées – ainsi que l'analyse algorithmique, renforcée par l'intelligence artificielle et l'apprentissage automatique – touche tous les domaines de la vie, de l'ensemble de la population. Nous recommandons que ce fait soit reconnu et pris en compte, par l'entremise d'une grande collaboration avec des intervenants d'autres domaines – de la recherche, de l'éducation, des affaires et des différents paliers de gouvernement, des groupes de réglementation et de la société civile – de façon multisectorielle. De plus, certains domaines requièrent une attention prioritaire, compte tenu des réalités démographiques actuelles et de l'expansion rapide de l'analyse des données au Canada. Les domaines prioritaires sont l'âge, la géographie, la santé et la race[49].

ENFIN, VOICI TROIS DERNIÈRES RECOMMANDATIONS :

Protéger la vie privée et instaurer une justice des données

L'une des principales recommandations de ce projet est que la protection de la vie privée, aussi importante soit-elle, doit s'inscrire dans un ensemble beaucoup plus vaste d'exigences pour répondre adéquatement à l'intensification de la surveillance dans les sociétés numériques. La législation relative à la protection de la vie privée porte plus particulièrement sur les enjeux de manipulation inappropriée des données et de contrôle des renseignements personnels. Il s'agit principalement d'une situation qui s'opère entre des personnes et des organisations. Toutefois, la valeur sociale de la vie privée, en tant que droit de la personne, exige des protections plus vastes, qui s'étendent au-delà de la protection des données.

Comme le soulignent Lisa Austin et David Lie, en faisant référence au projet Sidewalk Labs, « la collecte de données réalisée dans des environnements intelligents ne correspond pas vraiment au modèle de partage intentionnel de renseignements personnels avec une organisation qui fournit un produit ou des services. Il s'agit plutôt d'une collecte opaque de renseignements qui peuvent ou non concerner des personnes et qui peuvent ou non être identifiables[50]. »

En dépit de cette « opacité » du traitement des données, certains préjudices de suridentification sont engendrés, dont plusieurs ont été abordés dans les pages précédentes. Les « effets dissuasifs », par exemple, étaient autrefois considérés comme trop vagues pour justifier des poursuites judiciaires. Toutefois, Jonathan Penney démontre comment la surveillance freine les recherches sur Internet. Les utilisateurs sont devenus plus prudents dans leur utilisation de certains mots potentiellement suspects, ce qui indique que la surveillance de la sécurité après les attentats du 11 septembre a eu des effets dissuasifs tangibles[51]. Cette situation ne relève pas des préoccupations connues en matière de « vie privée », mais elle n'en constitue pas moins un « préjudice » réel créé par la surveillance.

Aujourd'hui, nous devons prendre en considération d'autres préjudices, particulièrement dans les environnements intelligents où, par exemple, le comportement est modifié. Comme Mark Burdon et Tegan Cohen l'expliquent au sujet de Google Home, les préjudices comprennent « ... la capacité d'exploiter, de diriger et de fournir une "fréquence" aux flux de données de capteurs, pour en arriver à une modification continue du comportement et à façonner les normes sociales sur les objectifs et les avantages d'une telle modification »[52]. Il ne s'agit pas seulement de tri social, mais aussi de façonnement social. Ce que Shoshana Zuboff conçoit sur le plan individuel s'avère également un enjeu profondément *social et politique*.

Après avoir reconnu les préjudices de la surveillance sociale, nous devrions élaborer de nouvelles façons de formuler des mesures, notamment des « droits en matière de données » (ou « droits numériques »). Pour Bianca Wylie, il s'agit « d'un éventail de protections entourant l'accès à Internet, la protection de la vie privée, la transparence concernant la façon dont les données sont utilisées, le contrôle sur la façon dont les données sont utilisées, la participation démocratique aux décisions technologiques municipales et plus encore »[53]. Au-delà de ces protections, de façon plus générale, il y a la « justice des données » qui témoigne de la façon dont la surveillance rend visible, identifie, représente et traite des populations données de façon inégale, en raison, par exemple, de biais intégrés aux algorithmes[54].

Ces concepts doivent également être mobilisés dans plus d'un domaine, en établissant un lien entre les préoccupations relatives à la protection de la vie privée et la concurrence, par exemple, et en révisant *conjointement* les deux lois fédérales canadiennes sur la protection des renseignements personnels. Nous avons discuté de chacun de ces exemples dans les pages précédentes. De plus, des questions de propriété intellectuelle sont soulevées, ainsi que la nécessité d'élaborer des lignes directrices éthiques pour une science informatique appropriée.

Accroître la collaboration

Une deuxième recommandation est de renforcer la recherche collaborative dans ce domaine. Le programme de recherche sur la surveillance des mégadonnées a offert de nombreuses possibilités de collaboration accrue, tant à l'intérieur qu'à l'extérieur du Canada. Nous sommes heureux que le CRSH ait appuyé notre travail, au fil des ans, ainsi que celui d'autres collègues dans de nombreuses disciplines. La beauté de cette relation particulière réside dans le fait qu'elle exige que les chercheurs s'impliquent activement avec des *partenaires*. Dans notre cas, des chercheurs en sciences humaines et en sciences des données sont mis en relation avec des groupes de réglementation et de la société civile, plus particulièrement ceux qui se consacrent à la justice des données et aux droits en matière de données.

Lorsque les chercheurs ont l'occasion de *collaborer* avec d'autres personnes qui abordent les mêmes enjeux sous un angle différent, celui du *praticien*, les avantages sont réciproques. Nos partenaires peuvent profiter de la recherche dont ils ont besoin, alors qu'ils n'ont ni le temps ni le budget pour la mener, et les chercheurs ont accès aux personnes directement concernées et dont le quotidien est touché par les enjeux sur lesquels porte la recherche. Pour nous tous, il s'agissait d'une occasion unique, en près de deux décennies de recherche sur les questions de surveillance et de protection de la vie privée au Canada.

Toutefois, de telles occasions ne doivent pas être tenues pour acquises. Le présent rapport recommande également que ces partenariats multidisciplinaires et collaboratifs soient maintenus, mais également élargis. Cet aspect devrait être fondamental, plus particulièrement dans les domaines liés à notre société numérique, pour laquelle les études de surveillance sont essentielles. La rapidité, l'ubiquité et la conséquentialité des changements dans ce secteur sont si énormes et universelles qu'il faut davantage de partenariats de recherche continus et élargis comme celui dont ce projet bénéficie depuis 2015.

Sensibiliser le public et la population

Enfin, la troisième et dernière recommandation est que les questions abordées ici dans un format universitaire et axé sur les politiques soient vulgarisées de toute urgence à l'aide d'outils en ligne et discutées dans le cadre de pratiques d'apprentissage en personne traditionnelles. Ces résultats de recherche ne sont pas destinés à des intérêts purement universitaires, ni même uniquement au bénéfice de nos partenaires. Ces résultats doivent permettre d'informer la société canadienne à de nombreux niveaux. Il nous faut des moyens de diffusion créatifs, réalisés avec différents types de partenaires, allant au-delà de ceux avec qui nous travaillons déjà.

"La surveillance est aujourd'hui un enjeu public majeur, qui exige une attention à plusieurs niveaux. La protection de la vie privée demeure importante, mais la surveillance d'aujourd'hui met de l'avant le besoin d'une attention sérieuse portée aux nouveaux préjudices qu'elle cause et aux nouvelles dimensions de la vie sociale dans lesquelles elle est impliquée. Puisqu'elle rend visible, en identifiant, en représentant et en traitant les gens de nouvelles manières, elle rend nécessaires les droits en matière de données, mais aussi la justice des données comme objectif. Enfin, les données en tant qu'infrastructure publique requièrent de nouvelles approches pour minimiser les préjudices, mais aussi pour permettre l'épanouissement humain à l'ère du numérique."

Par exemple, sur le plan de l'éducation du public, notre projet a également permis la réalisation des courts métrages de la série *Screening Surveillance*, qui illustrent les enjeux dans un format destiné aux jeunes. Ils sont disponibles sur YouTube et ont également été diffusés dans des festivals et dans des contextes éducatifs, avec des sous-titres, partout dans le monde.

Comme nous l'avons déjà mentionné, les utilisateurs informés et actifs sont essentiels à la santé d'Internet et du monde numérique en général. Les avantages sociaux et politiques du monde numérique ne seront pas pleinement réalisés sans des changements importants, notamment en ce qui concerne la sensibilisation, la connaissance et l'engagement de ses utilisateurs de tous âges et de toutes les régions du Canada.

CONCLUSION

L'heure est aux possibilités, alors que la pandémie s'essouffle tranquillement et que nous apprenons à composer avec cette réalité. Beaucoup en ont parlé en termes « apocalyptiques », en soulignant ses effets désastreux. Le mot « apocalypse », emprunté au grec, parle d'une catastrophe, mais fait aussi référence au dévoilement, à une exposition au grand jour. Or, la pandémie a dévoilé, justement, la croissance rapide des nouvelles formes de surveillance : axées sur les données, intelligentes et évoluant d'une manière qui dépasse largement les mesures de protection de la vie privée et des données, elles qui ont le devoir de veiller à ce que la surveillance ne soit utilisée qu'à des fins positives. La surveillance est aujourd'hui un enjeu public majeur, qui exige une attention à plusieurs niveaux. La protection de la vie privée demeure importante, mais la surveillance d'aujourd'hui met de l'avant le besoin d'une attention sérieuse portée aux *nouveaux préjudices* qu'elle cause et aux *nouvelles dimensions* de la vie sociale dans lesquelles elle est impliquée. Puisqu'elle rend visible, en identifiant, en représentant et en traitant les gens de nouvelles manières, elle rend nécessaires les droits en matière de données, mais aussi la justice des données comme objectif. Enfin, les données en tant qu'infrastructure publique requièrent de nouvelles approches pour minimiser les préjudices, mais aussi pour permettre l'épanouissement humain à l'ère du numérique.

Notes

1 La CBC a signalé que certaines recherches de la police n'étaient pas liées à des interventions en cours, laissant entendre que des enquêtes exploratoires étaient menées : https://www.cbc.ca/news/canada/toronto/covid-police-database-1.5745481

2 Swikar Oli. 2021. « Canada's public health agency admits it it it track it 33 million mobile devices during lockdown », *National Post*, 24 décembre, tiré de : https://nationalpost.com/news/canada/canadas-public-health-agency-admits-it-tracked-33-million-mobile-devices-during-lockdown/

3 David Lyon et David Murakami Wood (éd.) 2020. *Big Data Surveillance and Security Intelligence*, UBC Press.

4 Colin Bennett et David Lyon. 2019. édition spéciale sur « Data-Driven Elections » dans *Internet Policy Review* 8 (4).

5 Kirstie Ball et William Webster. 2020. édition spéciale sur « Big Data and Surveillance : Hype, Commercial Logics and New Intimate Spheres » *Big Data & Society* 7 (1).

6 Valerie Steeves et David Murakami Wood. 2021. édition spéciale sur « Smart Surveillance » dans *Surveillance & Society*, 19 (2).

7 Par exemple, Mark Andrejevic et Zala Volcic. 2021. « Pandemic lessons: Total surveillance and the post-trust society », *The Political Economy of Communication* 9 (1); Kirstie Ball. 2021. *Electronic Monitoring and Surveillance in the Workplace* (discussion sur certains développements liés à la COVID-19) European Union JRC Publications Repository; Stéphane Leman Langlois. 2022. cité dans Raphaël Pirro, « Données géographiques : la pertinence du programme L'ASPC remise en question », *Le Journal de Montréal*, 21 janvier; David Lyon. 2022. *Pandemic Surveillance*, Cambridge : Polity Press; David Murakami Wood, dans Yann Sweeney. 2020. « Tracking the debate on COVID-19 surveillance tools », *Nature Machine Intelligence*, vol. 2, no 301-304. Valerie Steeves, Val Michaelson et Robert Porter. 2021. « For teenagers, the internet helps during lockdowns, but it's no substitute for the outside world » *The Conversation*, 18 mai.

8 Sachil Singh, 2021. Big Data Surveillance: Collated Research Findings. Rapport sur la recherche sur la surveillance des mégadonnées, septembre à avril.

9 Voir Scott Thompson et David Lyon. 2021, « Pixies, Pop-out Intelligence and Sandbox Play », dans Lyon et Murakami Wood (éd.) *Big Data Surveillance and Security Intelligence: The Canadian Case*, UBC Press.

10 Voir Bennett et Lyon. 2019.

11 Valerie Steeves. 2020. « A Dialogic analysis of Barbie's "conversations" with children ». *Big Data & Society*, Janvier-Juin 1-12.

12 Steeves. 2020: 10.

13 Voir https://www.policingthepandemic.ca/

14 David Lyon. 2022. *Pandemic Surveillance*, chapitre 4.

15 *Blaxites* dans la série Screening Surveillance, tiré de : www.screeningsurveillance.ca.

16 Sachil Singh. 2021. Rapport de la recherche sur la surveillance des mégadonnées.

17 Kirstie Ball et William Webster. 2020. « Big Data and Surveillance: Hype, Commercial Logics and New Intimate Spheres », *Big Data & Society*, janvier-juin : 1-5.

18 Aron Darmody et Detlev Zwick. 2020. « Manipulate to empower: Hyper-relevance and the contradictions of marketing in the Age of Surveillance Capitalism ». *Big Data & Society*, janvier-juin : 1-12.

19 Craig Forcese. 2020. « Bill C-59 and the Judicialization of Intelligence Collection », dans Lyon et Murakami Wood (éd.) *Big Data Surveillance and Security Intelligence: The Canadian Case*, UBC Press.

20 Andrew Clement. 2020. « Limits to Secrecy: What Are the Communications Canada's Interception Canadians' Internet Communications », dans Lyon et Murakami Wood (éd.) *Big Data Surveillance and Security Intelligence: The Canadian Case*, UBC Press.

21 LAIPVP : Loi sur l'accès à l'information et la protection de la vie privée; LPRPS : Loi sur la protection des renseignements personnels sur la santé.

22 Teresa Scassa. 2020. « Interesting amendments to Ontario's health data and public sector privacy laws buried in omnibus bill ». 30 mars, tiré de : https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=323:interesting-amendments-to-ontarios-health-data-and-public-sector-privacy-laws-buried-in-omnibus-bill&Itemid=80.

23 Matt Bubbers. 2020. « What kind of data is my new car collecting about me? Nearly everything it can, apparently. » *The Globe and Mail*, 15 janvier, tiré de : https://www.theglobeandmail.com/drive/technology/article-what-kind-of-data-is-my-new-car-collecting-about-me-nearly-everything

24 Voir p. ex., Robert Pallitto. 2020. *Bargaining with the Machine: Surveillance, and the Social Contract*. Lawrence: UP of Kansas.

25 Comparution du Commissaire devant le comité ETHI, le 7 février 2022, tirée de : https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2022/parl_20220207/. Les chercheurs David Lyon et David Murakami Wood ont également témoigné devant le comité ETHI.

26 Les membres de l'équipe sur la surveillance des mégadonnées ont participé à l'élaboration de la Loi sur la mise en œuvre de la Charte du numérique (projet de loi C-11).

27 Andrew Clement et David Lyon. 2018. « Facebook: A mass media micro-surveillance monopoly », *The Globe and Mail*, 23 avril, tiré de : https://www.theglobeandmail.com/opinion/article-facebook-a-mass-media-micro-surveillance-monopoly/

28 Tim McSorley et Anne Guertin. 2020. « Confronting Big Data : Popular Resistance to Government Surveillance in Canada since 2001 », dans Lyon et Murakami Wood (éd.) *Big Data Surveillance and Security Intelligence: The Canadian Case*, UBC Press.

29 Lex Gill et Cara Zwibel. 2017. « Why does Canada spy on its own indigenous communities? » *Open Democracy*, 6 décembre.

30 Andrew Crosby et Jeff Monaghan. 2018. *Policing Indigenous Movements: Dissent and the Security State*, Black Point N.-É. : Fernwood.

31 Steven Hayle, Scot Wortley et Julian Tanner. 2016. « Race, street life, and policing : Implications for racial profiling ». *Revue canadienne de criminologie et de justice pénale*, 58 (3) : 322-353.

32 David Williams et Ronald Wyatt. 2015. « Racial bias in health care and health : challenges and opportunities ». *Jama*. 11 août, 314 (6) : 555-6.

33 Stephanie Austin, Sari Tudiver, Miga Chultem et Mireille Kantiebo. « Gender-based analysis, women's health surveillance and women's health indicators-working together to promote equity in health in Canada », *International Journal of Public Health*, 52 : S41-S48.

34 Kirstie Ball et Laureen Snider (éd.). 2013. *The Surveillance-Industrial Complex: A Political Economy of Surveillance*, Londres : Routledge.

35 David Lyon. 2018. « State and surveillance » *CIGI Online*, tiré de : https://www.cigionline.org/articles/state-and-surveillance/

36 Jim Balsillie. 2021. « Liberal privacy bill fails to curtail surveillance economy or protect Canadians. » *National Post*, 15 mars, tiré de : https://nationalpost.com/opinion/jim-balsillie-liberal-privacy-bill-fails-to-curtail-surveillance-economy-or-protect-canadians

37 Daniel Therrien, Rapport annuel du CPVP. 2021. Cité par Jim Bronskill, Canadian Press/CBC, décembre, tiré de : https://www.cbc.ca/news/politics/privacy-commissioner-report-daniel-therrien-1.6279665

38 *Derrière nos écrans de fumée [The social Dilemma]*, un documentaire de Netflix, 2020, tiré de : https://www.thesocialdilemma.com/

39 Evgeny Mozorov. 2014. *To Save Everything: Click Here*, New York : Affaires publiques.

40 Chambre de commerce de l'Ontario. 2020. *In Data We Trust*, tiré de : https://occ.ca/wp-content/uploads/OCC-DataReport.pdf

41 CBC. 2022. « Where did things go wrong with Canada's COVID Alert app? » 9 février, tiré de : https://www.cbc.ca/radio/costofliving/from-boycott-to-bust-we-talk-spotify-and-neil-young-and-take-a-look-at-covid-alert-app-1.6339708/where-did-things-go-wrong-with-canada-s-covid-alert-app-1.6342632

42 Voir p. ex., Rob Kitchin. 2020. « Civil liberties or public health or civil liberties and public health: Using surveillance technologies to tackle the spread of COVID-19 », *Space & Polity*, mai, tiré de : https://kitchin.org/wp-content/uploads/2021/01/SP-2020-civil-liberties-and-public-health.pdf

43 Voir Kirstie Ball et William Webster. 2018. « Workshop Report: New Lines of (In)Sight: Big Data Surveillance and the Analytically Driven Organization », tiré de : https://www.sscqueens.org/sites/sscqueens.org/files/bds-crisp_report_stream_two_2018_0.pdf, p.1.

44 Oscar Gandy. 1993. *The Panoptic Sort: A Political Economy of Personal Information*, New York : Oxford, 2021 (édition mise à jour du livre publié en 1993 par Westview Press).

45 David Lyon. 2006. « Airport screening, surveillance and social sorting: Canadian responses to 9/11 in context », *Revue canadienne de criminologie et de justice pénale*, 48 (3) : 397-411.

46 Stéphane Leman Langlois. 2020. « Big Data Against Terrorism » dans Lyon et Murakami Wood.

47 https://www.queensu.ca/research/features/smart-cities-city-future

48 Ana Qarr. 2022. « Canada must reform competition and privacy law together to protect consumers », *Policy Options/ Options Politique*, 28 février.

49 Voir le rapport sur la surveillance des mégadonnées de Sachil Singh, 2021.

50 Lisa Austin et David Lie. 2021. « Data trusts and the governance of smart environments: Lessons from the failure of Sidewalk Labs' Urban Data Trusts », *Surveillance & Society*, 19(2) : 255-261.

51 Jonathan Penney. 2021. « Understanding chilling effects » *Minnesota Law Review*, tiré de : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3855619/

52 Mark Burdon et Tegan Cohen. 2021. « Modulation harms and the Google Home » *Surveillance & Society*, 19 (2) : 154-167.

53 Bianca Wylie. 2019. « Why we need data rights : everything about us should not be for sale », *CIGI online*, 30 janvier, tiré de :https://www.cigionline.org/articles/why-we-need-data-rights-not-everything-about-us-should-be-sale/

54 Voir Linnet Taylor. 2017. « What is data justice? The case for connecting digital rights and freedoms globally », *Big Data & Society*, novembre 2017, tiré de : https://journals.sagepub.com/doi/10.1177/2053951717736335 et Lina Dencik, Arne Hintz, Joanna Redden et Emiliano Treré. 2019. « Exploring data justice : Conceptions, applications and directions », *Information, Communication & Society*, mai, tiré de : https://www.tandfonline.com/doi/full/10.1080/1369118X.2019.1606268 La revendication d'une justice des données soulève également des questions à savoir quelles configurations sociopolitiques pour la propriété et le contrôle des systèmes de surveillance à forte intensité de données sont compatibles avec la politique démocratique et la protection des droits civiques et humains.

The
Office of the Privacy
Commissioner of Canada