# Les risques intersectionnels en matière de vie privée liés à l'échange de données entre les forces de l'ordre et les collectivités locales

Un projet de Nord Ouvert

Financé par le programme de contributions du Commissariat à la protection de la vie privée 2022/23

NORD OUVERT

# REMERCIEMENTS

## Vous pouvez citer ce rapport comme

Nord Ouvert. 2023. "Les risques intersectionnels en matière de vie privée liés à l'échange de données entre les forces de l'ordre et les collectivités locales." Nord Ouvert

## Avis de non-responsabilité

Si vous créez une adaptation de cette œuvre, veuillez ajouter l'avis de non-responsabilité suivant avec l'attribution : *Ceci est une adaptation d'une œuvre originale de Nord Ouvert. Les points de vue et opinions exprimés dans l'adaptation relèvent de la seule responsabilité de l'auteur et l'adaptation n'est pas approuvée par Nord Ouvert.*

## Attribution



## Auteurs

Thomas Linder, Merlin Chatwin

## Collaborateurs

Ce projet a été rendu possible grâce au généreux financement accordé par le Programme des contributions du Commissariat à la protection de la vie privée. Nous tenons à remercier le CPVP pour son travail continu de défense et de promotion de la protection de la vie privée au Canada, et pour le soutien qu'il apporte à ce projet et à bien d'autres du même genre.

Ce projet n'aurait pas non plus été possible sans le vaste réseau d'amis et de collaborateurs de Nord Ouvert, qui ont souvent pris le temps, dans leur emploi du temps chargé, de fournir des conseils et des commentaires. Il s'agit, sans ordre particulier, de Brenda McPhail, Renee Sieber, Teresa Scassa, Vivek Krishnamurthy, Christopher Parsons, Cristiano Therrien, Jonathan Obar, Bianca Wylie, Daniel Konikof, Alex Luscombe, Ushnish Sengupta, Alok Mukherjee, Meghan McDermott, Katrina Ingram, Nabeel Ahmed, Jamie Duncan, Jagtaran Singh, Kevin Webb, Pierre-Antoine Ferron et Ana Qarri.

Nous remercions également tous les individus interrogés au sein des collectivités locales et des services de police d'un bout à l'autre du pays. Ces personnes ont pris le temps de nous parler et de contribuer à une meilleure compréhension de la manière dont le partage des données est administré au Canada.

La collaboration est le fondement de l'élimination des silos, de la conception de meilleurs systèmes et de l'édification d'une société meilleure. Nous nous réjouissons de participer à l'avancement de ce travail !

# TABLE DES MATIÈRES

# RÉSUMÉ

De plus en plus, il devient évident que si les villes peuvent bénéficier de la collecte détaillée de données, d'analyses algorithmiques, d'outils basés sur des plateformes ou encore des systèmes en réseau, les risques inhérents à ces techniques nécessitent de mettre davantage l'accent sur les politiques de gouvernance. Parallèlement, une série de scandales publics a révélé la mesure dans laquelle les forces de l'ordre ont également adopté les technologies fondées sur les données, mais souvent dans le secret et en violation des normes de protection de la vie privée, voire des lois. À mesure que la transformation numérique des systèmes sociétaux se poursuit, ces dynamiques se jouent de plus en plus au sein de la même infrastructure numérique et du même écosystème de données - et peuvent avoir une incidence sur le droit à la vie privée des résidents. En outre, les récents développements des systèmes dits de « big data » et d'« intelligence artificielle » ont remis en question la pertinence du droit existant en matière de protection de la vie privée. Ce débat s'est invité dans le discours public et a contribué à une baisse continue de la confiance dans l'utilisation des données et des technologies numériques par les gouvernements. Ce rapport explore la question du partage des données entre les forces de l'ordre et les organismes municipaux, ainsi que les risques intersectionnels que ce partage fait peser sur les communautés déjà confrontées à des préjudices systémiques. Sur la base d'entretiens avec 27 décideurs des forces de l'ordre et des autorités municipales, ainsi que de deux ateliers d'experts, nous soulignons l'ambiguïté qui existe autour du partage des données, l'hétérogénéité des pratiques de gouvernance existantes, et exposons les appels à la réforme. Sur cette base, nous recommandons la création d'un groupe de travail composé d'experts de la société civile, de représentants des forces de l'ordre et d'employés municipaux responsables afin d'élaborer des propositions politiques pour résoudre ce problème.

# INTRODUCTION

Ces dernières années, le discours canadien sur la gouvernance de l'utilisation publique des données et des technologies numériques dans les villes a connu des évolutions simultanées mais inutilement décorrélées. Il est de plus en plus évident que si les villes peuvent tirer d'immenses avantages d'une collecte de données plus granulaires, d'analyses algorithmiques, d'outils basés sur des plateformes ou encore des systèmes en réseau, il est nécessaire de mettre davantage l'accent sur une politique de gouvernance préemptive. Alors que le projet de « ville intelligente » de Sidewalk Labs s'est effondré en 2020, en partie sous le poids de la critique soutenue de ses politiques de gouvernance des données (Artyushina, 2020), le Défi des villes intelligentes a souligné l'importance des valeurs et des principes de gouvernance ouverte et responsable (Valverde et Flynn, 2020). Par la suite, les villes de Toronto et de Montréal ont publié des cadres décrivant leurs principes directeurs pour l'utilisation éthique et responsable des données et des technologies émergentes et travaillent actuellement à l'opérationnalisation de ces cadres. Cependant, dans le même temps, une série de scandales publics a révélé la mesure dans laquelle les forces de l'ordre ont également adopté les technologies axées sur les données, mais souvent dans le secret et en violation des normes de protection de la vie privée, voire des lois. Le scandale le plus récent, lié à l'utilisation de l'outil de reconnaissance faciale Clearview, a incité le service de police de Toronto à élaborer une politique de gouvernance de l'intelligence artificielle (Brandusescu et al., 2021).

Au Canada, la relation entre les services de police et les municipalités fait l'objet d'un différend de longue date. De nombreux services de police, comme celui de Toronto, sont financés par la municipalité mais ne sont pas dirigés par elle, et relèvent plutôt d'une entité distincte, la commission des services policiers, théoriquement civile. Cette situation a engendré des tensions autour des questions de financement et un manque de contrôle démocratique et de compréhension de ce que ces fonds permettent de financer. En outre, il existe des désaccords permanents sur ce que les commissions ont le pouvoir de gouverner et sur ce qui reste du ressort « opérationnel » des services de police eux-mêmes (Roach, 2022). Ces débats sur la responsabilité et la gouvernance montrent clairement qu'au moins en ce qui concerne l'écosystème des données et des technologies numériques de la société, qui connaît une croissance rapide, les villes et les services de police sont profondément imbriqués (Artyushina et Wernick, 2021 ; Lorinc, 2021). Non seulement ces entités sont confrontées à des problèmes de réglementation similaires, mais leurs systèmes de données et de technologie s'intègrent rapidement les uns aux autres : bases de données communes, accès à la télévision en circuit fermé (vidéosurveillance), projets de partage de données, outils d'analyse similaires, le tout fonctionnant au sein de l'infrastructure numérique des villes et contribuant à cette dernière (Linder, 2021). Les risques

Ces débats sur la responsabilité et la gouvernance montrent clairement qu’au moins en ce qui concerne l’écosystème des données et des technologies numériques de la société, qui connaît une croissance rapide, les villes et les services de police sont profondément imbriqués.

que ces technologies peuvent présenter, en particulier pour les communautés marginalisées, sont également devenus inévitablement évidents : les données biaisées, les violations de la vie privée, l'acquisition et l'utilisation secrètes de nouvelles technologies, le partage non éthique des données, les cas d'utilisation illégitimes et les algorithmes discriminatoires ont tous contribué à une baisse de la confiance du public dans l'utilisation des données et des technologies par les services gouvernementaux (Bannerman et Orasch, 2019).

Ce projet répond à une pénurie de recherche sur cet écosystème de données entremêlées et ce domaine de gouvernance cloisonné. Grâce à 27 entrevues avec des praticiens des forces de l'ordre et des autorités locales, ainsi qu'à deux ateliers d'experts, nous avons mis en lumière l'état du partage des données et de la gouvernance entre les forces de l'ordre et les autorités municipales. Ce rapport documente ce que l'on sait de ce type de partage de données, de l'état de leur gouvernance et des types de cadres d'évaluation des risques d'atteinte à la vie privée qui sont en place. Notre objectif est de catalyser une conversation plus approfondie sur la manière de gouverner ouvertement, démocratiquement et responsablement cette intersection ainsi que de protéger les résidents confrontés à des risques intersectionnels liés à des préjugés systémiques profondément ancrés.

## Contexte

La transformation numérique de la société canadienne et de son gouvernement est en marche depuis plus d'une décennie, motivée par la promesse d'une meilleure connaissance de la dynamique, des besoins et des obstacles des résidents, ainsi que par la capacité d'agir sur la base de ces connaissances. Ces projets touchent un large éventail de questions sociétales, de la logistique de la gestion des transports publics aux interventions d'urgence, en passant par la sensibilisation à l'environnement, la prestation de services sociaux ou la sécurité publique - et nombre de ces questions concernent à la fois les services en charge de faire appliquer de la loi ainsi que d'autres services municipaux. De cette imbrication sont nés des projets de transformation numérique tels que le Saskatchewan Hub Model, conçu pour mieux recueillir, évaluer et trier les besoins en services sociaux à haut risque grâce à une centralisation des données et des prestataires de services (S. P. Canada, 2018). De même, le lancement des plans de sécurité et de bien-être communautaires promet spécifiquement une « feuille de route sur la façon dont la ville et les systèmes sociaux qui servent les Torontois, tels que les services communautaires, les systèmes de soins de santé, les systèmes éducatifs, les systèmes judiciaires, la police et les entreprises, peuvent travailler en collaboration à travers les différents secteurs et les gouvernements pour soutenir la sécurité et le bien-être de la communauté » (Toronto, 2021). Malgré ces nobles intentions, la réalité est souvent celle de services encore silencieux, d'une gouvernance fragmentée et disparate, et de processus et d'outils d'évaluation des risques inadéquats.

Nord Ouvert est à la pointe de l'ouverture et du partage des données pour le bien commun, et de la technologie qui permet ce partage, depuis 2011. Pour nous, la recherche du bien commun signifie que nous dépassons les considérations à court terme et les intérêts individuels ou organisationnels pour développer des communautés saines, justes et durables avec des processus démocratiques forts. Grâce à notre travail sur la gouvernance des données et la transformation numérique, nous avons observé que les forces de l'ordre municipales, provinciales et fédérales sont en marge des meilleures pratiques conçues pour protéger la vie privée, la sécurité et le bien-être général des résidents. Par exemple, dans le cadre de notre participation au forum multipartite sur le gouvernement ouvert avec le gouvernement fédéral, nous avons observé que les engagements du gouvernement ouvert pour l'ouverture et le partage des données ne prenaient pas en compte les organismes chargés de faire appliquer la loi. De même, le projet de loi C-27 sur la protection de la vie privée et l'intelligence artificielle, récemment déposé, exempte spécifiquement les forces de l'ordre et les services de sécurité de la réglementation, et l'engagement du Programme *Partenariat pour un gouvernement ouvert* de l'Ontario, sur le thème de l'intelligence artificielle fiable, n'inclut pas la police provinciale de l'Ontario. Au niveau municipal, la ville de Toronto a élaboré un cadre stratégique pour l'infrastructure numérique qui couvre tous les aspects de l'utilisation des données et de la technologie numérique par la ville - mais elle n'a même pas été en mesure d'y mentionner le service de police de Toronto en raison de sa différenciation institutionnelle légale, même si, d'un point de vue technologique, les deux sont profondément connectés, sont responsables auprès des mêmes résidents et se voient accorder les mêmes droits et libertés.

## Énoncé du problème

Si l'intégration et la numérisation accrues des services sociaux par le biais d'outils numériques de collecte, d'analyse, de diffusion et de prise de décision promettent de nombreux avantages, le paysage des risques continue de changer radicalement. La quantité de données collectées, leur granularité, la grande variété de sources dont elle sont issues et la multiplicités des points de contacts dans la vie des individus, signifient que les protections existantes en matière de vie privée ne sont pas suffisantes - en particulier dans le cas de groupes déjà marginalisés et victimes de discriminations.  En raison du racisme, du sexisme, du classisme et de l'homophobie systémiques, ces groupes sont plus exposés que d'autres et, comme l'ont montré de nombreuses études (Palmater, 2016 ; Wortley et Owusu-Bempah, 2011, 2022), sont également plus menacés par certaines institutions gouvernementales, comme la police, que d'autres.

Il en résulte un contexte complexe de menaces différentielles posées par la production et l'utilisation de données qui ne sont pas suffisamment reflétées dans la compréhension institutionnelle de la situation ainsi que dans les cadres de gouvernance et les documents politiques disponibles. En outre, la question spécifique

du partage des données avec les forces de l'ordre est opaque et ne fait l'objet d'aucune surveillance publique. Ce rapport vise à éclairer cet aspect particulier de la transformation numérique gouvernementale et à interroger les principaux décideurs au sein des villes et des forces de l'ordre :

1. Que savent-il de l'état actuel du partage des données ;
2. Comment le partage des données est-il encadré ;
3. Quels sont les cadres d'évaluation des risques qui sont en place ;
4. Des changements de gouvernance sont-ils nécessaires aujourd'hui ou à l'avenir.

Avec ces informations, nous cherchons à susciter une conversation plus approfondie sur la manière dont les institutions peuvent permettre un partage des données qui soutienne une prestation de services efficace, tout en évitant les préjudices. À cette fin, nous recommandons la création d'un groupe de travail réunissant des experts du monde universitaire, des organisations de défense des libertés civiles, des municipalités et des organismes chargés de faire appliquer la loi, afin d'examiner les résultats, d'identifier des alternatives innovantes et d'établir des pistes d'action pour l'avenir.

Ce rapport décrit d'abord notre méthodologie, puis donne un aperçu détaillé de la littérature pertinente sur la vie privée et l'intersectionnalité, la transformation numérique des villes, la transformation numérique des forces de l'ordre et la façon dont la littérature sur la gouvernance des données peut servir de cadre d'analyse pour ces problématiques. Il présente ensuite un aperçu des résultats empiriques et de l'analyse des données, et conclut en proposant des pistes pour l'avenir.

# MÉTHODOLOGIE

Étant donné la quasi-absence de recherches sur les pratiques en matière d'échange de données entre les agences gouvernementales et les forces de l'ordre, ce projet était nécessairement exploratoire. Afin de tenir compte, sur le plan méthodologique, de la nature exploratoire de ce processus, nous nous sommes concentrés sur les entretiens semi-structurés en tant que méthode principale pour offrir la plus grande souplesse d'échantillonnage. Cependant, il est notoirement difficile d'obtenir des entretiens avec les forces de l'ordre (Monaghan, 2017), en particulier sur des sujets potentiellement sensibles tels que la protection de la vie privée et le partage des données. En utilisant une approche d'échantillonnage en boule de neige pour développer le plus vaste échantillon possible, nous espérions rassembler suffisamment de participants pour atteindre nos objectifs. À la fin de la phase de collecte des données, nous avions mené des entretiens avec 27 personnes dans cinq services de police municipaux ou régionaux et dix administrations municipales ou régionales. Presque tous les entretiens ont duré entre 30 et 45 minutes et ont suivi un guide d'entretien semi-structuré. Les notes et les enregistrements, lorsque le consentement à l'enregistrement a été donné, ont été cryptés et protégés par un mot de passe.

En raison de la résistance du personnel municipal et des forces de l'ordre à participer aux entretiens ainsi que de la nature opaque des réponses données par ceux qui y ont participé, notre analyse des données s'est concentrée sur ce qui n'était pas dit autant que sur ce qui était dit. Afin d'identifier rigoureusement les thèmes et les modèles, nous avons utilisé des méthodes qualitatives courantes d'analyse de contenu (Anderson, 2007 ; Roller, 2019) pour les données des entretiens, en identifiant les points clés et les arguments en conjonction avec le cadre d'analyse de la littérature.

Après analyse, nous avons formulé un certain nombre d'hypothèses préliminaires sur les raisons pour lesquelles les détails de la gouvernance des données et des cadres éthiques ne se dégageaient pas des données des entretiens et nous avons ajouté deux ateliers d'experts aux méthodes de recherche. Brenda McPhail, Renee Sieber, Merlin Chatwin, Teresa Scassa, Vivek Krishnamurthy, Christopher Parsons, Cristiano Therrien, Jonathan Obar, Bianca Wylie, Daniel Konikof, Alex Luscombe, Ushnish Sengupta, Alok Mukherjee, Meghan McDermott et Jamie Duncan, Akwasi Owusu-Bempah, Jagtaran Singh, Michael Kempa et Kent Roach ont été invités à participer à ces ateliers d'experts. Ces ateliers ont fourni une analyse approfondie et une évaluation contextuelle cruciale de nos résultats, validant nos énoncés de problèmes et soulignant la nécessité de poursuivre sérieusement les travaux sur l'innovation et l'amélioration de la gouvernance en matière de partage des données. Les résultats de ces ateliers sont résumés dans la deuxième section du chapitre présentant les analyses.

## Limites

Alors que nous savions dès le départ qu'il était peu probable d'obtenir un taux de réponse suffisamment représentatif sur le plan géographique, nous avons été surpris par le niveau de résistance face à nos demandes de renseignements et de participation aux entretiens. Si nous avons pu mener des entretiens avec des membres du personnel de cinq agences de forces de l'ordre différentes, beaucoup d'autres nous ont opposé un refus ou se sont rétractés avant que l'entretien n'ait pu avoir lieu. Le taux de refus était également élevé dans les villes, mais dans une moindre mesure. Le taux de non-réponse parmi les forces de l'ordre était d'environ 75 %, alors qu'il était d'environ un tiers parmi les contacts municipaux. En tant que tels, nos résultats ne peuvent être considérés que comme une confirmation de l'existence du problème, et non comme une indication de la représentativité des cas à travers l'ensemble du Canada. Bien que ce manque de coopération et de transparence soit une limite, il constitue également une preuve flagrante de l'insuffisance du travail en matière de gouvernance publique, responsable et démocratique des données, à l'intersection des forces de l'ordre et des municipalités au Canada.

# REVUE DE LITTÉRATURE

## Vie privée, intersectionnalité et transformation numérique

Le droit de la protection de la vie privée au Canada est bien expliqué par de nombreuses ressources (Bannerman et Orasch, 2019 ; Canada, Ministère de la Justice, 2019 ; CPVP, 2014 ; Grieman, 2019 ; Robertson, Khoo et Song, 2020) et il n'est pas nécessaire que nous nous y attardions ici. L'élément central de ce rapport est que le droit canadien à la protection de la vie privée fait l'objet de critiques constantes pour n'avoir pas su s'adapter aux changements massifs du paysage numérique. Teresa Scassa, entre autres, a écrit que « l'évolution rapide du paysage numérique et des données a exercé une pression croissante sur les cadres de protection des données existants au Canada » et que « tandis que la loi sur la protection des données stagne, la collecte de données continue d'augmenter en volume et en variété » (Scassa, 2020a, p. 173). Le présent rapport n'a pas pour but de critiquer davantage la réglementation canadienne en matière de protection de la vie privée, et encore moins de suggérer des pistes pour l'avenir. La présente section vise plutôt à établir la façon dont la protection de la vie privée et les risques qui y sont associés sont actuellement envisagés en ce qui concerne l'échange de données entre les organismes gouvernementaux locaux et les organismes en charge de faire appliquer la loi, en donnant un aperçu des principaux sujets de préoccupation qui s'inscrivent dans la littérature.

Outre les critiques générales selon lesquelles le droit canadien de la protection de la vie privée n'est plus adapté à l'économie numérique à l'ère du « big data » et de l'« IA », des préoccupations plus spécifiques ont été exprimées concernant l'accent ontologique mis sur la protection de la vie privée des individus. Comme cela a été largement soutenu (Bannerman et Orasch, 2019 ; Scassa, 2020a), le droit à la vie privée au Canada (ainsi que dans d'autres pays de l'Organisation de coopération et de développement économiques) adopte une approche ontologiquement individualiste en accordant une protection à un type de données très spécifique, connu sous le nom de renseignements personnels, en vertu d'un ensemble de lois qui s'appliquent à différents secteurs. La loi sur la protection de la vie privée (Loi sur la protection des renseignements personnels et les documents électroniques, LPRPDE) couvre la collecte, l'utilisation et la divulgation des renseignements personnels par le gouvernement du Canada ; la LPRPDE, à quelques exceptions près, couvre le secteur des entreprises privées (avec des lois essentiellement similaires en vigueur en Colombie-Britannique, en Alberta et au Québec) ; et les provinces ont leurs propres lois sur la protection de la vie privée dans le secteur public (Commissariat à la protection de la vie privée, 2008). La définition des renseignements personnels diffère légèrement d'une loi à l'autre, mais en général, on peut dire qu'elle couvre (Commissariat à la protection de la vie privée, 2014) :

- la race, l'origine nationale ou ethnique,
- la religion,
- l'âge, l'état civil,
- les antécédents médicaux, éducatifs ou professionnels,
- des informations financières,
- l'ADN,
- les numéros d'identification tels que votre numéro d'assurance sociale ou votre permis de conduire, et
- des points de vue ou des opinions sur vous en tant qu'employé.

Ce qui n'est pas considéré comme des renseignements personnels peut inclure :

- Les renseignements qui ne concernent pas un individu, parce que le lien avec une personne est trop faible ou trop éloigné (par exemple, un code postal seul qui couvre une vaste zone avec de nombreux foyers) ;
- Les renseignements sur une organisation telle qu'une entreprise ;
- Les renseignements rendus anonymes, tant qu'il n'est pas possible de relier ces données à une personne identifiable ;
- Certains renseignements sur les fonctionnaires, tels que leur nom, leur poste et leur titre ; et
- Les coordonnées professionnelles d'une personne qu'une organisation recueille, utilise ou divulgue dans le seul but de communiquer avec cette personne dans le cadre de son emploi, de son entreprise ou de sa profession.

En d'autres termes, la législation sur la protection de la vie privée protège les données qui se rapportent directement à un individu. Dans le contexte de l'échange de données entre les autorités locales et les forces de l'ordre, les renseignements personnels sont définis par la législation provinciale sur la protection de la vie privée (par exemple, en Ontario, la loi sur l'accès à l'information et la protection de la vie privée, LAIPVP, et la loi sur l'accès à l'information municipale et la protection de la vie privée, LAIMPVP) et cette législation constitue la base de la détermination des risques pour la vie privée effectuée dans le cadre d'une évaluation des facteurs relatifs à la vie privée (EFVP). Les évaluations des facteurs relatifs à la vie privée sont devenues l'outil et la procédure standard permettant d'évaluer le risque potentiel pour la vie privée posé par une nouvelle technologie numérique ou un nouveau système de collecte et d'analyse de données.

Toutefois, cette approche de la protection de la vie privée fondée sur les informations nominatives fait l'objet de critiques constantes. Les spécialistes des technologies de l'informatique ont montré qu'à l'ère du big data, les principales techniques d'atténuation telles que l'anonymisation ou la dépersonnalisation des données (c'est-à-dire l'élimination des renseignements personnels des données ou, par d'autres processus informatiques, l'élimination des renseignements personnels) peuvent facilement être annulées par la corrélation de plusieurs ensembles de données (Bradbury, s.d. ; Lomas, 2019 ; Rocher, Hendrickx, et de Montjoye, 2019). Cela porte gravement atteinte à une garantie essentielle de la législation canadienne en matière de protection de la vie privée (Ladak, Ladak et Ladak, 2021 ;

Rosner, 2019). Cela a conduit à de nouveaux appels à la mise en œuvre de techniques dites de protection de la vie privée dès la conception, même si l'on ne sait pas très bien dans quelle mesure ces techniques sont réellement adoptées et non pas simplement défendues pour la forme.

Outre le caractère insuffisant de cette technique d'atténuation fondamentale, les EFVP dans leur ensemble ont été critiquées. Scassa (2020a, p. 182) note que « le commissaire de la Colombie-Britannique était préoccupé par le fait qu'une EFVP qui n'évalue que la conformité technique ne tient pas compte des risques plus vastes que les initiatives peuvent soulever pour la vie privée des personnes dont la vie et les renseignements personnels sont touchés » (CPVP, 2004, p. 26). L'évaluation la plus récente de l'état de l'application des EFVP remonte maintenant à dix ans, mais les auteurs (R. M. Bayley et Bennett, 2012, p. 184) notaient alors qu'en ce qui concerne la mise en œuvre, « les EFVP canadiennes ne sont pas non plus à la hauteur. On ne sait pas dans quelle mesure les EFVP sont réexaminées et révisées et dans quelle proportion les mesures d'atténuation promises sont appliquées. Cependant, les régulateurs de la vie privée ont des raisons de croire que les plans d'EFVP ne sont pas toujours mis en œuvre ».

Au-delà de la technique centrée sur les renseignements personnels, et en particulier à la lumière de l'émergence des technologies de « big data » et d'« intelligence artificielle », les experts en technologie[1] soutiennent de plus en plus qu'une telle ontologie individualiste est insuffisante pour couvrir tous les risques liés à la vie privée (Barocas et Nissenbaum, 2014 ; Bennett et Bayley, 2016 ; Taylor, Floridi, et Van der Sloot, 2016). Comme le soulignent Taylor et al. (2016, p. 10), « les concepts d'anonymisation, de protection de l'identité individuelle et de sauvegarde des informations personnelles font l'objet d'une grande attention. Cependant, à l'ère du big data, où les analyses sont développées pour fonctionner à l'échelle la plus large possible, l'individu est souvent accessoire dans l'analyse. Les technologies d'analyse des données sont plutôt orientées vers le niveau du groupe ». En d'autres termes, si les renseignements ne sont pas protégés par l'une des lois (c'est-à-dire qu'ils ne sont pas reconnus comme des « renseignements personnels »), les obligations de confidentialité ou d'atténuation prévues par la loi ne s'appliquent pas. La question de savoir si les données peuvent être divulguées en vertu de la loi à l'insu ou sans le consentement du consommateur, et si la police a besoin d'un mandat ou d'une ordonnance de production pour les obtenir, dépend en grande partie de la nature des données collectées. Les données qui ne sont pas identifiantes, qui ne permettent pas de localiser une personne ou son appareil et qui ne concernent pas une personne en particulier peuvent ne pas être suffisamment privées pour bénéficier des protections de la LPRPDE ou de l'article 8 de la Charte canadienne. Pourtant, ces données présentent également des risques importants pour les libertés que le droit à la vie privée est censée protéger : « Les droits à la vie privée sont de plus en plus considérés comme ayant des dimensions collectives et pas seulement individuelles » (Scassa, 2020a, p. 175).

(1) La justification de l'utilisation des guillemets sera examinée dans les sections suivantes

La raison d'être de la protection de la vie privée des individus n'était pas seulement de protéger le caractère sacré de leurs renseignements personnels en soi, mais plus fondamentalement de garantir « l'autonomie, la dignité humaine, la liberté personnelle ou les intérêts liés au développement personnel et à l'identité » (Taylor et al., 2016, p. 14). Le Haut-Commissariat des Nations unies aux droits de l'homme (2011, p. 5) a défini la vie privée comme la « présomption que les individus devraient disposer d'un espace de développement autonome, d'interaction et de liberté » ; cette liberté est souvent considérée comme le fondement d'autres droits, car, comme l'écrit Privacy International, elle « nous donne un espace pour être nous-mêmes sans jugement, nous permet de penser librement sans discrimination et constitue un élément important pour nous permettre de contrôler qui sait quoi à notre sujet » (Privacy International, 2017). Cependant, comme l'écrivent Barocas et Nissenbaum (p.45), « les applications courantes du big data sapent les valeurs que l'anonymat protégeait traditionnellement » et « même lorsque les individus ne sont pas "identifiables", ils peuvent toujours être "accessibles" ».

Les technologies liées au big data permettent d'analyser des ensembles de données tellement vastes et englobant - par exemple, toutes les données de localisation des téléphones portables dans une ville - que l'autonomie, la liberté et les intérêts des personnes pourraient bien être bafoués sans que l'on comprenne qui elles sont exactement. Taylor et al. (p. 15) écrivent que « les politiques et les décisions sont prises sur la base de profils et de modèles et, en tant que tels, affectent négativement ou positivement des groupes ou des catégories ». C'est sur cette base que des philosophes de la vie privée comme Nissenbaum, Taylor et Floridi ont conceptualisé l'idée de « vie privée de groupe » (Taylor et al., 2016) comme un moyen de positionner les groupes, même anonymisés, comme étant à risque de violations de la vie privée.

Ces dernières années, nous avons vu de nombreux exemples de la manière dont les technologies liées au big data et, plus récemment, à l'intelligence artificielle, ont discriminé des groupes de personnes (Barocas et Selbst, 2016). Dans la plupart des cas, il s'agissait de groupes déjà marginalisés, comme dans le cas de technologies utilisées pour prendre des décisions en matière de protection sociale (Eubanks, 2018), d'immigration (Molnar et Gill, 2018), d'évaluation des risques de récidive (Mattu, s.d.), de publicité et de résultats de recherche en ligne (Noble, 2018), et - ce qui est le plus directement pertinent pour le présent rapport - dans le domaine du maintien de l'ordre. Des recherches approfondies ont désormais montré que les outils de « big data » ou d' « IA » tels que la police prédictive ou l'analyse des points chauds (Brayne, 2017 ; Linder, 2021 ; Richardson, Schultz et Crawford, 2019 ; Robertson et al., 2020 ; Tulumello et Iapaolo, 2022) utilisent les mêmes techniques d'identification et de concordance des motifs pour former des groupes de personnes, ou des zones où vivent des groupes de personnes, et les isoler en vue d'une action spécifique. Dans une évaluation approfondie de la situation au Canada, Robertson, Khoo et Song (2020) sont parvenus à la conclusion que ces technologies risquaient de violer les droits des Canadiens garantis par la

Ces dernières années, nous avons vu de nombreux exemples de la manière dont les technologies liées au big data et, plus récemment, à l’intelligence artificielle, ont discriminé des groupes de personnes.

Charte. En effet, s'agissant spécifiquement de la question du partage des données entre les forces de l'ordre et d'autres organismes gouvernementaux, ils citent le Conseil des droits de l'homme des Nations unies, selon lequel le partage des données entre les forces de l'ordre et d'autres organismes publics est susceptible de violer le droit à la vie privée « parce que les mesures de surveillance qui peuvent être nécessaires et proportionnées pour un objectif légitime peuvent ne pas l'être pour un autre objectif » (Conseil des droits de l'homme des Nations unies, 2014, p. 27).

Cependant, les réglementations en matière de protection de la vie privée sont encore à la traîne par rapport à cette prise de conscience. Comme l'écrivent Bennett et Raab, « En effet, cette compréhension n'est pas totalement absente chez les défenseurs et les régulateurs en matière de vie privée, bien que la mesure dans laquelle ils peuvent y adhérer soit limitée par la persistance du paradigme individualiste et axé sur les droits » ( 2018, p. 34). L'élaboration récente de politiques autour des technologies d'intelligence artificielle a commencé à introduire une réflexion plus large sur la vie privée collective ou de groupe. En 2022, le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique a publié un rapport sur les technologies de reconnaissance faciale qui rend compte des risques sociaux et collectifs que posent ces technologies pour les groupes. Les politiques en matière d'intelligence artificielle actuellement élaborées par le service de police de Toronto reconnaissent également que ces technologies peuvent être discriminatoires à l'égard de certains groupes. Dans ces développements, il est tacitement admis que les technologies de « big data » ou d'« IA » peuvent être discriminatoires sur le plan intersectionnel. En d'autres termes, elles ont historiquement une prédisposition à amplifier les préjugés existants fondés sur le genre, la race et la classe sociale.

La jonction entre l'intersectionnalité, le risque pour la vie privée et les technologies émergentes est un sujet extrêmement vaste qui a été abordé sous de nombreux angles (Benjamin, 2019 ; Crawford, 2021 ; Grzanka, 2018 ; Rambukkana, 2021). Les deux sections suivantes examinent spécifiquement la littérature relative à la transformation numérique des villes et au risque d'intersectionnalité, ainsi qu'à l'application de la loi.

## Transformation numérique des villes et risques

Les villes sont devenues des épicentres essentiels pour répondre aux risques systémiques dans l'ensemble de la société. De la pauvreté à la nutrition, de l'éducation au vieillissement, de l'inégalité des richesses à la discrimination, de la santé à la protection sociale, du changement technologique à la dégradation de l'environnement, ou des conflits à l'immigration, tous ces problèmes se croisent au sein des villes - et, par conséquent, on y retrouve également bon nombre des solutions proposées et mises en place. Le rôle central que jouent les villes a incité des

organismes mondiaux tels que l'ONU, la Banque mondiale ou l'Union européenne à investir des sommes considérables pour repenser la gouvernance des villes afin de relever ces défis. La transformation numérique des villes est l'un des domaines où les tensions se manifestent de la manière la plus spectaculaire. Les villes ont toujours été le lieu et le banc d'essai de projets politiques, et l'essor rapide de la technologie numérique et de ses promesses au cours des dernières décennies a donné lieu à une pléthore de théories, de discours, de projets, de mouvements et d'intérêts économiques et sociaux, qui rivalisent tous pour définir un nouveau paradigme basé sur la technologie pour soutenir la structure municipale (Lorinc, 2022 ; Mosco, 2019).

Ce discours urbain axé sur la technologie a souvent été appelé « ville intelligente », mais il est désormais largement reconnu que ce terme est une création des relations publiques du secteur privé et qu'il induit davantage en erreur qu'il ne clarifie - en particulier lorsqu'il s'agit de délimiter les risques intersectionnels posés (Green, 2019). Nous parlons plutôt de la transformation numérique des villes par l'adoption de technologies intelligentes, un concept qui permet une analyse davantage orientée vers les sciences sociales des effets structurels, sociaux, économiques et politiques qui ont résulté de l'utilisation et de la tentative d'utilisation des technologies numériques dans la gouvernance urbaine. Il existe une vaste littérature sur ce sujet, qui couvre tous les domaines, de l'économie politique à l'élaboration de politiques et aux sciences de l'environnement. Notre objectif dans cette section est de fournir un aperçu fondamental de la littérature sur la façon dont la collecte et l'utilisation des données se développent dans les villes ainsi que sur les risques intersectionnels qu'elles posent.

Avant même la notion de « villes intelligentes », la capacité technologique et informatique de collecter des quantités toujours plus importantes de données, de les stocker, de les partager et de les analyser, a donné naissance à une « vision remarquablement cohérente de la réforme de la gestion publique à l'ère numérique » (Clarke, 2020, p. 98). Selon Clarke, cette vision a donné naissance à une dynamique d'auto-propulsion dans laquelle « lorsque les services et les espaces publics sont numérisés, ils produisent et sont donc façonnés par de vastes quantités de données » (105). Les données ont commencé à acquérir une importance, une valeur et une fonction au sein de la gouvernance municipale qui étaient qualitativement et quantitativement différentes par comparaison avec la collecte et l'utilisation de l'information dans l'histoire urbaine jusqu'à ce moment-là - c'est ce qu'on a appelé l'urbanisme numérique, la ville numérique, la ville intelligente, l'urbanisme intelligent, ou une foule de termes similaires (Brown et Toze, 2017 ; Lauriault, McArdle et Kitchin, 2018 ; Meijer, 2018).

La promesse était que l'augmentation de la collecte et de l'analyse de larges volumes de données rendrait la ville « connaissable » de manière plus approfondie et plus complète que ce qui était possible jusqu'à présent, tandis que les analyses algorithmiques et automatisées et les systèmes de prise de décision

Les villes sont devenues des épicentres essentiels pour répondre aux risques systémiques dans l'ensemble de la société. De la pauvreté à la nutrition, de l'éducation au vieillissement, de l'inégalité des richesses à la discrimination, de la santé à la protection sociale, du changement technologique à la dégradation de l'environnement, ou des conflits à l'immigration, tous ces problèmes se croisent au sein des villes - et, par conséquent, on y retrouve également bon nombre des solutions proposées et mises en place.

permettraient d'apporter des réponses viables à ces nouvelles connaissances à grande échelle et à grande vitesse (Kitchin, 2014a, 2014b). Comme l'écrivent Tulomello et Iapaolo (2022, p. 6),

> *« Fondée sur des visions positives de l'omniscience urbaine guidée par les données, l'hypothèse épistémologique qui sous-tend l'urbanisme intelligent est que chaque ville fonctionne, du moins idéalement, comme un « système de systèmes » complexe - comprenant les transports, l'énergie, l'éducation, les soins de santé, la sécurité publique et la sécurité (cf. IBM, 2011, p. 2 ; Marvin et Luque-Ayala, 2017). En tant que telle, la performance globale des villes peut être optimisée en abordant les problèmes urbains de manière holistique et coordonnée grâce à l'analyse intégrative des données géosociales ».*

Comme l'affirment les auteurs et de nombreux autres chercheurs (Mattern, 2021 ; Shapiro, 2020), la vision de la gouvernance fondée sur les données était celle d'un immense partage d'informations permanent dans une ville totalement interconnectée et en réseau numérique, associé à une analyse et à une réaction à ces données aussi proches que possible du temps réel.

Un tel système de gouvernance a toutefois nécessité un changement important des lieux de pouvoir et de contrôle. À cette échelle, à cette vitesse et à ce niveau profond d'intégration des systèmes de technologie de l'information, de nombreuses décisions ont échappé à une forme de contrôle facilité : « Dans ces circonstances, le gestionnaire des données (l'acteur ou les acteurs qui contrôlent et gèrent ces données) devient *de facto* ou *de jure*, selon l'arrangement, l'acteur dominant de la gouvernance qui exerce des contrôles politiques, de surveillance et de réglementation » (Clarke, 2020, p. 105). Les critiques ont également souligné que les fournisseurs de technologies privés avaient un impact considérable sur les solutions technologiques conçues pour résoudre les problèmes (Green, 2019 ; Valverde et Flynn, 2020), ce qui a conduit à ce que certains ont appelé « l'élaboration de politiques par l'approvisionnement » (Crump, 2016). Comme l'affirment Franke et Gailhofer, « dans le cas des villes intelligentes et de la numérisation en général, le secteur public n'exerce pas un contrôle prépondérant, et encore moins monopolistique, sur les données ou les outils permettant de les utiliser. Il est plutôt confronté à une transformation sociétale globale dominée par des entreprises privées. En outre, les relations entre les différents acteurs ont changé et sont devenues plus complexes » ( 2021, p. 4). Bien que cette recherche soit largement basée sur l'expérience des grandes villes mondiales, le lobbying des entreprises privées auprès des municipalités est évident dans le contexte canadien.

Comme nous avons commencé à l'explorer dans la section sur la vie privée et le risque intersectionnel, et comme nous pouvons le concrétiser ici en ce qui concerne les municipalités, ces changements technologiques ont également été des changements politiques, économiques et sociaux qui ont engendré un nouveau

spectre de risques associés. Une dynamique centrale, et selon nous souvent négligée, dans la réflexion sur les risques - et en particulier les risques liés à la vie privée - est le risque simultané résultant de l'inclusion dans le système et de l'exclusion de celui-ci. C'est ce que l'on a appelé le problème de l'hypervisibilité et de l'invisibilité dans les études de surveillance (Benjamin, 2019 ; Browne, 2015). L'inclusion dans le système signifie l'exposition aux violations de la vie privée, aux biais algorithmiques et aux effets des mesures de gouvernance fondées sur les données, avec une longue histoire d'effets négatifs et intersectionnels pour les communautés marginalisées. L'exclusion du système peut signifier l'évitement de certains de ces effets, mais aussi le manque d'accès à des services nécessaires et bénéfiques tels que les soins de santé, les transports, la sécurité, les services financiers, etc. Ces tensions ne sont pas une dichotomie, mais se chevauchent fréquemment et se manifestent le long de la fracture numérique : le fossé des inégalités qui s'est creusé de manière spectaculaire entre ceux qui ont le privilège et les ressources nécessaires pour accéder aux services de haute technologie d'une ville sans risque d'invisibilité ou d'hypervisibilité et ceux qui n'ont pas ce privilège et doivent donc faire face aux deux (Abdelaal et Andrey, 2022 ; Andrey, Masoodi, Malli, et Dorkenoo, 2021).

C'est sur ces lignes de tension que l'intersectionnalité devient un prisme essentiel. La fracture, les effets de l'hypervisibilité et de l'invisibilité, ne sont pas polarisés, mais plutôt répartis de manière différentielle entre toute une série de groupes différents en fonction de l'âge, du sexe, de la sexualité, de la racialisation et de la classe. Si les droits à la vie privée servent à sauvegarder les droits et libertés tels que l'autonomie, la dignité, l'expression, l'absence de discrimination, etc., ils doivent commencer par prendre en compte la manière dont ces droits et libertés sont affectés par les lignes intersectionnelles de la transformation numérique des villes.

Il existe d'innombrables exemples de violations ou d'invasions de ce type dans les villes du monde entier, mais dans le cadre de ce projet sur le partage des données, plusieurs questions importantes se posent. Comme l'ont souligné les experts, les données ne se trouvent pas naturellement dans le monde, elles sont créées. Elles sont le fruit de la fabrication de systèmes technologiques répondant à des besoins économiques, politiques et sociaux, et souffrent donc des mêmes problèmes de biais, d'erreur et de partialité. En outre, en tant que produit d'intérêts variés, les données sont aussi inévitablement le produit d'intérêts puissants. Ce qui est mesuré, comment et dans quel but est, dans une large mesure, déterminé par le pouvoir (Beer, 2016 ; Foucault, 2019). Dans les villes, la marginalisation des groupes peut être causée, au moins en partie, par le fait que les questions qui les concernent sont mal documentées (couverture des transports publics, accès à des aliments nutritifs, accès à l'internet haut débit, effets du dérèglement climatique, etc.), ou que les données sont soustraites à leur contrôle et utilisées contre eux avec peu de possibilités de recours (données des services sociaux, données financières, etc.). C'est dans ces structures de pouvoir différentielles des

données que nous trouvons le risque intersectionnel pour l'autonomie, la dignité, l'expression personnelle, la protection contre la discrimination, etc. contre lequel les réglementations en matière de protection de la vie privée sont censées nous prémunir.

Enfin, la vaste littérature sur la fonction et la gouvernance des villes, ainsi que le travail influent de Nord Ouvert, qui présente une « ville intelligente ouverte » plus progressiste (Nord Ouvert, s.d.), nous enseignent également que les villes ne sont pas des monolithes. En effet, l'idée même de la ville intelligente en tant que « système de systèmes » partageant constamment des données repose sur la compréhension du fait que les villes sont en réalité des assemblages hétérogènes de divers acteurs, chacun ayant ses propres pouvoirs, intérêts et effets. Ce que les études urbaines intersectionnelles nous montrent, c'est qu'historiquement et continuellement, certains de ces acteurs ont eu des effets nettement plus néfastes sur les communautés marginalisées que d'autres. Ainsi, du point de vue du partage et de la gouvernance des données, nous devons nous demander si une évaluation globale des risques pour la vie privée peut être appliquée à tous les acteurs d'une ville, ou si certains d'entre eux doivent être traités avec une prudence particulière.

## Transformation numérique des forces de l'ordre et risques

Parallèlement à la transformation numérique que connaissent les villes dans leur ensemble, la police a changé radicalement dans son utilisation des données et de la technologie. L'histoire du changement technologique remonte, via de multiples généalogies, à l'avènement des voitures de patrouille et des radios bidirectionnelles, d'une part, et à l'introduction de statistiques informatiques centralisées pour l'analyse de la criminalité, d'autre part (Wilson, 2017, 2019a, 2019b). De ces développements est née, à la fin des années 90 et avec une croissance rapide après le 11 septembre, une transformation massive et de grande envergure de la collecte, de l'analyse et de la communication des données au sein des services de police et entre les services de police et d'autres entités gouvernementales (Brayne, 2020 ; Ericson et Haggerty, 1997 ; Ferguson, 2019 ; Linder, 2021). Un grand nombre des idées concernant la gouvernance, ou le maintien de l'ordre, sur la base de la collecte et de l'analyse du « big data » ont également émergé dans les services de police - en partie sous l'impulsion des mêmes fournisseurs privés tels que Microsoft, IBM ou Motorola qui exercent d'intenses pressions sur les services de police pour qu'ils achètent et mettent en œuvre leurs technologies (Linder, 2021).

Les chercheurs spécialisés dans les études sur la surveillance et la sécurité ont expliqué en détail comment, dans le sillage du 11 septembre et de la pression et du financement qui ont suivi aux États-Unis pour que la police s'engage dans

En effet, l’idée même de la ville intelligente en tant que « système de systèmes » partageant constamment des données repose sur la compréhension du fait que les villes sont en réalité des assemblages hétérogènes de divers acteurs, chacun ayant ses propres pouvoirs, intérêts et effets.

une surveillance antiterroriste massive (Ajana, 2013 ; Muller, 2010), de vastes systèmes de collecte, d'analyse et de partage des données ont été mis en place (McQuade, 2015). Le développement de l'infrastructure et des technologies informatiques pour mener une telle surveillance, collecter et stocker les données, les analyser et les partager, a entraîné la construction d'un large système de données policières qui s'est étendu bien au-delà des États-Unis, avec des développements similaires au Royaume-Uni et au Canada et dans le reste du réseau mondial de surveillance Five Eyes ( « Five Eyes | Privacy International » , s.d.). À un niveau plus local et municipal, Ferguson (2019) et Brayne (2020) ont expliqué en détail comment les services de police ont commencé à acquérir et à utiliser de nombreux nouveaux outils de surveillance pour collecter des données sur la localisation des téléphones portables, des véhicules, des médias sociaux, des réseaux de vidéosurveillance et des données biométriques, et pour puiser dans les bases de données détenues par d'autres organismes gouvernementaux tels que les services sociaux, les services d'immatriculation des véhicules, les services de la circulation, d'autres services d'urgence et de planification urbaine. Comme Linder (2021) l'a décrit en détail, au Canada (ainsi qu'aux États-Unis où la tendance a commencé), ces technologies continuent d'être utilisées par la police longtemps après la disparition de toute menace terroriste et sont désormais fréquemment centralisées dans ce que l'on appelle les centres d'opérations en temps réel (COTR). Les COTR servent d'unités centrales de commandement et de contrôle pour la collecte, l'analyse et la diffusion en temps réel de quantités massives de données. Leur fonction est d'accéder, d'analyser et de partager des données provenant d'un large éventail de systèmes de vidéosurveillance, de bases de données, d'outils d'exploration de données algorithmiques et d'outils de prise de décision automatisée dans le but de, comme les villes, traiter les données et y répondre à une échelle et à une vitesse qui étaient auparavant impossibles.

Au Canada, ainsi qu'aux États-Unis et ailleurs, la dernière décennie a vu de nombreux exemples de services de police enfreindre la réglementation sur la protection de la vie privée avec des outils tels que les capteurs d'identité internationale d'abonné mobile (IMSI) ou ClearviewAI, ou opérant dans des zones non réglementées qui ont été jugées inadmissibles par la suite (Bennett, Haggerty, Lyon, et Steeves, 2014). En plus de ce mépris des lois sur la protection de la vie privée, de nombreux spécialistes du maintien de l'ordre affirment que ces technologies de surveillance et d'analyse des données exacerbent les tendances existantes à la discrimination intersectionnelle. D'importantes recherches ont montré que la discrimination historique de la police canadienne à l'égard des communautés racialisées (Maynard, 2017 ; Roach, 2022) et d'autres groupes marginalisés comme les sans-abri se poursuit encore aujourd'hui (CBC News, 2022 ; Kwon et Wortley, 2022 ; Palmater, 2016 ; Stelkia, 2020 ; Wortley et Owusu-Bempah, 2011). Des technologies telles que la police prédictive, l'analyse des points chauds, la reconnaissance faciale, la détection des coups de feu ou l'analyse des réseaux sociaux ont toutes été accusées de manière crédible d'amplifier les biais qui existent déjà dans les données, de contribuer à l'hypervisibilisation de groupes déjà

Au Canada, ainsi qu’aux États-Unis et ailleurs, la dernière décennie a vu de nombreux exemples de services de police enfreindre la réglementation sur la protection de la vie privée.

discriminés, de masquer les pratiques discriminatoires derrière un faux vernis d'objectivité technologique et d'introduire davantage de discrimination par le biais d'algorithmes biaisés (Brayne, 2017 ; Ferguson, 2019 ; Linder, 2021 ; Richardson et al., 2019; Tulumello et Iapaolo, 2022). Une analyse approfondie de ces systèmes dans le cadre du système juridique canadien a abouti à la conclusion que ces technologies et pratiques ont « le potentiel de violer les libertés et droits fondamentaux de la personne qui sont protégés par la Charte canadienne des droits et libertés ("la Charte") et le droit international relatif aux droits de la personne » (Robertson et al., 2020, p. 3).

Ce que des chercheurs comme Brayne (2020) et Linder (2021) ont montré, c'est que ces technologies potentiellement dangereuses reposent souvent sur des données acquises par le biais du partage de données avec des agences municipales. Il est grand temps de mettre fin au cloisonnement de la réflexion sur la transformation numérique éthique et responsable des villes et des forces de l'ordre. La section suivante examine de plus près ces intersections et fournit une analyse de la situation juridique de ces technologies croisées qui ont été examinées par les tribunaux.

## Convergence de la transformation numérique et des risques émergents pour les municipalités et les forces de l'ordre

Du point de vue de l'évolution de l'utilisation des données et de la technologie numérique, les villes et les forces de l'ordre ne se distinguent pratiquement plus en termes de ressources investies au cours de la dernière décennie. Comme l'écrivent Tulumello et Iapaolo, « Ainsi, mise en perspective, la mise en œuvre à l'échelle de la ville de solutions intelligentes, y compris la police prédictive, comme outils pour résoudre des problèmes autrement insolubles, peut être comprise comme faisant partie d'une tendance plus large vers l'élaboration de politiques basées sur des algorithmes, et doit être encadrée dans le contexte du discours et de l'imaginaire global de la ville intelligente » et « Le contrôle et la prévention de la criminalité sont interconnectés avec pratiquement tous les domaines de la politique urbaine, fonctionnant ainsi comme une synecdoque pour la politique urbaine plus généralement » ( 2022, p. 5). Joh propose la même analyse, affirmant que « À mesure que les villes deviennent "intelligentes", connectées et vigilantes, la police deviendra un aspect moins visible et plus intégré de l'environnement urbain. Ces développements ne représentent qu'une étape supplémentaire dans les changements rapides apportés à l'activité policière par l'utilisation croissante des données numérisées et de l'intelligence artificielle » (Joh, 2019, p. 181).

Cette convergence de l'application de la loi et de la gouvernance municipale provoque une érosion généralisée de la confiance du public, comme le détaillent

Interrogés sur les aspects spécifiques des villes intelligentes, les participants à l’étude ont exprimé la plus grande inquiétude concernant le partage de données avec la police, 76 % d’entre eux affirmant que ce partage ne devrait pas être autorisé ou seulement avec des garanties appropriées.

Bannerman et Orasch (2019). Leur enquête a révélé que 88 % des Canadiens étaient préoccupés par leur vie privée dans les contextes de villes intelligentes. Interrogés sur les aspects spécifiques des villes intelligentes, les participants à l'étude ont exprimé la plus grande inquiétude concernant le partage de données avec la police, 76 % d'entre eux affirmant que ce partage ne devrait pas être autorisé ou seulement avec des garanties appropriées. Dans leur analyse juridique de cette intersection, Robertson et al. (2019) ont constaté que « des problèmes peuvent survenir lorsque des données sont partagées entre les organismes chargés de l'application de la loi, d'autres organismes gouvernementaux et le secteur privé » (p. 74) et que « de tels accords de partage de données pourraient également éroder la confiance du public dans les services sociaux essentiels et les employés des services publics, ou dissuader les personnes vulnérables d'accéder à ces services » (p. 83).

Un exemple clair de cette convergence a été illustré par la proposition de Thunder Bay dans le cadre du Défi des villes intelligentes. La candidature prévoyait l'utilisation des fonds destinés aux villes intelligentes pour soutenir le développement d'un vaste appareil de surveillance policière (DUNCAN et BARRETO, 2022). L'offre fait apparaître clairement les parallèles technologiques entre les dispositifs de la ville intelligente et ceux de la police. Elle appelle à des « investissements dans des technologies et des infrastructures de sécurité publique intelligentes » (Thunder Bay, 2018) dans le cadre desquels :

- « Les poteaux intelligents serviront de stations de sécurité connectées et comprendront des caméras de surveillance intelligentes qui enregistreront et analyseront les images en temps réel (et) enverront des alertes en cas d'activités suspectes » ;
- « Les systèmes analytiques à base cognitive (intelligents et dotés d'analyses prescriptives) analyseront les données en continu et enverront des alertes aux équipes d'intervention appropriées pour qu'elles agissent (par exemple, en fonction de la taille et des activités d'un groupe). Le système peut détecter la violence ou les citoyens en état d'ébriété » ; et
- « La vidéosurveillance avec des caméras intelligentes et des capteurs d'occupation extérieurs (capteurs LoRa) sera utilisée pour analyser et suivre les personnes (sans compromettre la vie privée) rapidement grâce à la reconnaissance faciale et à la reconnaissance des mouvements. L'application de localisation, superposée à la reconnaissance du mouvement et à l'association, peut être utilisée pour réduire le rayon de recherche des personnes disparues ».

Bien qu'elle ait finalement échoué, cette demande de financement fédéral est une copie conforme des centres d'opérations en temps réel existant dans les services de police des grands centres urbains du Canada et des États-Unis. Ce paradigme de transformation numérique basé sur la surveillance ne rencontre qu'une résistance partielle et fragmentaire lorsque des technologies isolées sont critiquées et jugées par les tribunaux. Cependant, ce qui peut être critiqué et jugé devant les

Ce qui peut être critiqué et jugé devant les tribunaux est principalement le produit de ce que le public peut découvrir, et les forces de l’ordre en particulier se comportent de manière extrêmement secrète en ce qui concerne les technologies liées aux données numériques.

tribunaux est principalement le produit de ce que le public peut découvrir, et les forces de l'ordre en particulier se comportent de manière extrêmement secrète en ce qui concerne les technologies liées aux données numériques. Comme l'ont attesté un certain nombre de chercheurs au Canada (Linder, 2021 ; Monaghan, 2017), le secret policier entrave le contrôle démocratique et le débat sur la validité de ces technologies, ce qui nuit considérablement à leur légitimité. Robertson et al. (2020) affirment que « l'absence d'informations complètes pose un défi important pour déterminer dans quelle mesure les utilisations existantes ou potentielles des technologies policières algorithmiques peuvent violer les obligations des services de police sur le plan constitutionnel et en matière de droits de la personne, ou peuvent soulever d'autres problèmes juridiques » (p. 150). Cette opacité et cette ambiguïté ont été l'une des principales motivations de ce projet, et également l'une de ses principales conclusions. Toutefois, avant de passer à cette discussion, il est nécessaire d'examiner de plus près la manière dont les tribunaux ont abordé la question.

## Quelle est la contribution de la littérature en matière de gouvernance des données à cette problématique ?

Comme nous l'avons soutenu jusqu'à présent, l'évolution rapide des technologies numériques a souvent été catastrophiquement antidémocratique et exploitante, et l'un des vecteurs ayant permis ce phénomène - bien que ce ne soit pas le seul - est la violation directe et indirecte de la vie privée ainsi que les risques intersectionnels qui en résultent pour les droits de la personne ainsi que les libertés. Les violations parfois subtiles, parfois flagrantes de ces droits ont entraîné un effondrement généralisé de la confiance du public dans l'utilisation privée et publique des technologies numériques (Bannerman et Orasch, 2019). Nous soutenons dans cette section que la gouvernance des données évolue pour devenir un outil crucial permettant de repenser la manière dont les données et les technologies sont utilisées dans la société et de rétablir cette confiance.

Le discours et la pratique autour de la gouvernance des données ont considérablement évolué au cours de la dernière décennie, passant d'un concept essentiellement corporatif à un cadre socio-économique explicitement politisé pour déplacer le pouvoir, les bénéfices et les responsabilités dans une société qui se numérise rapidement. Ce changement comporte plusieurs aspects, mais les plus pertinents pour le présent rapport sont les promesses de la gouvernance des données de rétablir la confiance dans les systèmes numériques grâce à la responsabilité, à la transparence et à des mesures favorisant l'inclusion. Bien qu'elles soient encore en pleine évolution, plusieurs mesures de gouvernance des données sont en train de se développer pour atteindre ces objectifs en transformant la manière dont le public est impliqué dans la prise de décision tout au long du cycle de vie des

données et des technologies et la manière dont la vie privée et les risques sont évalués aux niveaux collectif et systémique, ainsi qu'au niveau individuel.

Le concept de gouvernance des données provient à l'origine du secteur privé et a été mis en avant dans l'industrie des entreprises comme un cadre permettant de maximiser la valeur qui peut être tirée des données détenues par une entreprise. De nombreux guides et manuels, notamment le « *Data Management Body of Knowledge* », mais bien d'autres encore, attestent de ce traitement de la gouvernance des données en tant que ressource à gérer efficacement et à exploiter de manière rentable. Cependant, avec l'essor de la « ville intelligente » tel que décrit ci-dessus, l'idée de la gouvernance des données a également fait son entrée dans la sphère de la gouvernance municipale. Étant donné la structure nettement néolibérale et axée sur le secteur privé des premiers projets de « ville intelligente » (Cardullo, Di Feliciantonio et Kitchin, 2019 ; Mattern, 2021 ; Mosco, 2019 ; Valverde et Flynn, 2020), ce croisement n'est pas surprenant, en particulier dans le sillage de décennies de transformation du concept de Nouvelle gestion publique. Dans ce discours, les villes ont été exhortées à comprendre la valeur multivalente et pluripotente des données : prendre conscience de ses multiples utilisations et valeurs, et concrétiser au mieux cette réalisation par une gouvernance des données complète et rigoureuse (Abraham, Schneider et vom Brocke, 2019 ; König, 2021).

Toutefois, à mesure que le domaine du développement des villes intelligentes a mûri, des mouvements se sont développés pour s'éloigner des paradigmes centrés sur le secteur privé et les utilisateurs en faveur de conceptions plus écosystémiques des villes en tant que réseaux avec des parties prenantes, des communautés, des intérêts et des motivations très hétérogènes. « La gouvernance des données », comme le disent Franke et Gailhofer (2021, p. 5), « décide à son tour quelles données peuvent être collectées et utilisées, par qui, de quelle manière et dans quel but, y compris, par exemple, les droits d'accès et/ou d'utilisation des données ainsi que les règles de gestion et de contrôle de la qualité et de l'exhaustivité des données ». Le concept de gouvernance des données s'est donc élargi. Comme nous l'avons vu dans les sections précédentes, la réflexion sur les données ne se limite plus à les considérer comme une ressource unique, mais comme un environnement, ou une « datasphère » (Davies, 2022). Comme l'écrivent Choenni et al., « Étant donné, d'une part, l'importance du partage des données dans une ville intelligente et, d'autre part, la complexité accrue liée au partage des données entre les (nombreuses) parties prenantes, nous soutenons la nécessité d'établir des écosystèmes de données appropriés » (Choenni, Bargh, Busker, et Netten, 2022, p. 32). Ce paradigme considère que « les données ne sont pas seulement des données », mais qu'elles sont à la fois constitutives et représentatives de la structure de la société (Linder, 2023). Les données, comme l'a affirmé Kitchin, ne sont pas un élément naturel mais sont plutôt construites par des systèmes mis en place par des personnes. Dans ce cas, la gouvernance des données est un mécanisme crucial impliqué dans cette construction. Qu'il

s'agisse de la collecte, de la qualité, du partage, de la gestion, de la vente, de la visualisation ou de la destruction des données, toutes ces questions relèvent de la gouvernance des données et sont fondamentales, au sens central du terme, pour la structure de notre société. La gouvernance des données s'intéresse donc à la société en tant que système.

Ce changement de mentalité met davantage l'accent sur trois éléments clés et, ce faisant, réoriente de manière cruciale le but et l'objectif de la gouvernance des données : la participation, la valeur et le risque. Comme le montre la définition de Franke et Gailhofer ci-dessus, le premier changement qui apparaît clairement dans leur définition est la centralisation du « qui » de la prise de décision avant le « quoi » de la décision. Si la gouvernance des données est fondamentale pour la structure de la société, il incombe à une démocratie d'être inclusive dans la structure de la prise de décision. La prise de conscience de l'existence de multiples types d'intérêts, voire d'intérêts contradictoires, dans la création de valeur à partir des données s'est accompagnée d'une prolifération effrénée de réflexions et d'expériences sur différents modèles de gouvernance des données, tels que les fiducies de données, les biens communs, les collaborations, les coopératives et d'autres modèles d'intendance. Pour reprendre une expression : les données sont trop importantes pour être confiées aux gestionnaires - le public doit être impliqué.

La question d'une participation et d'une valeur plus larges est cruciale, mais moins immédiatement pertinente pour ce projet particulier. En ce qui concerne la question de l'intersection des risques et de la gouvernance en matière de protection de la vie privée, l'évolution de la réflexion sur la gouvernance des données a également mis l'accent, dans la littérature, sur une réflexion plus large sur les risques et sur la nécessité d'un engagement démocratique plus participatif. Dans les approches d'entreprise, le risque est traité principalement sous l'angle de la conformité, et les outils de gouvernance des données s'intéressent à des questions telles que la cybersécurité ou le respect de la législation en matière de protection de la vie privée. Au Canada, l'effondrement du projet de ville intelligente Sidewalk Labs à Toronto était, dans une large mesure, lié à l'inadéquation de la réflexion sur la gouvernance des données autour des questions de risque, de protection de la vie privée, et de la question de savoir qui avait son mot à dire sur les données partagées avec qui, dans quel but, ainsi que sur la manière dont les risques étaient analysés et atténués (Lorinc, 2022 ; O'Kane, 2022 ; Valverde et Flynn, 2020). En effet, Scassa, écrivant sur les tentatives avortées d'élaboration de nouveaux modèles de gouvernance des données vers la fin du projet Sidewalk Labs, déclare que « dans certains cas, la nature et/ou le volume des données à collecter, la demande évidente d'accès aux données, les intérêts individuels ou collectifs dans les données, ou la nécessité d'un compromis entre les partenaires des secteurs public et privé, peuvent exiger la création d'un nouveau cadre de gouvernance des données pour faciliter le partage des données en fonction de valeurs articulées » (2020b, p. 46). En réponse, la gouvernance municipale des données au Canada

tend vers plus « d'ouverture et de collaboration » (Chen, 2023, p. 105), et certaines grandes villes comme Toronto et Montréal ont commencé à élaborer des chartes numériques sur la gouvernance des données pour mettre l'accent sur l'évaluation des risques et l'engagement de la communauté, par exemple le cadre stratégique de l'infrastructure numérique de la ville de Toronto.

Choenni et al (2022, p. 41) ont réalisé une évaluation récente des changements identifiés en matière de gouvernance des données suite aux types de problèmes de protection de la vie privée que nous avons identifiés dans la section précédente. Il vaut la peine de les citer longuement ici. Les auteurs préconisent un cadre qui :

- s'attache à identifier et à atténuer les risques pour la vie privée, plutôt que d'établir une dichotomie entre les renseignements personnels et non personnels, ou entre les sphères privée et publique,
- propose une nouvelle approche de la communication et du choix, en mettant l'accent sur la sensibilisation et la compréhension de l'utilisateur plutôt que sur la présentation d'exonérations de responsabilité de la part des entreprises,
- répartit les responsabilités en fonction de l'utilisation des données et des risques encourus par les personnes concernées, plutôt que d'établir une dichotomie formelle entre les responsables du traitement des données et les sous-traitants,
- établit un équilibre raisonnable entre les besoins en matière de conservation des données et le droit des personnes à l'oubli ; et
- régit les transferts transfrontaliers de données sur la base de l'obligation de rendre compte et de la responsabilité permanente, plutôt que de créer des barrières arbitraires et d'exiger de remplir des formulaires bureaucratiques.

Les deux premiers points ont été considérés comme particulièrement importants, et Choenni et al. (p. 41) terminent eux-mêmes leur évaluation par : « En résumé, il est nécessaire de trouver d'autres types d'accords, tels que la formation d'organismes et de mécanismes multipartites pour aider à la gouvernance de la protection de la vie privée ». Ces dernières années ont été marquées par des innovations considérables dans la pensée et, progressivement, dans les faits, en matière de protection de la vie privée. La prise de conscience croissante des risques pour l'autonomie, la dignité, l'autodétermination, la liberté d'expression, etc. - des droits qui sont protégés au moins en partie par le droit à la vie privée, qui fonctionnent au niveau collectif, du groupe ou bien plus haut dans la chaîne de valeur, et qui ne sont donc pas pris en compte par les réglementations centrées sur les renseignements personnels identifiables - a conduit à des appels croissants à l'incorporation de la mobilisation du public dans l'évaluation des facteurs relatifs à la vie privée ainsi que des risques.

Cet élargissement de la réflexion sur la gouvernance des données pour inclure activement la mobilisation du public a été particulièrement notable dans la section concernant la gouvernance de l'intelligence artificielle et des technologies de

big data. En effet, Solano et al, écrivant sur la gouvernance des données liées à l'IA pour l'Union européenne (Solano, de Souza, Martin et Taylor, 2022, p. 4), affirment qu'étant donné les changements rapides dans la manière dont les données sont collectées et utilisées, et donc l'inconnaissabilité des risques émergents, l'implication structurelle de la participation publique, en particulier des communautés marginalisées et touchées, est essentielle. La littérature croissante sur les évaluations d'impact algorithmique (Moss, Watkins, Singh, Elish et Metcalf, 2021 ; Reisman, Schultz, Crawford et Whittaker, 2018) souligne l'importance cruciale de l'implication des communautés dans l'évaluation des risques intersectionnels, mais prévient également qu'il s'agit d'un terme potentiellement très large qui peut être compris différemment par les différentes parties prenantes et finir par obscurcir plus qu'il ne clarifie. En tant que tel, il est crucial, comme Nord Ouvert l'a largement soutenu (Linder, 2023), de veiller à ce que l'engagement public soit déterminé de manière transparente et responsable dans un cadre de gouvernance des données, tout en veillant à ce qu'il soit suffisamment flexible pour s'adapter à la question examinée.

Alors que, comme de nombreux chercheurs continuent de le souligner, le domaine de la recherche et du développement en matière de gouvernance des données continue d'évoluer rapidement, cette esquisse montre que la gouvernance des données est en train d'élargir son champ d'action pour couvrir un écosystème numérique beaucoup plus vaste. Cette expansion est motivée, en partie, par des préoccupations concernant les risques pour la vie privée qui ne sont pas faciles à appréhender dans le cadre des réglementations plus établies en matière de protection de la vie privée : la vie privée des groupes, les préjudices sociaux, le risque lié aux utilisations de données agrégées ou dépersonnalisées, les biais algorithmiques, et les risques émergents encore inconnus. Bien que la gouvernance des données ne soit pas une solution en soi, et que les structures exactes qu'elle devrait prendre ne soient pas encore claires, elle devient rapidement un outil clé dans la boîte à outils des municipalités. Des recommandations telles que des mécanismes clairs et responsables pour l'engagement public, une prise de décision transparente tout au long du cycle de vie des données, une analyse des risques au-delà des renseignements personnels ainsi que des modèles alternatifs de gestion des données sont autant de nouveaux paradigmes pour une gouvernance des données tenant compte de l'intersectionnalité.

Pourtant, malgré cette avancée et le débat actuel sur la police et les données, la littérature sur la gouvernance des données s'intéresse exclusivement aux villes en général et aux niveaux supérieurs de l'administration, ou aux entreprises privées. Le discours ne s'est pas encore suffisamment élargi pour prendre en compte explicitement une entité telle que les forces de l'ordre, même s'il s'agit d'un acteur important et unique dans l'écosystème des données numériques. La section suivante fait un pas dans cette direction en décrivant nos résultats empiriques sur l'état de la gouvernance du partage des données entre les forces de l'ordre et les villes.

# RÉSULTATS DE LA RECHERCHE

## Application de la loi et collectivités locales

Comme indiqué dans la section « Méthodologie » ci-haut, nous avons mené des entretiens avec 27 personnes dans cinq services de police municipaux ou régionaux et dix administrations municipales ou régionales. En raison de la forte résistance que nous avons rencontrée lors des entretiens, nos résultats ne peuvent pas être considérés comme représentant la fréquence ou la distribution réelle des « états de la gouvernance et du partage des données ». Toutefois, comme le montrent les sections suivantes, ces « états » ont été reconnus lors des entretiens avec suffisamment de régularité pour être considérés comme assez courants et mériter un examen approfondi.

Bien que les entretiens aient porté sur de nombreux aspects différents du partage et de la gouvernance des données, nous avons choisi de nous concentrer sur quatre domaines : ce que les personnes interrogées ont reconnu savoir de l'état actuel du partage des données ; comment l'état actuel de la gouvernance du partage des données a été articulé ; si une évaluation des impacts sur la vie privée a été entreprise au-delà des renseignements personnels ; et si les participants pensent qu'il était nécessaire de modifier la gouvernance qui encadre le partage des données. Un codage minutieux du contenu des entretiens a révélé un certain nombre de catégories pour chacun des quatre domaines d'intérêt. Les sections suivantes sont organisées par domaines et catégories plutôt que par personnes interrogées, institutions ou études de cas. Les personnes interrogées sont ainsi mentionnées plusieurs fois dans la section, ce qui nous permet de mettre en évidence des tendances ainsi que des incohérences et des tensions.

### L'état du partage des données entre les forces de l'ordre et les autres agences municipales

La première et principale question posée dans tous les entretiens concernait la quantité de données échangées entre les autorités municipales ou régionales et les différents services de police. Cette question a donné lieu à des réponses très variées : les personnes interrogées n'étaient pas toutes d'accord sur la quantité de données réellement échangées, ni sur la quantité de données qu'elles soupçonnaient être échangées mais dont elles n'avaient pas la certitude. Il s'agit d'une différenciation cruciale, comme on le verra dans les sections suivantes, car elle souligne le résultat dominant de cette recherche, à savoir qu'il y a souvent peu

de contrôle exercé sur la quantité de données partagées ainsi que sur la manière dont elles le sont et avec qui.

### Catégorie no 1 : Il existe peu d'échanges

Une première réponse commune était que les répondants ne pensaient pas qu'il y ait beaucoup de partage de données. Il a été difficile de définir ce que l'on entendait par « beaucoup » et il ne fait aucun doute que les évaluations subjectives des personnes interrogées différaient les unes des autres. Cependant, les réponses exactes sont révélatrices. Un directeur du département de technologies de l'information (TI) d'un service de police de l'Ontario a déclaré : « Je dirais qu'il y a beaucoup d'intersections. Mais je pense aussi, et c'est surprenant, qu'il y a très peu d'échanges de données entre les entités » et « donc, en ce qui concerne l'échange de données, il n'y a pas grand-chose que je sache ». Un autre directeur d'un département de technologies de l'information d'un grand service de police albertain a déclaré que « la police a fait un travail absolument terrible en termes de partage de données, à travers l'organisation et à travers le pays ».

Les employés municipaux qui dirigent le pôle « ville intelligente » d'une ville de la région du Grand Toronto (RGT) ont fait écho à cette déclaration, affirmant qu'ils partageaient des données sur la circulation en cas d'accidents ou d'autres incidents, mais qu'ils n'étaient pas au courant d'autres cas de figure. Cette évaluation, selon laquelle il existe potentiellement un certain niveau de partage de données sur la circulation, mais peu d'autres éléments, a été réitérée par un autre responsable des technologies numériques d'une grande ville de l'Ontario. Il a ajouté : « Mais autrement, du point de vue des données de la ville, ou de choses de ce genre, je n'ai rien constaté de tel depuis que je travaille ici. Non, il n'y a pas non plus d'accords de partage de données en place » et « du point de vue du partage de données, je n'ai pas connaissance de cas où des données ont été partagées ».

À première vue, il semblerait qu'un pourcentage significatif des institutions que nous avons interrogées ne pense pas qu'il y ait beaucoup, voire pas du tout, de partage de données entre les forces de l'ordre et les autorités locales. Toutefois, les personnes interrogées ci-dessus, ainsi que d'autres, ont souvent nuancé cette réponse initiale en déclarant que, bien qu'elles ne sachent pas exactement ce qui était partagé ou quelle était l'ampleur de ces partages, elles pensaient que ceux-ci avaient probablement lieu, mais qu'ils n'étaient pas suffisamment documentés ou encadrés pour que ces personnes en aient connaissance, ou encore que ces échanges avaient lieu à un niveau non officiel et ne figuraient pas en tant qu'« accord » de partage de données.

### Catégorie no 2 : Le volume d'échange est uncertain

Le directeur du département de technologies de l'information de l'un des services de forces de l'ordre cités plus haut a poursuivi en expliquant : « Nous avons [...] un manque de politique formelle de gouvernance ou de partage des données. Je vous

garantis qu'il y a d'autres instances qui ont partagé des données, avec ou sans protocole d'accord, et dont je n'ai peut-être pas connaissance. Il pourrait y avoir d'autres cas, mais je ne suis pas au courant ». Ces précisions apportées par les répondants après avoir déclaré qu'il n'y avait pas, à leur connaissance, beaucoup de partages de données, était une tendance commune à toutes les déclarations des personnes interrogées.

Un membre de la commission des services policiers de l'Ontario a déclaré que le partage des données était une question opérationnelle et ne relevait donc pas de la compétence de la commission, et « en ce qui concerne les opérations, je n'ai connaissance d'aucun partage direct de données ». Un responsable d'un centre d'opérations en temps réel (COTR) de la région du Grand Toronto a longuement discuté du partage des données du centre d'opérations en temps réel avec d'autres organismes chargés de faire appliquer de la loi, ainsi que de ses efforts en cours pour étendre l'accès direct aux réseaux de vidéosurveillance municipaux et privés (par exemple, dans les centres commerciaux, les écoles, les campus universitaires, etc.), mais il a ajouté qu'« indirectement, certains de nos collaborateurs ont des contacts avec d'autres villes d'affectation où ils peuvent échanger des informations, mais je ne sais pas si cela se fait à un niveau formel » et « pour ce qui est du reste, je ne sais pas vraiment comment cela se passe ».

Ce type de réponses jette une lumière différente sur les allégations selon lesquelles seul un partage limité des données a lieu. Il ne s'agit pas d'affirmer que celles-ci sont incorrectes, mais plutôt de démontrer que la terminologie elle-même est trompeuse. Qu'est-ce que toutes les parties prenantes entendent exactement par « partage des données » ? Comment expliquer que les responsables des départements de technologies de l'information (TI) ou les gestionnaires opérationnels d'unités à forte densité de données, telles que les COTR, déclarent « ne pas être au courant » d'un quelconque partage de données ? Il ne s'agit pas de poser des questions rhétoriques ou fantaisistes, mais plutôt de souligner l'étonnante ambiguïté que nous avons rencontrée en posant ce que nous pensions être des questions simples sur la quantité de données partagées ainsi que sur la manière et les personnes avec qui elles le sont.

### Catégorie no 3 : Oui, il existe bien des partages de données

Aussi souvent que l'on nous a dit qu'il n'y avait pas de partage de données, ou qu'il pourrait y en avoir mais que la quantité n'était pas connue, on nous a également dit sans équivoque qu'il y en existait - bien que ce soit parfois par les mêmes personnes qui nous ont dit qu'il n'y en avait pas ou qu'elles n'en savaient rien.

Les deux domaines de partage de données les plus fréquemment mentionnés sont les incidents de circulation (presque systématiques parmi les personnes interrogées) et les données relatives aux services sociaux et à la santé. Par exemple, un directeur du service TI d'un service de police de l'Alberta, bien qu'il ait déclaré précédemment que le partage des données était inadéquat et que

la qualité de celles-ci était médiocre, a affirmé : « Nous partageons beaucoup de données avec la ville. Nous essayons de faire en sorte que notre système de santé soit en quelque sorte intégré à ce concept global du maintien de l'ordre ». Deux directeurs TI de grands services de police de la région du Grand Toronto ont également évoqué l'importance et la difficulté de partager des données liées à la santé dans le but de prodiguer des services sociaux, qu'il s'agisse d'appels de service liés à la crise des opioïdes ou encore à la santé mentale. Le directeur informatique albertain a ajouté que : « Nous travaillons également en étroite collaboration avec, vous savez, les règlements, et certaines données relatives aux perturbations sociales. Nous avons donc des amis, vous savez, par exemple un certain supermarché à [ville X] qui attire beaucoup de perturbations sociales, ou encore un camp de sans-abri qui s'installe à un endroit. Nous travaillons donc en étroite collaboration avec certaines de nos structures d'aide aux sans-abri et d'autres organismes de ce type. Nous échangeons ces données dans les deux sens ».

L'un des directeurs TI de l'Ontario a déclaré qu'il n'avait « partagé des données qu'avec une seule entité, et ce dans le cadre d'un protocole d'accord officiel ». Cette entité était un organisme de sécurité publique qui menait un projet de modélisation des terrains à risque (MTR). Le MTR est une technologie de police prédictive importante, basée sur les données big data, qui cherche à tirer parti de la collecte et du partage de données provenant de nombreuses sources dans une ville pour prédire quels éléments de l'infrastructure d'une ville (haies, lumières, proximité de bars et de magasins d'alcool, etc.) sont criminogènes (Robertson et al., 2020). Toutefois, un protocole d'accord n'est pas un accord formel de partage de données et la gouvernance des données du protocole d'accord de la police de Peel n'est pas claire.

Le COTR avec lequel nous nous sommes entretenus continue à rechercher activement des accords de partage de données avec des réseaux de vidéosurveillance appartenant à des villes ainsi qu'à des centres commerciaux, des chaînes de stations-service, des chaînes de dépanneurs, des écoles et des campus. De même, l'ambiguïté et ses causes potentielles ont été mises en évidence par un autre service de police de la région du Grand Toronto après que nous nous soyons entretenus avec son conseil d'administration. Après avoir déclaré que le partage de données était une question opérationnelle et qu'ils n'en avaient pas connaissance, les deux directeurs TI principaux du service ont déclaré indépendamment l'un de l'autre qu'il existait un vaste réseau de partage de données dans le cadre d'une politique entre de nombreuses organisations, y compris le service de la circulation routière de la ville et diverses agences de services sociaux. Ces contradictions inhérentes mettent en évidence l'absence de langage et de compréhension normalisés et, par conséquent, de contrôle global des données partagées. Sur la base des nombreux entretiens menés dans le cadre de cette étude, il apparaît que l'ambiguïté ne résulte pas d'un manque de sincérité, mais plutôt d'un manque de politique et de langage communs en matière de gouvernance des données.

Une autre ville albertaine a également fait état de projets de partage de données de grande envergure, remontant à plusieurs années. Outre les cas habituels de partage de données sur la circulation, elle a également mentionné un autre projet de modélisation des terrains à risque, ainsi qu'un autre projet impliquant également le partage de données entre les forces de l'ordre et diverses agences de la ville. Le directeur du service TI de la ville a parlé non seulement des nombreux projets de partage de données existants, mais aussi des détails liés aux données et à la technologie, ainsi que des cadres de gouvernance des données mis en place pour les structurer. Dans ce cas-ci, les cadres de gouvernance des données existants semblaient être considérablement plus développés que dans d'autres situations - mais une comparaison réelle est rendue impossible par le manque de données complètes.

Enfin, il s'est dégagé d'un certain nombre d'entretiens une tendance subtile mais perceptible consistant à évoquer les portails de données ouvertes comme réponse aux questions sur le partage des données. C'est ce qu'a fait, par exemple, un directeur informatique d'un service de police de la région du Grand Toronto : « En raison de la pression extérieure, nous avons élaboré une politique de données ouvertes et mis en ligne sur notre site web les données que nous pensions pouvoir publier ». Notre échantillon d'entretiens n'étant pas représentatif, il n'est pas possible de savoir si cette tendance reflète un phénomène concerté ; mais même s'il s'agit d'un ensemble d'incidents isolés, ou d'une réaction à une interprétation du « partage des données » qui se concentre davantage sur une notion générale, publique et axée sur la transparence du concept, elle mérite d'être soulignée. Six autres villes et organismes chargés de faire appliquer la loi ont cité leurs portails de données ouvertes comme exemples de ce qu'ils considèrent représenter un partage de données entre les services de police et les autorités locales.

Il est intéressant de noter que, dans certains cas, les portails de données ouvertes ont été décrits comme des substituts à des accords spécifiques de partage de données. Quelques participants ont déclaré que ce remplacement s'était fait au détriment de leurs projets, car la qualité des données - en particulier le rythme auquel elles étaient mises à jour - avait baissé, ce qui avait entraîné l'arrêt des projets ou leur réorganisation radicale. La mention des portails de données ouvertes en tant que type de partage de données, ou comme substitut à ce dernier, implique qu'il s'agit d'un moyen plus simple et moins coûteux de répondre aux demandes de données sans la difficulté de travailler dans le cadre d'accords de partage de données orientés vers un objectif précis. C'est sur ces accords que nous allons maintenant nous pencher.

## L'état de la gouvernance du partage des données

La deuxième série de questions portait sur les cadres et les politiques de gouvernance des données en place pour réguler le partage des données. Nous avons reçu un éventail de réponses tout aussi divergentes, ce qui, une fois de plus,

reflète vraisemblablement autant le manque de langage normalisé et de compréhension de la notion de gouvernance des données que l'état de la gouvernance des données en tant que telle.

### Catégorie no 1 : Nous ne disposons pas d'une politique formelle et globale

Pour revenir sur la question des portails de données ouvertes en tant que forme de partage de données entre les forces de l'ordre et les municipalités, un certain nombre de personnes ayant soulevé cette problématique ont indiqué que le fait de considérer des données comme étant « ouvertes » est suffisant en termes de gouvernance. En d'autres termes, toute donnée pouvant être désignée comme ouverte - parfois explicitement sur la base de la législation relative à la l'accès à l'information, parfois implicitement - peut être partagée avec n'importe quelle entité, ce qui rend superflue toute autre considération de gouvernance. Dans certains cas, il a été sous-entendu que cette solution avait été choisie en lieu et place d'un cadre de gouvernance plus complexe et spécifique au partage des données. Par exemple, un directeur TI d'un service de police du sud de l'Ontario a évoqué les données ouvertes comme étant leur méthode de partage des données : « La façon dont nous partageons les informations entre notre organisation... entre nous et la région - nous n'avons pas eu de discussions sur ces sujets. Et peut-être que nous devrions le faire, en effet... mais à propos de comment partager les données... nous ne nous sommes jamais réunis pour en parler ». Ce point a été repris par un directeur TI de la région du Grand Toronto, qui a déclaré : « Je suis relativement certain qu'il y a des gens qui... des gens intelligents dans notre organisation qui se connectent aux portails de données ouvertes et obtiennent des données ... Je ne sais pas si c'est fait d'une manière coordonnée. Vous savez, ce sont les gens qui prennent l'initiative d'y aller. Mais je dirais que nous n'avons pas - à ma connaissance, nous n'avons pas de politique existante à ce sujet ».

Dans le prolongement des commentaires ci-dessus sur la gouvernance des données ouvertes, les participants ont également déclaré qu'en général, il n'existait pas de cadre couvrant de manière exhaustive l'ensemble du partage des données. Le directeur TI cité plus haut a déclaré : « Nous n'avons pas eu, et nous n'avons toujours pas de politique de gouvernance ou de partage des données formelles. Je vous garantis qu'il y a d'autres endroits qui ont partagé des données, avec ou sans protocole d'accord, et dont je n'ai peut-être pas connaissance ». Faisant écho à ce commentaire, le responsable principal du COTR issu de la même agence de forces de l'ordre a déclaré : « Indirectement, certains de nos employés ont des relations avec d'autres personnes au sein des villes et ils peuvent échanger des informations, mais je ne sais pas si cela se fait à un niveau formel, vous comprenez ? ».

Cependant, ce service de police a également contredit cette déclaration, et la plupart des autres répondants ont également indiqué qu'ils avaient au moins des accords de partage de données, voire des cadres de gouvernance globaux en

place qui guident la politique de partage dans son ensemble. Nous avons classé ces accords en deux catégories.

### Catégorie no 2 : Il existe des politiques de différentes sortes

Un certain nombre de répondants ont déclaré avoir mis en place des procédures normalisées pour encadrer les demandes et les accords de partage de données. Le COTR, par exemple, a déclaré : « Maintenant, tout cet accès est régi non seulement par le protocole d'entente, mais aussi par le commissaire à l'information et à la protection de la vie privée ». Il ressort clairement de nos conversations que les services de police ont conclu des protocoles d'accord clairs et approuvés par le commissaire avec les propriétaires publics et privés des réseaux de vidéosurveillance auxquels ils peuvent accéder par l'intermédiaire du COTR. Ils ont également précisé que le partage des données avec le projet de modélisation des terrains à risque était également encadré par un protocole d'accord. Cette clarté semble indiquer que les projets importants, significatifs et en cours sont couverts par des protocoles d'accord, mais qu'il existe également un partage de données beaucoup plus informel. Les réponses que nous avons reçues ne permettent pas de savoir si ce partage informel contrevient à une politique ou s'il s'agit d'un domaine qui n'est pas couvert par les politiques existantes.

Le directeur des technologies de l'information de ce service de police  a rendu la situation encore plus ambiguë en déclarant : « Nous ne transmettons pas les données à n'importe qui. Si quelqu'un en fait la demande, il doit y avoir un accord formel entre nous et l'agence requérante ». Toutefois, un protocole d'accord n'est pas un accord formel en ce sens qu'il n'est pas juridiquement contraignant. Un accord de partage de données, tel que celui exigé par plusieurs villes pour partager leurs réseaux de vidéosurveillance avec les forces de l'ordre, est un accord juridiquement contraignant. Selon l'une de ces villes, les protocoles d'accord sont insuffisants à l'ère des données à risque et de grande valeur, et le passage à des accords de partage de données juridiquement contraignants est un élément clé de leur initiative naissante de partage de données. D'après eux, cette pratique est considérée comme exemplaire et devrait être adoptée par d'autres institutions publiques.

En effet, les protocoles d'accord ont été cités par de nombreuses autres personnes interrogées comme des cadres au travers desquels les accords de partage de données sont régis. Un autre directeur TI d'un service de police de la région du Grand Toronto a déclaré que le partage de données entre les services de police et les services sociaux, de la circulation et du logement communautaire était encadré par un protocole d'accord. Il est intéressant de noter que lorsque nous lui avons demandé de quelle manière ces types d'accords de partage de données étaient gérés et en vertu de quel type de politique, un autre directeur TI du même service a déclaré : « Ces accords sont gouvernés par le conseil d'administration et seront rendus publics à un moment donné ». Cela contredit directement ce qu'un

membre du conseil d'administration avait affirmé, à savoir que la gouvernance du partage des données était une question opérationnelle et ne relevait donc pas de la compétence du conseil d'administration. Cela semble refléter le désaccord de longue date sur les responsabilités des commissions de services de police vis-à-vis des services de police (Roach, 2022, p. 13), ou pourrait refléter une ambiguïté conceptuelle supplémentaire concernant les protocoles d'accord par rapport aux accords de partage de données juridiquement contraignants. Quoi qu'il en soit, cela témoigne d'un manque de compréhension ainsi que de la gouvernance inadéquate des « big data ». Enfin, l'une des villes albertaines a également déclaré qu'elle utilisait auparavant des protocoles d'accord avec son service de police pour tous les projets de partage de données, y compris le projet de modélisation des terrains à risque, jusqu'à ce que ces protocoles accords soient interrompus et remplacés par le portail de données ouvertes du service de police.

Les réponses obtenues n'indiquent pas clairement quelles mesures exactes de gouvernance des données ont été incluses dans les protocoles d'accord, mais l'évaluation des facteurs relatifs à la vie privée est l'un des mécanismes qui a été fréquemment mentionné. Ces dernières seront abordées plus en détail dans la section suivante sur l'analyse d'impact intersectionnel, mais en ce qui concerne la gouvernance des données, notre conversation avec une ville de Nouvelle-Écosse s'est avérée instructive. Son directeur TI a déclaré que même si un protocole d'accord avec le service de police n'était pas nécessaire, car il ne s'agit pas d'une entité distincte, tous les projets de collecte de données devaient faire l'objet d'une évaluation des facteurs relatifs à la vie privée, conformément à la législation sur la liberté de l'information. Toutefois, il appartenait au directeur exécutif de chaque unité opérationnelle de décider d'entreprendre ou non de telles mesures, et le service de police avait la réputation d'adopter un point de vue beaucoup moins strict sur leur nécessité, ce qui pouvait conduire à la collecte de données que d'autres unités opérationnelles n'auraient pas autorisées. Ici aussi, nous voyons un exemple dans lequel des projets de données individuels sont couverts *de jure*, mais *de facto*, le système dans son ensemble est incomplet en raison d'un cadre général de gouvernance des données insuffisant.

## L'état de l'évaluation intersectionnelle des risques au sein de la gouvernance

Comme le montre la conversation avec la ville d'Halifax, nos questions sur les cadres de gouvernance mènent rapidement à des conversations sur la protection de la vie privée et d'autres évaluations d'impact effectuées dans le cadre de la gouvernance des données. Ici aussi, nous avons reçu un éventail de réponses différentes détaillant la mesure dans laquelle les personnes interrogées évaluaient ou non la protection de la vie privée ou d'autres incidences lorsqu'elles s'engageaient dans un processus de partage de données. Bien qu'ils ne soient pas nécessairement représentatifs de la situation dans l'ensemble du Canada, les types de réponses que nous avons reçues indiquent différents niveaux de

compréhension de l'importance de l'évaluation des risques pour la vie privée des personnes. Comme nous l'avons mentionné dans la section sur l'analyse de la littérature existante, la protection de la vie privée comprise comme les renseignements personnels d'une personne est le paradigme dominant pour évaluer ce type de risque, mais ce n'est pas le seul - et on se rend de plus en plus compte que les technologies en matière de « big data » et d'« IA » nécessitent une conceptualisation plus large du risque d'atteinte à la vie privée. La présente section donne un aperçu de certaines façons dont les risques d'atteinte à la vie privée sont envisagés en ce qui concerne le partage de données entre les forces de l'ordre et les collectivités locales.

### Catégorie no 1 : Renseignements personnels

Comme on pouvait s'y attendre, les participants ont assez largement fait référence à la loi sur la liberté de l'information, affirmant sur cette base que tant que les données n'étaient pas des renseignements personnels identifiables, il n'y avait pas de problème à les partager. À cette fin, un certain nombre de projets de partage de données, tels que les projets de modélisation des terrains à risque, affirment ne partager que des informations dépersonnalisées et minimisées. Dans le cas d'une ville, il peut s'agir de points de données sur un incident, son lieu et sa date. Dans le cas du partage des données de vidéosurveillance, les protocoles d'accord conclus avec les propriétaires des caméras prévoient une durée de conservation des images pour l'accès en direct. Passé ce délai, une ordonnance de production est nécessaire pour accéder aux données. Certains ont mentionné les évaluations de facteurs relatifs à la vie privée comme des outils permettant de s'assurer que les renseignements personnels ont été correctement déterminés, car ce qui constitue un renseignement personnel n'est pas nécessairement évident dans l'immédiat. Les évaluations des facteurs relatifs à la vie privée sont censées générer le type d'analyse contextuelle permettant d'effectuer cette détermination. Plusieurs ont indiqué qu'ils réalisaient des évaluations de facteurs relatifs à la vie privée pour tous les projets de partage de données.

Toutefois, comme le montrent les recherches sur l'efficacité réelle des EFVP (R. Bayley et al., 2007 ; R. M. Bayley et Bennett, 2012), leur application est inégale, comme le confirment plusieurs personnes interrogées. Certaines ont également déclaré que, bien qu'elles ne fournissent des données d'incident dépersonnalisées que pour trois points de données (lieu, date, type d'incident), elles ont décidé d'utiliser ces points de données particuliers sans procéder à une évaluation des facteurs relatifs à la vie privée. La citation suivante d'un directeur TI d'un service de police de la région du Grand Toronto souligne une fois de plus le type d'ambiguïté que nous avons rencontrée en matière de gouvernance des données :

> *« Dans le cas du [projet MTR], nous avons veillé à ce que toutes les informations soient anonymes. Nous n'avons donc fourni aucun descripteur personnel. Je pense que nous avons indiqué une latitude et une longitude. Je suis sûr que*

*nous avons indiqué un âge et un sexe, puis le type d'incident. Dans ce cas, je ne pense pas que nous ayons fait une EFVP... Mais chaque fois que nous mettons en place un nouveau système, nous procédons à une évaluation de l'impact sur la vie privée. Et afin de reconnaître ce que nous devons faire pour maintenir la sécurité des données ? Oui, nous faisons ces évaluations. Tout à fait. En général, pas dans le contexte du partage des données, parce que, encore une fois, nous sommes - en tant qu'agence de police, nous avons tendance à ne pas partager beaucoup de données ».*

Cette citation montre à quel point une gouvernance des données complète, ainsi qu'une profonde compréhension du langage qui l'entoure, sont cruciales pour gouverner correctement cet écosystème de données qui émerge rapidement. Ce n'est un secret pour personne que les EFVP ne sont efficaces que dans la mesure où elles sont appliquées, font l'objet d'une surveillance continue (R. M. Bayley et Bennett, 2012 ; Bennett et Bayley, 2016 ; Bennett et Raab, 2018), et sont intégrées dans un cadre et une pratique de gouvernance écosystémique pour remplir le rôle qui leur est dévolu.

### Catégorie no 2 : Au-delà de l'anonymisation

La plupart des personnes interrogées ont évité de répondre à la question sur les risques intersectionnels ou collectifs, ou l'ont fait selon le prisme des renseignements personnels. Là encore, il est probable que cela résulte principalement d'un manque de sensibilisation à ce type de réflexion sur les risques d'atteinte à la vie privée, et non d'une tentative d'évitement ou d'un manque de transparence.

Parlant de son portail de données ouvertes comme d'un projet de partage de données, un directeur TI d'un service de police de la région du Grand Toronto a déclaré que l'évaluation des données qui pouvaient être considérées comme « ouvertes » en toute sécurité comportait une analyse visant à déterminer si les données pouvaient stigmatiser certains groupes de manière différentielle. Il a ajouté que cette évaluation avait été réalisée en collaboration avec des groupes de parties prenantes publiques afin de disposer d'une perspective suffisante sur la question. Ils n'ont pas été en mesure de fournir des détails sur la manière dont cet engagement des parties prenantes est organisé et dans quelle mesure il s'agit d'une politique normalisée, mais il s'agirait d'un exemple d'évaluation de l'impact sur la vie privée qui va au-delà de la prise en compte des renseignements personnels pour inclure les questions de protection de la vie privée des groupes intersectionnels.

L'une des villes albertaines que nous avons interrogées offre un autre exemple probant d'évaluation des risques intersectionnels en matière de protection de la vie privée. Pour tous ses projets, mais plus particulièrement en ce qui concerne sa MTR, elle affirme entreprendre une analyse comparative entre les sexes plus (ACS Plus) : « Nous procédons également à ce que nous appelons une évaluation de l'analyse basée sur le genre. En anticipant les impacts de ce projet, est-ce que

nous risquons de nuire aux populations vulnérables ? ». Les réponses que nous avons reçues n'indiquent pas clairement en quoi consistent exactement les évaluations de l'outil ACS Plus, mais on nous a affirmé qu'il ne s'agissait pas d'un simple exercice de cochage de cases. Le personnel a reçu une formation à l'ACS Plus et, pour chaque projet, il doit expliquer comment il a procédé à l'évaluation et quelles conclusions il en a tirées. Le spécialiste interne de l'éthique des données de la ville a expliqué que l'ACS Plus avait été introduite dans la ville à travers la politique ACS Plus du gouvernement fédéral (W. et G. E. Canada, 2021), et qu'elle était en train de mûrir son utilisation. Bien que le personnel ait été tenu de suivre une formation approfondie, il n'a pas encore suffisamment d'expérience dans son utilisation, et il s'agit là encore d'un processus de réflexion interne qui manque d'un engagement plus complet de la part des parties prenantes publiques.

L'ACS Plus a également été déployée dans le cadre d'une approche plus large de l'évaluation des risques et de l'impact. Le responsable de la science des données de la ville a déclaré : « Il y a trois choses que nous examinons dans les projets. Cela fait partie de notre processus d'évaluation. Le premier est la protection de la vie privée. Nous avons le bureau du greffier municipal ici dans la ville. Si un projet l'exige, nous procédons à une évaluation de l'impact sur la vie privée. La protection de la vie privée est donc l'un de ces aspects. Cela nous permet de savoir ce que nous pouvons faire et ce que nous ne pouvons pas faire. L'éthique des données en est une deuxième, qui nous dit ce que nous devons faire et ce que nous ne devons pas faire. Enfin, la dernière analyse est l'ACS Plus, qui est basée sur le genre ».

Bien que les étapes et les procédures exactes de cette évaluation n'aient pas été mentionnées lors de l'entretien, le responsable a donné un aperçu des résultats concernant l'évaluation intersectionnelle de la vie privée et des risques dans le cadre de leur projet MTR :

> *« Il s'agit d'une approche qui vise à diffuser auprès des organismes de services sociaux des informations qui ne seraient normalement détenues que par les organismes chargés faire appliquer de la loi. C'est donc une façon de servir l'ACS plus. Et même pour aller un peu plus loin dans la manière dont cette approche sert l'ACS plus, elle s'appuie sur les principes de minimisation des données. Il n'y a donc pas de renseignements personnels inclus. L'ensemble du modèle est basé sur trois champs de données. L'heure d'une localisation, enfin pardon, l'heure d'un incident, le lieu de l'incident et le type d'incident. Il n'y a donc pas de données sur les contrevenants ».*

Dans cette réponse, nous pouvons voir une approche des données, de leur partage et de leur utilisation qui prend en compte l'intersectionnalité bien au-delà de la compréhension étroite du simple risque pour la vie privée des individus. Cette approche tient compte des risques pour les groupes et de la manière dont ils peuvent être mieux servis, et non seulement protégés : « Nous effectuons des prévisions en matière de sécurité de la communauté, mais nous réfléchissons

aussi, sur la base d'un continuum de sécurité de la communauté, aux personnes les mieux à même de réagir, des services sociaux jusqu'aux forces de l'ordre. Une telle approche est bien plus conforme à la prise de conscience croissante du fait qu'il ne suffit pas d'atténuer les risques pour la vie privée, mais qu'il incombe également aux prestataires de services de veiller à ce que d'autres risques, tels que la répartition inéquitable des avantages, soient également pris en compte ».

Toutefois, l'approche de cette ville était minoritaire et un certain nombre de participants ont clairement indiqué qu'ils avaient besoin de meilleures politiques et de meilleurs cadres pour s'attaquer de manière adéquate à l'écosystème de données en pleine croissance. Dans la section suivante, nous nous penchons sur ces problématiques.

## Qu'est-ce qui doit changer ?

Conformément à notre évaluation globale de l'hétérogénéité et de l'ambiguïté liées à la gouvernance du partage des données entre les autorités locales et les forces de l'ordre, les réponses aux questions portant sur ce qui doit être changé pour améliorer la situation actuelle et/ou préparer l'avenir divergeaient fortement.

Un directeur TI d'un service de police de l'Ontario a déclaré, comme nous l'avons indiqué précédemment : « Nous n'avons pas eu, et nous n'avons toujours pas, de politique formelle de gouvernance ou de partage des données. Je vous garantis qu'il y a d'autres endroits qui ont partagé des données, avec ou sans protocole d'accord, et dont je n'ai peut-être pas connaissance ». Il a ajouté : « Je pense qu'il devrait y avoir des paramètres établis et un certain niveau de formalité » et « je pense donc que quelqu'un doit mettre en place un cadre de gouvernance : voici la manière dont vous devez faire telle chose pour que nous puissions être en conformité, parce que sinon, nous adopterons toujours la solution la plus facile ». Selon ce directeur TI, bien qu'il existe dans certains cas des politiques qui couvrent le partage des données, elles sont souvent inadéquates et n'offrent pas une couverture complète, en particulier à la lumière de la numérisation qui s'opère progressivement. Toutefois, il est d'avis que même si certains services de police commencent à élaborer leurs propres politiques (par exemple, la nouvelle politique en matière d'IA du service de police de Toronto), une politique normalisée mise en œuvre au niveau provincial est nécessaire pour mieux garantir un partage sûr entre les organisations et entre les provinces.

Un directeur TI d'un service de police albertain a noté qu'un autre aspect de ce problème est celui de la qualité des données : « La police a fait un travail absolument terrible en termes de partage des données au sein de l'organisation et à travers le pays » ; « La qualité des données dans la police est tout simplement terriblement mauvaise, ce qui a poussé les agences à dire, oh, honnêtement, je ne veux pas les partager ». Beaucoup ont souligné l'importance croissante du partage des données avec d'autres organismes de prestation de services, comme

les services sociaux, de santé et de logement, les services d'intervention d'urgence, etc. mais ont ensuite déploré les difficultés rencontrées pour partager les données en temps voulu et de manière efficace : « Oui, et nous aurions certainement besoin d'aide à ce sujet. Il n'y a pas de loi au Canada, ni même au niveau provincial, pour imposer la normalisation de ces champs. Une initiative de ce type aiderait vraiment à faire avancer les choses. Chaque agence fait donc ce qu'elle veut, comme vous le savez ».

Une préoccupation similaire a été exprimée par un directeur TI d'un service de police du sud de l'Ontario au sujet du système 911 de prochaine génération. Le système 911PG représente un exemple paradigmatique de l'intersection de la transformation numérique des forces de l'ordre et des collectivités locales : il s'agit d'un changement complet de système, passant des systèmes analogiques 911/e911 à un système entièrement numérique de gestion des appels d'urgence et des interventions, capable de collecter et de partager bien plus de données par rapport à un simple appel. Le système 911PG permettrait et peut-être même exigerait le partage interprovincial de données potentiellement à très haut risque, comme les données sur la santé, sur les incidents d'urgence, sur les contrevenants ainsi que les enregistrements vidéo en direct. Cependant, sans normalisation de la gouvernance des données, il serait très difficile de le faire de manière adéquate. Outre ce cas, près de la moitié des personnes interrogées ont mentionné (sans que nous l'ayons demandé) le 911PG comme un problème imminent en matière de partage de données. Les collectivités locales et les forces de l'ordre ont été mandatés pour passer au 911PG d'ici 2025, et selon nos répondants, très peu sont en bonne voie pour le faire avec des niveaux de gouvernance adéquats.

Dans un avenir proche, un directeur TI de la région du Grand Toronto a déclaré qu'une bien meilleure gouvernance écosystémique des données serait nécessaire pour gérer les plans de sécurité et de bien-être communautaires que la province de l'Ontario et d'autres ont mis au point. Ces plans sont destinés à coordonner les services d'urgence et les services sociaux à travers toute la région, mais ils ne disposent pas actuellement de systèmes de gouvernance des données suffisants pour garantir leur bon fonctionnement. En outre, comme l'a montré le travail du service de police de Toronto sur sa politique en matière d'IA, les agences à travers le pays ont encore beaucoup de travail à accomplir en matière de développement de pratiques de gouvernance pour maîtriser correctement les technologies plus perturbatrices qui se profilent à l'horizon.

Les idées spécifiques pour améliorer la gouvernance des données sont disparates et controversées. Un membre d'une commission de police de la région du Grand Toronto, par exemple, a déclaré que la récente politique de la commission en matière d'IA n'était pas suffisante pour couvrir les changements à venir. En ce qui concerne la gouvernance du partage des données en particulier, il a évoqué l'idée d'un registre de partage des données, semblable à l'idée du registre des systèmes d'intelligence artificielle, qui devient rapidement une pratique courante - mais a

refusé de préciser s'il pensait que ce registre était nécessaire ou non. Le directeur informatique de ce service a toutefois insisté sur le fait qu'un registre de partage des données était une bonne innovation en matière de politique de gouvernance des données. De nombreux autres participants ont reconnu la nécessité d'améliorations en général, mais sans savoir exactement ce que celles-ci devraient être et qui devrait les mettre en œuvre.

C'est dans ce contexte de besoins ambigus et de manque de solutions que nous présentons les résultats de nos deux ateliers d'experts sur les technologies numériques, la gouvernance des données et les forces de l'ordre dans la section suivante.

## Ateliers d'experts

Comme nous l'avons expliqué ci-haut, les résultats de notre recherche issus des entretiens étaient confus, ambivalents, très hétérogènes et donc difficiles à interpréter. Nous avons constaté au cours de nos entretiens que les personnes interrogées n'étaient pas en mesure de parler de la situation dans d'autres services de police ou d'autres collectivités locales. Nous avons donc décidé d'organiser deux ateliers avec des experts de ce domaine pour tenter d'ajouter une dimension supplémentaire de collecte et d'analyse d'information à notre recherche.

Les ateliers étaient organisés autour d'objectifs et de participants légèrement différents afin de recueillir un plus grand éventail d'opinions et de données. Le premier atelier s'est concentré sur l'utilisation des données et de la technologie numérique par la police au sens large, avec des questions exploratoires sur la gouvernance numérique et démocratique. Le second était plus étroitement axé sur les questions de risque intersectionnel liées à l'utilisation et au partage des données dans le cadre de l'application de la loi. Brenda McPhail, Renee Sieber, Merlin Chatwin, Teresa Scassa, Vivek Krishnamurthy, Thomas Linder, Christopher Parsons, Cristiano Therrien, Jonathan Obar, Bianca Wylie, Daniel Konikof, Alex Luscombe, Ushnish Sengupta, Alok Mukherjee, Meghan McDermott et Jamie Duncan ont participé à l'un de ces ateliers ou aux deux. Dans cette section, nous résumons les résultats des ateliers, avant de les mettre en parallèle avec les entretiens dans la conclusion finale. Les ateliers ont produit cinq évaluations clés des problèmes actuels liés à l'utilisation et au partage des données et des technologies basées sur les données par les forces de l'ordre et, partant de ce point, quatre recommandations pour améliorer la situation.

### Les forces de l'ordre ne sont pas comme les autres agences gouvernementales

Une question centrale sous-jacente à ce projet de recherche était de savoir si les services de police doivent être traités différemment des autres organisations

gouvernementales et si le partage de données avec les services de police ou l'acquisition et l'utilisation par les services de police de données et de technologies basées sur les données sont intrinsèquement plus risqués qu'avec d'autres institutions. Les participants aux deux ateliers ont convenu que c'était le cas, soutenant que la combinaison du pouvoir discrétionnaire de la police et du mandat légal pour l'utilisation de la violence justifierait à elle seule cette affirmation. Cependant, la police a également un passé et un présent bien établis de discrimination systémique contre les groupes minoritaires et marginalisés comme les femmes, les trans, les queers, les sans-abri, les personnes de couleur, les peuples autochtones, les personnes souffrant de problèmes de santé mentale, et les militants écologistes ou de gauche. Si l'on ajoute à cela le déploiement actuel des forces de l'ordre pour gérer toute une série de problèmes sociaux allant bien au-delà de la criminalité, on constate que le mélange de violence sanctionnée par l'État et de discrimination systémique exacerbe considérablement l'aspect intersectionnel du risque d'atteinte à la vie privée posé par l'accès et l'utilisation des données concernant ces groupes.

Brenda McPhail mérite d'être citée longuement ici : « Plus généralement, le partage de données avec les forces de l'ordre présente-t-il des risques particuliers ? Bien sûr, car les forces de l'ordre sont un organe qui, dans notre société, dispose d'un pouvoir discrétionnaire considérable pour prendre des mesures qui ont d'énormes conséquences sur la vie des individus. Il serait donc préférable de dire "*quels sont les risques spécifiques ?*" plutôt que "*existe-t-il [de tels risques] ?*". Les risques spécifiques proviennent de l'asymétrie de pouvoir entre les forces de l'ordre et les individus, ainsi que des impacts que les activités des forces de l'ordre ont sur la vie des individus, et sont exacerbés, pour parler de manière intersectionnelle, par la manière dont la discrimination systémique est ancrée dans les processus, les politiques et les comportements des forces de l'ordre.... Je dirai que l'intersectionnalité fournit un prisme qui est non seulement utile mais absolument nécessaire ».

Ce sentiment a été repris par les participants aux deux ateliers et est devenu une perspective clé pour interpréter l'ambiguïté des pratiques en matière de partage des données et de gouvernance présentée par les participants aux entretiens. L'absence de gouvernance concernant le partage des données au sein d'une institution dont les actions ont des conséquences négatives disproportionnées pour certains groupes communautaires souligne l'urgence de remédier à l'insuffisance des dispositifs de protection.

## La réglementation relative aux renseignements personnels est insuffisante

Comme nous l'avons déjà expliqué dans une section précédente, les arguments concernant ce qui constitue ou non un renseignement personnel sont débattus depuis des années. Les experts de l'atelier ont reconnu qu'il s'agissait d'une

question sérieuse, car les renseignements personnels délimitent fondamentalement, dans le droit canadien, la différence entre les données qui doivent être considérées comme présentant un risque et celles qui n'en présentent pas. Cependant, la nature délicate de cette dichotomisation conceptuelle ne fera qu'être exacerbée par les technologies émergentes. Le « big data » et l'analyse algorithmique permettent depuis un certain temps déjà d'utiliser des données anonymes pour identifier et influencer considérablement des groupes de personnes. Ces données ne sont pas protégées car elles ne rentrent pas dans le cadre des renseignements personnels, bien que ces techniques aient clairement un impact sur la vie privée du point de vue du droit à l'autonomie.

En outre, sur le plan de la protection de la vie privée des individus et des groupes, l'avènement plus récent de l'IA générative en tant que technique de traitement des « big data » et des données synthétiques qu'elle produit soulève des questions encore plus complexes concernant les données d'entraînement utilisées dans ces systèmes et le statut des données synthétiques produites. Les données synthétiques constituent-elles une opinion ? Constituent-elles des informations confidentielles ? Quels sont les mécanismes prévus par la législation sur la protection de la vie privée dont dispose un résident pour accéder à ces données et aux techniques qui ont permis de les produire ? Ces questions sans réponse ont conduit aux problématiques suivantes concernant l'accès, le consentement et la surveillance (Scassa, 2022).

## Le consentement n'est pas requis et l'accès est difficile

La législation canadienne sur la protection de la vie privée, qu'elle s'applique au secteur public ou privé, utilise principalement les principes du consentement ou de l'accès (ou les deux) comme mécanismes permettant de rendre la collecte et l'utilisation des données transparentes et responsables. Les forces de l'ordre n'ont pas besoin de consentement pour les données collectées dans le cadre de leur mandat, de sorte que l'accès est le seul mécanisme de contrôle et de recours. Cependant, les experts de l'atelier ont longuement souligné que l'accès est souvent difficile, voire impossible, pour un certain nombre de raisons. Comme l'a dit Vivek Krishnamurthy :

> *« L'idée qu'une personne puisse contacter Facebook ou Rogers pour obtenir ses informations, imaginez qu'elle doive faire la même chose avec la police. C'est vraiment intimidant. Dans un tel scénario, je pense que l'une des préoccupations des membres des communautés marginalisées et vulnérables, lorsque vous n'avez pas mis en place un système très transparent, est que la probabilité que les choses prévues par la loi, comme la possibilité de faire valoir la protection du choix ou le contrôle et l'audit de vos données, sont de moins en moins susceptibles de se produire, en particulier dans des contextes où les individus pourraient se sentir intimidés ou menacés. Cette situation n'est donc pas conforme aux mesures de protection de l'information qui sont fondamentales dans des*

*domaines tels que la législation sur la protection de la vie privée, la notification, le consentement et le choix - quelques-uns des mécanismes de protection les plus importants qui existent ».*

L'accès dépend lui aussi des renseignements personnels. Ainsi, lorsque les renseignements personnels n'incluent pas les données potentiellement biaisées ou discriminatoires, les résidents ne disposent d'aucun mécanisme pour les évaluer. En outre, comme l'a souligné Vivek Krishnamurthy, ces personnes ont souvent déjà subi la discrimination intersectionnelle de diverses manières, ce qui les dissuade encore plus de tenter d'accéder aux données des forces de l'ordre, une organisation bien connue d'elles comme étant l'agence de violence sanctionnée par l'État et ayant un long passé de discrimination. Sans consentement ni accès, en particulier pour ceux qui en ont le plus besoin, que reste-t-il du contrôle démocratique et de la responsabilité ?

## Le contrôle démocratique est insuffisant

Dans le cadre d'une conversation plus large sur l'acquisition et l'utilisation de données et de technologies dans les domaines de l'application de la loi et de la répression, un certain nombre de points cruciaux ont été soulevés au sujet d'une surveillance inadéquate.

Les commissions de police, en tant qu'organe de contrôle civil *de jure*, ont été largement évaluées comme n'ayant pas suffisamment d'informations sur les technologies que les services de police achètent et les données qu'ils utilisent. Les experts ont déclaré que les commissions ne sont souvent pas informées des nouvelles données et technologies, qu'elles ne disposent pas du temps et de l'expertise nécessaires pour les évaluer correctement ou qu'elles sont tenues dans l'ignorance de ces techniques et de leurs utilisations sous prétexte que celle-ci sont « opérationnelles » et ne relèvent donc pas de la compétence de la commission. Toutefois, la structure et la pratique des conseils d'administration se doivent d'aller plus loin pour garantir un engagement plus représentatif sur le plan intersectionnel et un retour d'information efficace sur les questions relatives aux données et aux technologies.

En effet, les experts ont souligné le manque d'engagement significatif du public sur les questions de données et de technologie. Bien que les efforts récents du service de police de Toronto en matière d'IA et de données raciales aient été salués comme de bons débuts, la pratique est généralement rare et, lorsqu'elle est mise en œuvre, elle prend la forme de « consultations » qui n'ont que peu d'impact clair ou de prise en compte intentionnelle des groupes marginalisés sur le plan de l'intersection. En particulier en ce qui concerne les questions d'évaluation de l'impact des algorithmes, la nécessité d'inclure des voix diverses provenant d'un éventail de groupes impactés est sans équivoque. En outre, de nombreux experts ont fait valoir que, notamment dans le cas des technologies qui apprennent et s'adaptent

au fil du temps, des audits réguliers réalisés par une tierce partie transparente et responsable auprès du public sont essentiels et constituent désormais une pratique à suivre bien établie.

Enfin, la politique existante ainsi que son application ont été généralement et spécifiquement critiquées comme étant insuffisantes et exacerbant les risques potentiels liés à la protection intersectionnelle de la vie privée. Les principaux points soulevés à ce sujet sont les suivants : les évaluations des facteurs relatifs à la vie privée ne sont que partiellement mises en œuvre et font l'objet d'une surveillance limitée ; les commissaires à la protection de la vie privée n'ont pas le pouvoir de prendre des ordonnances ; la législation sur la protection de la vie privée prévoit des exceptions pour les forces de l'ordre ; les données qui peuvent être collectées sans consentement dans le cadre du mandat opérationnel des forces de l'ordre sont très étendues ; la réutilisation des données à d'autres fins n'est pas claire. Ce paysage politique ambigu et ambivalent a été un thème clair tout au long de l'étude et a conduit au dernier thème de la section suivante.

## La politique est fragmentée et obsolète ; l'élaboration des politiques se fait en vase clos et sans gouvernance

L'inadéquation du fonctionnement de la politique a fait l'objet d'une critique soutenue tout au long des ateliers. Plusieurs experts ont déclaré que la politique existante en matière de collecte et de partage des données et de gouvernance globale dans le domaine de l'application de la loi est actuellement fragmentée et partiellement contradictoire, ce qui entraîne des tensions et des ambivalences en ce qui concerne les procédures opérationnelles correctes. « Les compétences, comme le dit Christopher Parsons, « peuvent être très divergentes » entre les grandes et les petites municipalités et agences chargées du maintien de l'ordre. « Au fil du temps, [cette divergence] s'étend par le biais d'une forme de dérapage fonctionnel activé par la politique », dans laquelle les procédures réelles s'éloignent lentement de la politique initiale, souvent à la suite d'une évolution technologique, et compromettent encore davantage les tentatives de faire respecter la politique de manière homogène et fiable dans l'ensemble de l'organisation.

Ces difficultés de mise en œuvre de la politique sont en même temps des difficultés d'élaboration de celle-ci. Comme l'a dit Parsons, « vous avez cette sorte de processus politique divergent dans le cadre duquel des éléments enfouis remontent à la surface de manière peu sophistiquée, et vous avez des choses qui viennent de grandes institutions et qui se propagent vers le bas », et « vous voyez beaucoup de partage informel de connaissances qui a lieu dans ces situations. Et c'est là que je pense que l'on voit une grande partie de l'élaboration des politiques, souvent dans le cadre de discussions au sein du personnel de niveau intermédiaire ». Plusieurs experts ont ensuite souligné que si quelques grandes agences, comme le service de police de Toronto, ont une certaine capacité à innover dans ce domaine, ce n'est pas le cas de la plupart d'entre elles. Par conséquent, l'élaboration et la

diffusion de politiques au sein des forces de l'ordre de plus petite taille peuvent être un processus ad hoc de connexions et d'influences non structurées dans lequel les petits services discutent entre eux et adoptent des pratiques dont ils sont témoins sans être sûrs qu'elles sont adéquates. Cette situation est d'autant plus probable que les changements technologiques en cours se traduisent par la transformation numérique des services et des processus opérationnels, ainsi que par l'arrivée de nouvelles technologies qui dépassent de manière ambivalente les protocoles de gouvernance existants.

En outre, plusieurs experts ont affirmé que cette situation est encore exacerbée par le manque de soutien officiel et d'options réglementaires pour l'expérimentation politique dans ce domaine. Il est réellement difficile de réglementer ces questions, et les forces de l'ordre n'ont pas la possibilité d'élaborer, de tester, d'itérer et d'innover en matière de politique. C'est le résultat de procédures et de normes d'élaboration de politiques établies qui ne peuvent pas faire face aux modes actuels d'évolution technologique, mais aussi du secret inutile qui entoure une grande partie de l'adoption et de l'utilisation des technologies dans le domaine des forces de l'ordre.

## Conclusions

À première vue, nos entretiens semblent avoir révélé plus de confusion que de clarté, et plus d'ambiguïté, de contradiction et d'hétérogénéité qu'un contexte clair de différenciation des politiques, sans parler de leur cohérence. Cependant, en examinant ces résultats, nous nous sommes rendu compte que cette confusion est un élément important qui nécessite une action délibérée et sans délai. Le fait que certaines personnes interrogées qui occupent des postes à haute responsabilité dans le domaine des TIC et de la politique des données sachent exactement comment le partage des données est encadré, alors que beaucoup ne le savent pas ou donnent des réponses contradictoires ou imprécises, est un résultat important de la recherche. Cela nous a conduits aux deux premières conclusions :

1. Le volume réel de l'échange de données actuel n'est pas bien connu en termes de mesures ni bien compris sur le plan conceptuel, mais
   a. nombreux sont ceux qui considèrent que cet échange de données est très important pour le fonctionnement des services publics,
   b. La plupart s'accordent à dire que ce volume est appelé à augmenter rapidement dans un avenir proche.
2. Pourtant, à l'échelle de l'institution, la gouvernance du partage des données n'est souvent pas considérée comme suffisamment importante pour justifier une normalisation ou un contrôle rigoureux.

Une citation d'un responsable des technologies de l'information dans un service de police illustre cette tension entre le besoin perçu d'avoir davantage de technologies de données numériques pour améliorer la prestation de services et la

sensibilisation croissante du public aux risques, ainsi qu'à la méfiance à l'égard de la manière dont ces technologies sont régulées (texte en gras à notre initiative) :

> *« D'une manière générale, et d'un point de vue stratégique, ce que j'essaie de faire, c'est de dire que nous devrions utiliser la technologie autant que possible pour saisir ce que la technologie a à offrir. Pensez donc aux caméras de surveillance sur les feux rouges - les gens qui tournent à droite à la volée au feu rouge, ce qui arrive souvent. C'est une situation très détectable, détectable par une machine. Et la police coûte de plus en plus cher, comme le fait d'avoir des agents qui coûtent de plus en plus cher chaque année. Il n'est donc pas logique de confier ce travail à des agents. Et nous délivrons de moins en moins de contraventions, parce que la ville est soumise à d'autres pressions. Par conséquent, nous devons envisager de recourir davantage à l'apprentissage automatique et à la vision artificielle, à l'automatisation et au numérique dans ce domaine.* ***Mais comme il y a un manque de confiance dans la police, dans les agences de police, il est préférable que ces expérimentations ne se fassent pas en leur sein, et que l'investissement n'aille pas à la police elle-même. De cette façon, l'argument de la diminution du budget de la police ne peut pas être invoqué*** *».*

Cette citation est au cœur du problème et a été reprise par de nombreux experts lors des deux ateliers que nous avons organisés. Ces technologies numériques et axées sur les données posent d'importants problèmes en matière de protection de la vie privée et de risques intersectionnels, et l'ampleur de leur utilisation s'accroît tandis que la sensibilisation à ces questions, tant au sein de la police qu'en dehors, s'intensifie également. Le manque de clarté et de débat public cohérent et ouvert crée des tensions sur le plan de la critique, du secret et de la nécessité d'une réforme politique responsable - y compris des innovations potentielles dans la gouvernance des données et des technologies dans lesquelles les capacités technologiques sont mieux circonscrites et réparties entre les agences gouvernementales les plus appropriées. Cependant, en posant des questions plus approfondies et en examinant la manière dont ce qui a été dit sur la gouvernance a été articulé, nous avons tiré d'autres conclusions :

3. La gouvernance qui existe est souvent ad hoc, sur la base d'un projet à la fois. Il peut exister un modèle de protocole d'accord ou un accord de partage des données juridiquement contraignant, mais rarement une politique globale.
4. En ce qui concerne l'évaluation des risques en matière de protection de la vie privée, il y a peu de sensibilisation ou de considération pour aller au-delà des mesures prescrites par la loi sur l'accès à l'information et la protection de la vie privée (LAIPVP) en ce qui concerne les renseignements personnels et pour mener à bien une évaluation des facteurs relatifs à la vie privée.
5. Parmi la minorité de répondants qui reconnaissaient l'importance d'une gouvernance globale et/ou des risques posés par le partage des données au-delà de ceux couverts par les conceptions individualistes de la vie privée, il y avait une appréciation concomitante de la nécessité d'une meilleure

gouvernance des données et d'une politique d'évaluation des risques.

6. Cependant, très peu d'entre eux ont été en mesure de formuler des suggestions sur le contenu de cette politique.

En effet, une autre citation décrit simultanément l'imbrication considérable des services municipaux, des besoins en matière de sécurité publique et des forces de l'ordre, ainsi que les complications liées à la gestion des flux de données sensibles entre eux : « Mais nous ne réalisons pas de projets pour [les forces de l'ordre], car elles ont leur propre équipe. Nous avons cependant des équipes chargées de l'application de la loi ici dans la ville. Nous avons donc une équipe de sécurité d'entreprise, une équipe d'agents de la paix, etc. Nous avons ce point de vue intéressant où tout le monde vient nous voir pour divers sujets, mais parfois ces équipes ne se parlent pas entre elles ».

La collaboration essentielle entre les services gouvernementaux est encore profondément cloisonnée et fragmentée, et nos conclusions montrent qu'il existe un large éventail, assez ambivalent, d'approches de la gouvernance du partage des données - un éventail que les praticiens eux-mêmes déclarent clairement avoir besoin d'une réforme complète pour répondre aux besoins d'une interconnexion numérique croissante. Ici aussi, les ateliers d'experts sont unanimes : l'état actuel des politiques existantes et des processus d'innovation politique doit être amélioré pour répondre aux besoins d'une gouvernance responsable en ces temps d'évolution technologique rapide. Les questions interdépendantes relatives aux renseignements personnels, à l'évaluation des risques, à la gouvernance des données et aux processus de partage doivent faire l'objet d'une attention plus soutenue, compte tenu notamment de la dangerosité intersectionnelle intrinsèque de la pratique policière.

Les entretiens et les ateliers ont permis de dégager quelques exemples de pratiques intersectionnelles tenant compte des risques. Il s'agit de projets dans lesquels l'élaboration des politiques s'est faite avec la participation du public et la contribution transparente des voix marginalisées concernées, comme le prévoient des cadres tels que l'ACS Plus. Toutefois, ces exemples restent peu nombreux - et s'ils montrent une voie potentielle vers l'avenir, il reste encore des progrès à faire, même lorsque ces projets sont mis en œuvre. Lors des ateliers d'experts et des entretiens, l'ACS Plus a été citée à plusieurs reprises comme un exemple de cadre d'évaluation intersectionnelle des risques (pour la vie privée). Ce cadre existe en théorie, mais, en pratique, il est rarement bien mis en œuvre. Comme l'a dit Chris Parsons, « L'analyse comparative entre les sexes est vraiment, vraiment, vraiment importante. Et franchement, je suis très déçu que le gouvernement n'ait pas réussi à l'instrumenter de manière générale. Une des difficultés réside dans le fait que l'analyse comparative entre les sexes est imposée par des niveaux relativement élevés du gouvernement, mais qu'elle n'est pas accompagnée d'un cadre de gouvernance qui soit significatif ou qui puisse être mis en œuvre par les parties prenantes chargées de l'appliquer ».

Ce que ce rapport a mis en lumière, c'est qu'il y a une préoccupation croissante dans tous les domaines concernant les risques intersectionnels pour la vie privée du partage et de l'utilisation des données des forces de l'ordre, mais cette préoccupation est très inégalement répartie, rarement présente dans les outils de gouvernance existants, et presque entièrement non discutée dans les processus d'élaboration des politiques. Il existe des outils existants ou en cours de développement qui permettraient de conceptualiser et d'opérationnaliser ces considérations, mais en l'absence d'une meilleure gouvernance conférant un pouvoir réglementaire à ces outils, leur utilisation reste sporadique ou incomplète. Une conversation beaucoup plus approfondie, transparente et socialement et démocratiquement inclusive est nécessaire pour garantir que cette situation ne se détériore pas, entraînant une érosion supplémentaire de la confiance du public dans la bonne gouvernance. Dans cette situation actuelle de crises croisées de la légitimité de l'application de la loi, c'est l'occasion de développer de nouvelles approches significatives en matière de données, de vie privée et des risques qu'elles impliquent, en particulier pour les plus vulnérables. C'est dans cet espace réglementaire et ce besoin croissant d'innovation significative que nous souhaitons insérer ce rapport, afin qu'il serve de tremplin à la discussion et au développement.

# PROCHAINES ÉTAPES

Ce projet de recherche s'est surtout distingué par l'absence d'exemples concrets de gouvernance des données ou de conversations sur le partage des données entre les forces de l'ordre et les autorités municipales. Nous avons tiré nos conclusions autant de ce qui n'a pas été dit que de ce qui a été dit. Compte tenu du risque disproportionné auquel sont confrontées de nombreuses communautés du fait des pratiques des forces de l'ordre, nous recommandons la création d'un groupe de travail chargé d'étudier le développement d'un cadre de gouvernance des données complet et écosystémique dans l'espace entre les forces de l'ordre et les autorités municipales.

Le partage des données est beaucoup trop omniprésent, incitatif et complexe dans le réseau social, économique et technologique d'une société numérisée pour qu'on le laisse être (mal) gouverné en silos. Les solutions à ce défi commencent à peine à être débattues (Ada Lovelace Institute, 2022 ; « Disrupting Data Governance », 2023 ; Linder, 2023). À la suite de ces conclusions, nous recommandons la création d'un groupe de travail composé d'experts issus du monde universitaire, d'organisations de défense des libertés civiles, des autorités locales, des forces de l'ordre et de représentants d'un large éventail de groupes sociaux. L'objectif est de commencer à définir ce qu'engloberait une meilleure gouvernance du partage des données des forces de l'ordre, comment prendre en compte la question croissante du risque intersectionnel et comment commencer à développer des stratégies pour mettre en œuvre des réformes.

Lors de la conceptualisation initiale de ce projet, nous avons émis l'hypothèse que l'accès des forces de l'ordre aux données privées jouerait un rôle important dans notre analyse. Afin de nous familiariser avec la structure juridique au sein de laquelle la police opère, nous avons effectué une analyse juridique approfondie de l'accès légal des forces de l'ordre aux données urbaines privées. Bien que les données empiriques de notre recherche aient orienté le document dans une direction différente, l'analyse est jointe à l'annexe A et constitue la première étape d'un tel projet de suivi.

Le partage de données entre différentes entités publiques n'en est qu'à ses débuts et, bien que les systèmes techniques gagnent rapidement en complexité, nous possédons la capacité d'élaborer des politiques pour orienter ce développement vers des structures qui profitent à la société et évitent les risques. Ce rapport présente une situation initiale à laquelle le groupe de travail doit réagir et sur laquelle il doit s'appuyer. Le groupe de travail et la mobilisation des connaissances qui s'ensuivra pourraient tirer parti de cette dynamique et nous rapprocher un peu plus d'une gouvernance numérique plus ouverte, plus démocratique et plus responsable. En outre, au cours des entretiens et des ateliers d'experts, nous avons rencontré de nombreuses personnes et organisations des services de police, des autorités

locales et de la société civile, qui ont manifesté un vif intérêt pour la poursuite de ce travail à nos côtés.

Cette recherche, combinée à la résonance et au soutien considérables qu'elle a rencontrés, représente une opportunité pour le Commissariat à la protection de la vie privée de continuer à financer la recherche et l'élaboration de politiques dans ce domaine.

# BIBLIOGRAPHIE


Abdelaal, N., et Andrey, S. (2022). *Overcoming Digital Divides: What We Heard and Recommendations.* Toronto: Ryerson University. Extrait de : https://www.ryersonleadlab.com/overcoming-digital-divides

Abraham, R., Schneider, J., et vom Brocke, J. (2019). Data governance: A conceptual framework, structured review, and research agenda. *International Journal of Information Management, 49*, 424–438.

Ada Lovelace Institute. (2022). Rethinking data and rebalancing digital power. Consulté le 9 mars 2023 à l'adresse suivante : https://www.adalovelaceinstitute.org/project/rethinking-data/

Ajana, B. (2013). *Governing through biometrics: The biopolitics of identity*. Springer.

Anderson, R. (2007). Thematic content analysis (TCA). *Descriptive presentation of qualitative data*, 1–4.

Andrey, S., Masoodi, M. J., Malli, N. et Dorkenoo, S. (2021). *Mapping Toronto's Digital Divide.* Ryerson Leadership Lab and Brookfield Institute for Innovation + Entrepreneurship. Consulté sur le site : https://brookfieldinstitute.ca/wp-content/uploads/TorontoDigitalDivide_Report_Feb2021.pdf

Andreychuck, K. (2019). *Contextual Analysis of Crime in Edmonton, Canada Herman Goldstein Award Submission 2019*. Extrait de : https://popcenter.asu.edu/sites/default/files/19-17_edmonton_ab_contextual_analysis_of_crime.pdf

Artyushina, A. (2020). Is civic data governance the key to democratic smart cities? The role of the urban data trust in Sidewalk Toronto. *Telematics and Informatics, 55*, 101456.

Artyushina, A. et Wernick, A. (2021, November 8). Smart city in a post-pandemic world: Small-scale, green, and over-policed. *Spacing Toronto.* Consulté le 9 février, 2022 sur le site : http://spacing.ca/toronto/2021/11/08/smart-city-tech-post-pandemic-small-scale-green-over-policed/

Bannerman, S., et Orasch, A. (2019). *Privacy and Smart Cities: A Canadian Survey.* Rapport pour le Commissariat à la protection de la vie privée du Canada (CPVP). Université McMaster. Consulté le 9 décembre 2019 sur le site : https://smartcityprivacy.ca/wp-content/uploads/2019/01/Bannerman-Orasch-Privacy-and-Smart-Cities-A-Canadian-Survey-v1-2019.pdf

Barocas, S. et Nissenbaum, H. (2014). Big data's end run around procedural privacy protections. *Communications of the ACM, 57*(11), 31-33. ACM New York, NY, États-Unis.

Barocas, S. et Selbst, A. D. (2016). Big data's disparate impact. *California law review*, 671-732. JSTOR.

Bayley, R., Bennett, C., Charlesworth, A. J., Clarke, R., Warren, A. et Oppenheim, C. (2007). Privacy impact assessments : International study of their application and effects. UK Information Commissioner's Office.

Bayley, R. M., et Bennett, C. J. (2012). Privacy impact assessments in Canada. *Privacy Impact Assessment*, 161–185. Springer.

Beer, D. (2016). *Metric power.* Springer.

Benjamin, R. (2019). *Race After Technology: Abolitionist Tools for the New Jim Code*. John Wiley et Sons.

Bennett, C. J. et Bayley, R. M. (2016). Privacy protection in the era of 'big data': Regulatory challenges and social assessments. *Exploring the boundaries of big data, 205*. Amsterdam University Press Amsterdam.

Bennett, C. J., Haggerty, K. D., Lyon, D. et Steeves, V. (2014). *Vivre à nu : La surveillance au Canada.* Athabasca University Press.

Bennett, C. J. et Raab, C. D. (2018). Revisiting the governance of privacy: Contemporary policy instruments in global perspective. *Regulation & Governance, 14*(3), 447–464.

Bradbury, D. (s.d.). De-identify, re-identify: Anonymised data's dirty little secret. Consulté le 9 mars 2023 sur le site : https://www.theregister.com/2021/09/16/anonymising_data_feature/

Brandusescu, A., Chan, A., Diaz, F., Ferraro, A., Ketchum, A., McKelvey, F., Rhim, J. et al. (2021). *Comments on the Toronto Police Services Board Proposed Policy on AI Technologies—Montréal Society and Artificial Intelligence Collective (MoSAIC)* (SSRN Scholarly Paper No. ID 3987388). Rochester, NY : Social Science Research Network. Consulté le 22 mars 2022 sur le site : https://papers.ssrn.com/abstract=3987388

Brayne, S. (2017). La surveillance par le big data : Le cas du maintien de l'ordre. *American sociological review, 82*(5), 977-1008. SAGE Publications Sage CA : Los Angeles, Californie.

Brayne, S. (2017). Big data surveillance: The case of policing. *American sociological review, 82*(5), 977–1008. SAGE Publications Sage CA: Los Angeles, Californie.

Brayne, S. (2020). *Predict and surveil: Data, discretion, and the future of policing.* Presses de l'Université Oxford, États-Unis.

Brown, D. C. et Toze, S. (2017). Information governance in digitized public administration. *Canadian public administration, 60*(4), 581–604. Wiley Online Library.

Browne, S. (2015). *Dark matters: On the surveillance of blackness.* Presses de l'Université Duke.

Canada. Ministère de la Justice. (2019, 20 août). Modernisation de la Loi sur la protection des renseignements personnels du Canada. Consulté le 23 mars 2020 à l'adresse suivante : https://www.justice.gc.ca/fra/sjc-csj/lprp-pa/modern.html

Canada. Commissariat à la protection de la vie privée du Canada. (2008, 15 août). Lois et organismes de surveillance provinciaux et territoriaux en matière de protection de la vie privée. Consulté le 4 mars 2023 à l'adresse suivante : https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/collaboration-avec-les-provinces-et-les-territoires/lois-et-organismes-de-surveillance-provinciaux-et-territoriaux-en-matiere-de-protection-de-la-vie-privee/

Canada. Commissariat à la protection de la vie privée du Canada. (2014, 15 mai). Aperçu des lois sur la protection des renseignements personnels au Canada. Consulté le 4 mars 2023 à l'adresse suivante : https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/02_05_d_15/

Canada. Sécurité Publique. (2018, 21 décembre). Le modèle du carrefour. Consulté le 15 mars 2023 à l'adresse suivante : https://www.securitepublique.gc.ca/cnt/cntrng-crm/crm-prvntn/nvntr/dtls-fr.aspx?i=10015

Canada. Femme et Égalité des genres. (2021, 31 mars). Analyse comparative entre les sexes plus (ACS Plus). Consulté le 7 mars 2023 à l'adresse suivante : https://femmes-egalite-genres.canada.ca/fr/analyse-comparative-entre-sexes-plus.html

Cardullo, P., Di Feliciantonio, C., et Kitchin, R. (2019). *The right to the smart city.* Emerald Group Publishing.

CBC News. (2022, June 15). “We do not accept your apology,” activist tells Toronto’s police chief after race-based data released | CBC News. Consulté le 14 mars 2023 sur : https://www.cbc.ca/news/canada/toronto/toronto-police-race-based-data-use-force-strip-searches-1.6489151

Chen, Q.-S. (2023). *Investigating the current approach to developing data governance in the Canadian smart city* (Mémoire de maîtrise). Université de Waterloo.

Choenni, S., Bargh, M. S., Busker, T., et Netten, N. (2022). Data governance in smart cities: Challenges and solution directions. *Journal of Smart Cities and Society* (préimpression), 1–21. IOS Press

Clarke, A. (2020). Data Governance: The Next Frontier of Digital Government Research and Practice. Dans E. Dubois et F. Martin-Bariteau (Eds.), *Citizenship in a Connected Canada: A Policy and Research Agenda* (pp. 97–118). Ottawa : Presses de l’Université d’Ottawa.

Conseil des droits de l’homme des Nations unies. (2014, 30 juin). Le droit à la vie privée à l’ère numérique : Rapport du Haut-Commissariat des Nations Unies aux droits de l’homme. Extrait de : https://undocs.org/A/HRC/27/37

Crawford, K. (2021). *The Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*. Presses de l’Université Yale.

Crump, C. (2016). Surveillance policy making by procurement. *Wash. L. Rec., 91*, 1595. HeinOnline.

Davies, T. (2022). *Data governance and the Datasphere: Literature Review.* Datasphere Initiative. Extrait de : https://www.thedatasphere.org/datasphere-publish/data-governance-and-the-datasphere

Disrupting Data Governance: A Mozilla Guide for Reshaping the Data Economy. (2023, February 15). *Fondation Mozilla.* Consulté le 9 mars 2023, à l’adresse suivante : https://foundation.mozilla.org/en/blog/disrupting-data-governance-a-mozilla-guide-for-reshaping-the-data-economy/

DUNCAN, J. et BARRETO, D. (2022). Policing Canadian Smart Cities. *Changing of the Guards : Private Influences, Privatization, and Criminal Justice in Canada, 99.* UBC Press.

Ericson, R. c. et Haggerty, K. D. (1997). Policing the risk society. Presses de l’Université de Toronto.

Eubanks, c. (2018). *Automating Inequality : How High-Tech Tools Profile, Police, and Punish the Poor.* St. Martin’s Publishing Group.

Ferguson, A. G. (2019). *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. Presses de NYU.

Five Eyes | Privacy International. (s.d.). Consulté le 3 août 2023 sur le site : https://www.privacyinternational.org/learn/five-eyes

Foucault, M. (2019). *Power: The essential works of Michel Foucault 1954-1984*. Penguin UK.

Franke, J. et Gailhofer, P. (2021). Data governance and regulation for sustainable smart cities. *Frontiers in Sustainable Cities*, *3*, 148. Frontiers.

Gouvernement de l'Alberta. (2021). *Prix du ministre pour l'excellence municipale 2021*. Extrait de : https://open.alberta.ca/dataset/6b7bfcb4-9c45-4c3c-a4e4-28667affc1ca/resource/ce14e32d-4b22-4cee-84d6-66d9fba9783c/download/ma-ministers-awards-for-municipal-excellence-2021.pdf

Green, B. (2019). *The Smart Enough City: Putting Technology in Its Place to Reclaim Our Urban Future*. The MIT Press. Consulté le 30 juin 2022 à l'adresse suivante : https://direct.mit.edu/books/book/4204/the-smart-enough-cityputting-technology-in-its

Grieman, K. (2019). *Smart City Privacy in Canada*. (Rapport pour le Commissariat à la protection de la vie privée du Canada). Clinique d'intérêt public et de politique d'Internet du Canada Samuelson-Glushko (CIPPIC). Consulté sur le site : https://smartcityprivacy.ca/wp-content/uploads/2019/03/Greiman-OPC-Report_Final-2019.pdf

Grzanka, P. R. (2018). *Intersectionality: A Foundations and Frontiers Reader*. Routledge.

Joh, E. E. (2019). Policing the smart city. *International Journal of Law in Context*, *15*(2), 177-182. Presses de l'Université Cambridge.

Kitchin, R. (2014a). *The data revolution: Big data, open data, data infrastructures & their consequences*. Los Angeles, California: SAGE Publications.

Kitchin, R. (2014b). The real-time city? Big data and smart urbanism. *GeoJournal*, *79*(1), 1–14.

König, P. D. (2021). Citizen-centered data governance in the smart city: From ethics to accountability. *Sustainable Cities and Society*, *75*, 103308. Elsevier.

Kwon, J. et Wortley, S. (2022). Policing the police: Public perceptions of civilian oversight in Canada. *Race and Justice*, *12*(4), 644–668. SAGE Publications Sage CA: Los Angeles, CA.

Ladak, A. M., Ladak, R. et Ladak, I. (2021). Data Access and Privacy in the Age of Artificial Intelligence.

Lauriault, T. P., McArdle, G. et Kitchin, R. (2018). *Data and the City.* Routledge.

Linder, T. (2021, mai). *Intelligence-Captivated Policing : Real-Time Operations Centres and Real-Time Situational Awareness in Canadian Police Services (Centres d'opérations en temps réel et connaissance de la situation en temps réel dans les services de police canadiens)*. (Thèse de doctorat). Université Queen's, Kingston, ON. Consulté sur le site : http://hdl.handle.net/1974/28866

Linder, T. (2023, 16 février). Data Governance for Equity: Principles-Driven and Structurally Iterative. *Nord Ouvert*. Consulté le 9 mars 2023 à l'adresse suivante : https://opennorth.ca/2023/02/3102/

Lomas, N. (2019, 24 juillet). Researchers spotlight the lie of "anonymous" data. *TechCrunch.* Consulté le 9 mars 2023 à l'adresse suivante : https://techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data/

Lorinc, J. (2021, 5 janvier). How exactly are smart cities built? From facial recognition and 5G networks to cheap sensors — these are the essential components. *Thestar.com*. Consulté le 15 mars 2023 à l'adresse suivante : https://www.thestar.com/news/atkinsonseries/2021/01/05/how-exactly-are-smart-cities-built-from-facial-recognition-and-5g-networks-to-cheap-sensors-these-are-the-essential-components.html

Lorinc, J. (2022). *Dream States: Smart Cities, Technology, and the Pursuit of Urban Utopias.* Coach House Books.

Mattern, S. (2021). *A city is not a computer: Other urban intelligences.* Places books (1ère éd.). Princeton : Presses de l'Université Princeton.

Mattu, J. L., Julia Angwin, Lauren Kirchner, Surya (s.d.). How We Analyzed the COMPAS Recidivism Algorithm. *ProPublica*. Consulté le 7 mars 2023 à l'adresse suivante : https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm

Maynard, R. (2017). *Policing Black Lives: State Violence in Canada from Slavery to the Present*. Fernwood Publishing.

McQuade, B. (2015). *Securing the homeland? Inside the world of intelligence fusion.* Université d'État de New York à Binghamton.

Meijer, A. (2018). Datapolis: A Public Governance Perspective on "Smart Cities." *Perspectives on Public Management and Governance, 1*(3), 195–206.

Molnar, P. et Gill, L. (2018). Bots at the gate: A human rights analysis of automated decision-making in Canada's immigration and refugee system. Citizen Lab et le International Human Rights Program (Faculté de droit, Université de Toronto).

Monaghan, J. (2017). *Security aid: Canada and the development regime of security*. Presses de l'Université de Toronto.

Mosco, c. (2019). *The Smart City in a Digital World.* Emerald Group.

Moss, E., Watkins, E. A., Singh, R., Elish, M. C. et Metcalf, J. (2021). Assembling accountability: Algorithmic impact assessment for the public interest. *Disponible sous le numéro SSRN 3877437.*

Muller, B. J. (2010). *Security, risk and the biometric state: Governing borders and bodies*. Routledge.

Noble, S. U. (2018). *Algorithms of Oppression: How Search Engines Reinforce Racism*. NYU Press.

O'Kane, J. (2022). *Sideways: The City Google Couldn't Buy.* Random House of Canada.

Nord Ouvert. (s.d.). Principes et domaines en matière de ville intelligente ouverte.

Palmater, P. (2016).Shining light on the dark places: Addressing police racism and sexualized violence against Indigenous women and girls in the national inquiry. *Revue canadienne de la femme et du droit, 28*(2), 253-284. Presses de l'Université de Toronto.

Privacy International. (2017). *What Is Privacy? Privacy International.* Consulté le 8 mars 2023, à l'adresse suivante : http://privacyinternational.org/explainer/56/what-privacy

Rambukkana, N. (2021). *Intersectional Automations: Robotics, AI, Algorithms, and Equity.* Rowman et Littlefield.

Reisman, D., Schultz, J., Crawford, K. et Whittaker, M. (2018). Algorithmic Impact Assessments: A Practical Framework for Public Agency. *AI Now.*

Richardson, R., Schultz, J. M. et Crawford, K. (2019).Dirty data, bad predictions: How civil rights violations impact police data, predictive policing systems, and justice. *NYUL Rec. en ligne, 94*, 15. HeinOnline.

Roach, K. (2022). *Canadian Policing: Why and how it Must Change*. Irwin Law, Incorporated.

Robertson, K., Khoo, C. et Song, Y. (2020). *To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada.* Citizen Lab (Munk School of Global Affairs et Public Policy, Université de Toronto) et le International Human Rights Program (Faculté de droit, Université de Toronto). Extrait de : https://citizenlab.ca/2020/09/to-surveil-and-predict-a-human-rights-analysis-of-algorithmic-policing-in-canada/

Rocher, L., Hendrickx, J. M. et de Montjoye, Y.-A. (2019). Estimating the success of re-identifications in incomplete datasets using generative models. *Nature Communications, 10*(1), 3069.

Roller, M. R. (2019). *A quality approach to qualitative content analysis: Similarities and differences compared to other qualitative methods.* SSOAR-Social Science Open Access Repository.

Rosner, G. (2019). De-Identification as Public Policy. *Journal of Data Protection et Privacy, 3*(3), 1-18.

Safe City Mississauga. (2022). *Rapport annuel 2022 de Safe City Mississauga.* Consulté le 3 août 2023 sur le site : https://safecitymississauga.on.ca/reports/2022-annual-report.pdf

Scassa, T. (2020a). A human rights-based approach to data protection in Canada. *Citizenship in a Connected Canada: A Research and Policy Agenda, Ottawa, ON : Presses de l'Université d'Ottawa (2020)*, Document de travail de la Faculté de droit d'Ottawa., (2020-26).

Scassa, T. (2020b). Designing Data Governance for Data Sharing: Lessons from Sidewalk Toronto. *Technology and Regulation, 2020*, 44-56.

Scassa, T. (2022, 6 juillet). Anonymization and De-identification in Bill C-27. Consulté le 8 août 2023 à l'adresse suivante : https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=356:anonymization-and-de-identification-in-bill-c-27&Itemid=80

Shapiro, A. (2020). *Design, control, predict: Logistical governance in the smart city.* Presses de l'Université du Minnesota.

Solano, J. L., de Souza, S., Martin, A. et Taylor, L. (2022). Governing data and artificial intelligence for all: Models for sustainable and just data governance. Parlement européen.

Stelkia, K. (2020). Police brutality in Canada: A symptom of structural racism and colonial violence. *Yellowhead Institute, 72.*

Taylor, L., Floridi, L. et Van der Sloot, B. (2016). *Group privacy: New challenges of data technologies* (Vol. 126). Springer.

Thunder Bay. (2018). Candidature au Défi des villes intelligentes. Extrait de : https://www.thunderbay.ca/en/city-hall/resources/Documents/Grants-Incentives-and-Funding-Programs/Smart-Cities-Challenge-Application.pdf

Toronto, V. de. (2021, 1er février). SafeTO : A Community Safety et Well-Being Plan (Plan de sécurité et de bien-être de la communauté). *Ville de Toronto.* Ville de Toronto. Consulté le 15 mars 2023, à l'adresse : https://www.toronto.ca/community-people/public-safety-alerts/community-safety-programs/community-safety-well-being-plan/

Tulumello, S. et Iapaolo, F. (2022). Policing the future, disrupting urban policy today. Predictive policing, smart city, and urban policy in Memphis (TN). *Urban Geography, 43*(3), 448–469. Taylor & Francis.

Valverde, M. et Flynn, A. (2020). *Smart Cities in Canada: Digital Dreams, Corporate Designs: Independent experts analyze often-controversial schemes from Nunavut to Montreal to Toronto's failed Sidewalk Labs waterfront scheme.* James Lorimer & Company.

Ville d'Edmonton. (2017). *Gender-Based Analysis Plus (GBA+).* Extrait de : https://webdocs.edmonton.ca/siredocs/published_meetings/120/677815.pdf

Wilson, D. (2017). Algorithmic patrol: The futures of predictive policing. *Big data, crime and social control* (pp. 108–128). Routledge.

Wilson, D. (2019a). Predictive policing management: A brief history of patrol automation. *New formations, 98*(98), 139–155. Lawrence and Wishart.

Wilson, D. (2019b). Platform policing and the real-time cop. *Surveillance & Society, 17*(1/2), 69–75.

Wortley, S. et Owusu-Bempah, A. (2011). The usual suspects: Police stop and search practices in Canada. *Policing and society, 21*(4), 395–407. Taylor & Francis.

Wortley, S. et Owusu-Bempah, A. (2022). Race, police stops, and perceptions of anti-Black police discrimination in Toronto, Canada over a quarter century. *Policing: An International Journal*, (en avant-première). Emerald Publishing Limited.

# ANNEXE

## Analyse juridique de l'accès des forces de l'ordre canadiennes aux données des villes intelligentes

Il y a encore peu de jurisprudence canadienne qui traite directement de ces technologies émergentes. En effet, le droit se développe lentement et en général seulement lorsque la nécessité d'agir le requiert, un facteur qui est exacerbé par un manque de transparence de la part des organismes en charge de faire appliquer la loi. Si les services de police et les autres forces de l'ordre étaient plus transparents en ce qui concerne les techniques d'enquête qu'ils utilisent, celles-ci pourraient être examinées ouvertement ou leur constitutionnalité pourrait être évaluée régulièrement. Cependant, les techniques policières sont très peu documentées et ne sont souvent révélées que dans les rares cas où un accusé conteste leur constitutionnalité ou à la suite d'une enquête journalistique, comme c'était notamment le cas pour les intercepteurs d'IMSI (Braga, 2017). Le manque d'informations publiques entrave sérieusement le développement d'une jurisprudence constitutionnelle en matière de protection de la vie privée. Toutefois, certains cas peuvent être considérés à la fois comme des exemples directs d'accès des forces de l'ordre aux données des villes intelligentes ainsi que comme des analogies de la manière dont l'accès peut se produire. À mesure que la police des villes intelligentes se développe, celle-ci s'appuiera probablement sur l'ambiguïté offerte par ce cadre juridique pour déterminer si elle est tenue d'obtenir des ordonnances de production pour la collecte/les demandes de données liées aux villes intelligentes, ou si elle peut simplement demander ces données par le biais de mécanismes volontaires et de communications directes avec les organisations qui détiennent les données. Cette exploitation des ambiguïtés et des vides juridiques contribue directement à l'érosion de la confiance dans l'utilisation de ces technologies pour le bien commun et dans la responsabilité démocratique des institutions qui les utilisent.

### Données de localisation : possibilités pour les forces de l'ordre

La section ci-dessous aborde la question des « data dumps », un concept lié aux antennes de téléphonie cellulaire. Celles-ci relèveraient des ordonnances de production de données de transmission, ou encore des ordonnances de production de données de localisation, en fonction de la technique utilisée par les forces de l'ordre. L'utilisation des ordonnances de production pour obtenir des données historiques de localisation est moins bien documentée et les cas d'usage ne sont pas clairs. Cependant, les données historiques de localisation dépendent fortement des informations disponibles en matière de localisation. Les données

de localisation peuvent être recueillies à partir de n'importe quel type d'appareil qu'une personne porte sur elle, et pas seulement à partir des téléphones portables qui émettent des signaux vers les antennes. Différents types d'appareils intelligents peuvent envoyer des signaux Bluetooth à d'autres appareils, se connecter à des satellites ou aux systèmes infonuagiques de différentes entreprises, et créer une trace détaillée de données de localisation (abordée plus en détail dans la section sur les mandats de géorepérage).

Les ordonnances de production de données historiques de localisation sont fondées sur la norme la moins exigeante pour solliciter l'autorisation judiciaire de procéder à une intrusion dans la vie privée : l'existence de motifs de suspicion raisonnables.[2] Cela signifie que la police n'a pas besoin d'avoir des raisons valables de croire qu'une infraction a été ou sera commise, mais simplement de soupçonner qu'elle pourrait l'être et que les informations collectées aideront l'enquête Cette norme moins stricte s'applique à ce type d'ordonnance de production car l'incidence sur la vie privée des données de localisation est considéré comme moindre par rapport à des éléments tels que des photos, des messages, et autres types de contenu.

**Qu'en est-il des données de localisation en temps réel (par opposition aux données historiques) ?** Pour procéder au suivi en temps réel des dispositifs, la police doit obtenir un Mandat pour un dispositif de localisation qui l'autorise à installer, entretenir, utiliser et collecter des informations à partir d'un dispositif fixé sur les possessions du suspect (en général, il s'agit de véhicules).[3] Dans ce cadre, la police ne peut pas collecter des données de localisation en temps réel auprès d'entreprises ou d'agences, à moins d'avoir une relation informelle avec elles (ce qui est probablement limitée par les obligations de confidentialité dues par l'entreprise à ses consommateurs en vertu de la LPRPDE ou des lois sur la protection de la vie privée dans le secteur public). Le placement d'un dispositif de traçage sur un véhicule répond à la norme la moins exigeante (l'existence de motif de suspicion raisonnable qu'un crime a été ou sera commis). La Cour suprême a reconnu l'existence d'un droit à la vie privée en matière d'informations de localisation (ou, de manière plus restrictive, en matière d'informations relatives aux déplacements d'une voiture) dans l'affaire R. c. Wise 1992 (Cour suprême), où la police avait installé un dispositif de traçage sur la voiture d'un suspect sans mandat préalable.

**Quels types d'informations la police pourrait-elle collecter dans le cadre d'une ordonnance de production de données historiques de localisation ?** Les données historiques de localisation peuvent comprendre un grand nombre de types d'informations dans notre monde déjà très numérique et axé sur la localisation. Dans *Search and Seizure*, les auteurs citent les exemples suivants de possibilités offertes aux forces de l'ordre :[4]

1. **L'emplacement des réseaux Wi-Fi.** Chaque fois qu'un utilisateur se connecte à un réseau Wi-Fi, son appareil se voit attribuer une adresse unique de contrôle d'accès au réseau. Grâce aux adresses MAC uniques, vous pou-

(2) Code criminel (L.R.C. (1985), ch. C-46), art. 487.017 :

« Conditions préalables à l'ordonnance
(2) [Le juge de paix ou le juge] ne rend l'ordonnance que s'il est convaincu, par une dénonciation sous serment faite selon la formule 5.004, qu'il existe des motifs raisonnables de soupçonner, à la fois : a) qu'une infraction à la présente loi ou à toute autre loi fédérale a été ou sera commise; b) que l'identification de tout dispositif ayant servi à la transmission d'une communication ou de toute personne y ayant participé sera utile à l'enquête relative à l'infraction; c) que les données de transmission en la possession ou à la disposition d'une ou de plusieurs personnes – dont l'identité n'est pas connue au moment de la présentation de la demande – permettront cette identification ».

(3) Code criminel (L.R.C. (1985), ch. C-46), art. 492.1: RSC 1985, ch. C-46 | Code Criminel | CanLII

(4) David Schermbrucker, Randy Schwartz, Mabel Lai, Nader Hasan, *Search and Seizure* (2021, Emond Publishing) page 184.

vez trouver les emplacements des réseaux Wi-Fi auxquels cette adresse MAC a accédé à un moment précis.

2. **Les entreprises de covoiturage et de partage d'auto entre particuliers.** Elles conservent les données relatives à l'historique des déplacements des conducteurs et des passagers.Les enquêteurs peuvent parfois obtenir ces données à partir de l'appareil d'une personne en utilisant un mandat ordinaire de l'article 487 autorisant la saisie et l'examen de l'appareil. Si l'appareil n'est pas disponible ou si les données ont été supprimées, les enquêteurs peuvent également obtenir les données auprès de l'entreprise de covoiturage elle-même. Ils peuvent contraindre celle-ci à produire des informations relatives à l'historique des déplacements de la personne en tant que conducteur ou passager.
3. **Les services publics résidentiels.** Les données historiques des thermostats intelligents, les relevés de consommation d'électricité ou l'utilisation du réseau internet à domicile permettent de reconstituer la présence ou l'absence probable d'une personne à son domicile. Avec l'automatisation croissante des habitations, ce type de données va continuer à se développer.
4. **L'utilisation de la carte de crédit.** Les institutions financières peuvent fournir à la police de nombreuses informations sur les endroits où une personne s'est rendue, quand, à quelle fréquence, etc.

## Les « tower dumps ». En développement au Canada

Ce que l'on appelle familièrement « tower dump » est légalement « une ordonnance de production de tous les enregistrements du trafic cellulaire passant par une antenne cellulaire particulière au cours d'une période donnée ».[5] En d'autres termes, les « tower dumps » sont un type d'ordonnance de production visant à tracer les communications, également connu sous le nom d'ordonnance de production de données de transmission (section 487.015 du code pénal). Les enquêteurs utilisent les « tower dumps » pour identifier des suspects potentiels, des témoins ou des victimes en trouvant tous les téléphones actifs à proximité de la scène de crime ou d'intérêt. Selon les avocats de la défense, la police semble utiliser ces techniques dans deux cas : lorsqu'elle a des raisons de soupçonner que deux ou plusieurs délits ont été commis par la même personne à des endroits/heures différents et lorsque la police enquête sur un seul incident et a des raisons de croire qu'un auteur non identifié ou des témoins ont utilisé un téléphone portable sur les lieux.

(5) David Schermbrucker, Randy Schwartz, Mabel Lai, Nader Hasan, *Search and Seizure* (2021, Emond Publishing) page 170.

Lorsqu'elle demande une ordonnance de « tower dump », la police ne peut pas obtenir d'informations nominatives concernant les abonnés ou leur compte, mais elle peut obtenir leur numéro de téléphone. Si elle souhaite accéder à des informations nominatives sur les abonnés, la police doit obtenir une ordonnance générale de production, et celle-ci est soumise à un critère d'obtention plus élevé (parce qu'elle porte davantage atteinte à la vie privée qu'une ordonnance de « tower

dump », et pourrait être utilisée pour identifier des suspects potentiels plutôt que pour identifier une personne d'intérêt spécifique).[6]

(6) La norme est celle des « motifs raisonnables de soupçonner » ; http://criminalnotebook.ca/index.php/General_Production_Orders

Le seul litige public sur les « tower dump » est l'affaire R. v. Rogers Communications Partnership 2016. Bien que ces questions aient pu être posées auparavant, c'est la seule fois qu'un tribunal s'est penché sur les limites juridiques des ordonnances de production de données de type « tower dump ». Dans l'affaire R. c. Rogers, des agents enquêtant sur une série de vols dans des bijouteries ont obtenu des données de 37 antennes cellulaires. Ils ont obtenu des ordonnances de production de type « tower dump » mais n'ont pas limité leur demande aux données de transmission strictement définies. En effet, ils ont cherché à obtenir des données divulguant tous les noms, adresses, lieux, informations de facturation des consommateurs, y compris les cartes bancaires et les cartes de crédit. Les renseignements privés de tous les tiers innocents ont ainsi pu être consultés par la police. Les faits sont décrits plus en détail dans l'affaire :

> *« Dans le cadre d'une enquête sur une série de vols dans des bijouteries, la police a obtenu des ordonnances de production exigeant que les fournisseurs de services cellulaires fournissent les relevés de tous les téléphones activés, transmettant et recevant des données par l'intermédiaire de toutes les antennes Telus situées à proximité de 21 adresses municipales et de 16 antennes identifiées Rogers. Les informations requises par l'ordonnance de production comprenaient les noms, les adresses, les informations de facturation et, si la personne à qui la communication était adressée était également un client du fournisseur nommé, les mêmes données concernant ce client. Telus a estimé que les renseignements personnels d'au moins 9 000 clients auraient été divulgués. Du côté de l'entreprise Rogers, les renseignements de 34 000 abonnés auraient été révélés. Les ordonnances de production ne précisaient pas comment les renseignements sur les clients devaient être protégés et ne limitaient pas expressément les fins auxquelles la police pouvait utiliser les informations ».*

L'affaire montre clairement que ces types d'ordonnances de production ont été utilisés massivement par le passé :

(9) L'affidavit de Telus indique que depuis 2004, l'entreprise a traité des milliers d'ordonnances judiciaires exigeant des dossiers de téléphonie cellulaire. Pour la seule année 2013, elle a répondu à environ 2 500 ordonnances de production et mandats généraux. À la connaissance du déposant Telus, l'ordonnance actuellement contestée est la plus complète à ce jour en termes de nombre d'emplacements d'antennes cellulaires et de durée des périodes pour lesquelles des renseignements sur les clients sont demandés.

(10) La déclaration sous serment de l'entreprise Rogers indique qu'entre 1985 et 2014, celle-ci s'est conformée à plusieurs milliers d'ordonnances judiciaires exigeant la production de dossiers cellulaires. Pour la seule année 2013, elle a

fourni 13 800 « dossiers » en réponse à des ordonnances de production et à des mandats de perquisition.

Le juge a estimé que les Canadiens disposaient d'une attente raisonnable en matière de respect de la vie privée en ce qui concerne les enregistrements de leurs téléphones cellulaires et que, par conséquent, l'ordonnance de production ne pouvait pas être aussi large et illimitée que le demandait la police. Le juge a décidé que les ordonnances de production devaient être conçues en tenant compte des principes d'intrusion minimale dans la vie privée et d'incrémentation. Il a énoncé des lignes directrices que la police doit prendre en compte lors de l'élaboration d'ordonnances de production, notamment en encourageant la police à faire appel à des rapports créés par l'entreprise de télécommunications anonymisant et résumant adéquatement les données plutôt que de demander l'accès à l'ensemble des données existantes. Il est difficile de savoir dans quelle mesure ces lignes directrices sont suivies et si elles sont réellement applicables.[7] Parmi les autres lignes directrices, nous pouvons citer : 1) l'établissement d'un contexte permettant d'expliquer la pertinence des lieux, dates et heures visés et confirmer que les antennes pour lesquelles des enregistrements sont demandés desservent ces lieux ; 2) la garantie que la pertinence de toutes les données demandées soit clairement exposée et, si celles-ci ne sont pas pertinentes, à ce qu'elles soient omises des ordonnances ; 3) l'examen des faits de chaque cas et la vérification que tout a été mis en œuvre pour limiter le champ d'application ; et 4) la prise en compte des ressources de l'entreprise et du degré de faisabilité de la demande.

(7) Livre Search and Seizure, page 177

Il est important de noter qu'il ne s'agit que de lignes directrices et pas nécessairement d'impératifs constitutionnels. Il n'est pas certain qu'elles soient strictement respectées et il pourrait exister des canaux informels pour collecter les données relatives à la transmission des communications (dont les « tower dumps » font partie). Il n'existe pas de nouvelle jurisprudence sur ce sujet.

## Mandats de géorepérage

Il n'existe pas de jurisprudence au Canada sur les mandats de géorepérage. Des développements mineurs ont eu lieu récemment aux États-Unis. Les mandats de géorepérage recherchent des données de localisation qui identifient les appareils utilisés à un endroit précis ou dans une certaine zone géographique. Ces mandats s'appuient sur le suivi et la conservation détaillés des données de localisation effectués par les entreprises technologiques. Ces données comprennent les signaux GPS, les données d'antennes cellulaires, les dispositifs Wi-Fi et les connexions Bluetooth. L'Electronic Frontier Foundation les décrit ainsi : « À l'aide d'un seul mandat - souvent appelé mandat de "géorepérage" ou de "localisation inversée" - la police est en mesure d'accéder aux données de localisation de dizaines, voire de centaines d'appareils - des appareils qui sont liés à des personnes réelles, dont beaucoup (et peut-être dans certains cas toutes) n'ont aucun lien avec des activités criminelles et n'ont présenté aucune raison d'être soupçonnées. Les mandats

couvrent des zones géographiques allant d'un seul bâtiment à un quartier entier, et des périodes allant de quelques heures à une semaine ».

L'utilisation de mandats de géorepérage aux États-Unis a été confirmée par des rapports de Wired et du New York Times. Aucun rapport similaire n'a été publié au Canada. Toutefois, la structure des mandats de géorepérage est similaire à celle des « tower dump », en ce sens qu'ils reposent sur une structure similaire : l'identification de tous les appareils présents dans un lieu spécifique. Les mandats de géorepérage peuvent relever d'une ordonnance de production de données de localisation, plutôt que d'une ordonnance de production de données de transmission. Les exigences auxquelles les forces de l'ordre doivent satisfaire pour ces deux types d'injonctions sont essentiellement identiques. Cela signifie qu'il est probable que les mêmes principes de minimisation et d'incrémentation s'appliquent. Toutefois, étant donné que les mandats de géorepérage n'ont jamais fait l'objet de litiges ou de discussions publiques, il est impossible de savoir quel type de procédure la police suit pour obtenir des données géolocalisées.

Une affaire récente aux États-Unis, United States v. Chatrie, a conclu que l'utilisation de mandats de géorepérage tels que ceux documentés ci-dessus par le rapport violait les droits constitutionnels américains en matière de protection de la vie privée. Cette décision fait suite aux conclusions d'autres juridictions inférieures dans l'ensemble des États-Unis. Cette question n'a pas été examinée par une juridiction d'appel, ce qui signifie qu'il est possible que ces conclusions d'inconstitutionnalité changent au fil du temps, à mesure que ces questions continuent d'être débattues par des juridictions de niveau supérieur. Pour l'heure, cela signifie que les mandats de géorepérage doivent être limités dans leur champ d'application et ne pas recueillir les renseignements personnels d'un grand nombre de personnes potentiellement innocentes. Bien entendu, ces questions ne sont que rarement mises en lumière, comme l'explique le Mémo 1. Bien que les juges fassent parfois ces constats plusieurs années après l'émission des mandats, dans l'intervalle, de nombreuses personnes peuvent être sujettes à une forme de pêche aux information par la police dans l'espoir d'appréhender un individu lié à une activité criminelle.

Obligations de confidentialité envers les consommateurs : Quelles sont les obligations des entreprises privées envers leurs consommateurs lorsque la police demande la divulgation d'informations ?

Lorsque la police envoie à une entreprise une ordonnance de production demandant la divulgation de données, ces entreprises sont obligées de répondre puisque ces ordonnances sont mandatées par des juges. Comme le décrit le ministère canadien de la justice : « *La loi sur la protection des renseignements personnels et les documents électroniques* permet la divulgation de renseignements personnels à l'insu et sans le consentement de la personne concernée, à condition que cette divulgation soit demandée par une institution gouvernementale qui a

indiqué qu'elle était légalement autorisée à obtenir ces renseignements. Dans le cas des forces de l'ordre, un mandat ou une ordonnance de production répond à la définition d'une « autorité légitime » en vue de l'obtention des données.

Outre l'obligation de divulguer des informations lorsque la police est légalement autorisée à les demander, les entreprises peuvent également divulguer de leur propre chef des informations à l'insu ou sans le consentement du consommateur.[8] L'organisation devra développer ses propres motifs raisonnables de croire qu'un crime a été ou sera commis afin de justifier la divulgation en vertu de cette partie de la loi sur la protection de la vie privée dans le secteur privé. On peut supposer que les organisations disposent de leurs propres procédures internes pour identifier ce type d'informations et déterminer si la divulgation est nécessaire. **Il serait intéressant de comprendre dans quelle mesure les forces de l'ordre ont façonné ces politiques internes, le cas échéant, et si des canaux de communication sont établis entre l'entreprise et les agents de liaison des forces de l'ordre.**

(8) Article 7(2) de la LPRPDE : l'organisation ne peut utiliser de renseignement personnel à l'insu de l'intéressé ou sans son consentement que dans les cas suivants :
(a) dans le cadre de ses activités, l'organisation découvre l'existence d'un renseignement dont elle a des motifs raisonnables de croire qu'il pourrait être utile à une enquête sur une contravention au droit fédéral, provincial ou étranger qui a été commise ou est en train ou sur le point de l'être, et l'utilisation est faite aux fins d'enquête

La question de savoir si la police peut demander des informations sur les abonnés sans ordonnance ou mandat à un fournisseur d'accès à Internet a été examinée dans l'affaire R. c. Spencer 2014 SCC 43. Dans cette affaire, la Cour suprême a estimé que lorsque la police demande des informations sans autorisation judiciaire à un fournisseur d'accès à internet, les conditions contractuelles et les conditions légales (c'est-à-dire la LPRPDE) entre l'accusé (Spencer) et Shaw (le fournisseur) pèsent en faveur de la reconnaissance d'une attente raisonnable de protection de la vie privée en matière de données relatives aux renseignements personnels des abonnés. Le fait que la police demande à un fournisseur d'accès à internet de se soumettre volontairement au partage de ces informations équivaut à une « perquisition » au sens de l'article 8 de la Charte canadienne. Sans autorisation préalable, cette recherche serait déraisonnable et violerait le droit constitutionnel à la vie privée de l'individu.

Dans le contexte de la ville intelligente, cela signifie que les entreprises pourraient divulguer à la police des données provenant de capteurs et de solutions technologiques de villes intelligentes de deux manières : volontairement à partir de leurs propres systèmes de surveillance qui identifient des activités criminelles potentielles, ou elles peuvent être forcées à divulguer des informations par le biais d'une ordonnance de production. La possibilité de divulguer des informations à la suite d'une demande de la police (qui n'est pas accompagnée d'un mandat de perquisition ou d'une ordonnance de production) dépend du type d'informations qu'il est demandé de partager. Les données de localisation, par exemple, bénéficient d'une protection constitutionnelle en raison de la décision *R. c. Wise* de la Cour suprême, de sorte qu'il est possible de plaider que les renseignements recueillis à partir des cartes de bus/métro intelligentes nécessitent un mandat correspondant à un certain type d'ordonnance de protection des métadonnées. Cependant, toutes les données demandées par la police ne seront pas du type de celles qui bénéficient d'une protection constitutionnelle.

Comme le montre cette analyse, la police dispose de nombreuses méthodes pour accéder à un large éventail de données provenant des villes. Elle montre également qu'il existe plusieurs zones d'ambiguïté réglementaire qui ont été exploitées, et continueront sans aucun doute à l'être, pour accroître l'accès aux données. Les distinctions catégorielles entre les renseignements personnels et les autres données sont difficiles à établir et encore plus difficiles à régir actuellement, et une grande partie de ce qui peut être partagé « peut être dépersonnalisé et soumis à une série de techniques d'agrégation ou de floutage en termes d'identité individuelle, mais reflète toujours, à un niveau ou à un autre, le comportement et les activités des utilisateurs » (Taylor et al., 2016, p. 12).

Les risques intersectionnels en matière de vie privée liés à l’échange de données entre les forces de l’ordre et les collectivités locales