À PROPOS DU PRÉSENT RAPPORT

Le présent projet de recherche a été mené dans le cadre du programme de maîtrise en politiques publiques et en affaires internationales, à l'Université de la Colombie-Britannique. Les travaux de recherche ont été supervisés par les professeurs Timothy Cheek, Ph.D., Julian Dierkes, Ph.D., et Corrin Bulmer de l'École de politiques publiques et d'affaires internationales de l'Université de la Colombie-Britannique.

Nous tenons à remercier le Service canadien du renseignement de sécurité (SCRS) et la Direction de la liaison-recherche et de la collaboration avec les intervenants (LRCI) pour leur collaboration. Nous remercions également tous les répondants qui ont bien voulu donner un peu de leur temps précieux pour exprimer leurs points de vue, ainsi que Julian Dierkes, Ph.D., Corrin Bulmer et Timothy Cheek, Ph.D., pour leur soutien et leurs conseils tout au long du projet.

Nous tenons à préciser que le présent projet de recherche a été mené sur le territoire traditionnel, ancestral et non cédé des bandes xwməθkwəy̓ əm (Musqueam), Skwxwú7mesh-ulh (Squamish) et səl̓ilwətaʔɬ təməxʷ (Tsleil-Waututh).

AUTEURS

L'équipe qui a travaillé sur le présent projet de recherche se compose de quatre étudiants inscrits au programme de maîtrise en politiques publiques et en affaires internationales à l'Université de la Colombie-Britannique. Vous trouverez ci-dessous leurs notices biographiques.

<u>Melissa Hollobon</u>

Mme Hollobon a obtenu un baccalauréat ès arts en histoire et une mineure en relations internationales de l'Université de la Colombie-Britannique en 2018. Durant ses études de premier cycle, elle a suivi le programme d'études hispaniques et européennes à la Universitat Pompeu Fabra. Après avoir obtenu son diplôme, elle a fait un stage à titre d'analyste de données cartographiques au sein du Programme des Nations Unies pour l'environnement, dans le cadre d'un partenariat avec la Convention sur la conservation des espèces migratrices et le Conseil de coopération internationale de la Colombie-Britannique. Elle occupe actuellement un emploi étudiant comme analyste des politiques au Centre d'excellence Dallaire

pour la paix et la sécurité. Ses recherches portent principalement sur la sécurité humaine et la gouvernance mondiale, ainsi que sur la mise en œuvre des Principes de Vancouver et l'avancement du Programme mondial sur les femmes, la paix et la sécurité. Dans le cadre du présent projet de recherche, Mme Hollobon met à contribution ses expériences antérieures pour déterminer la façon dont les biais de données accentuent les inégalités.

Voir le compte LinkedIn

David Markwei

M. Markwei a obtenu un baccalauréat ès arts en relations internationales à l'Université de la Colombie-Britannique, en 2016. Il étudie actuellement les problèmes de développement et de changement social dans le cadre du programme de maîtrise en politiques publiques et en affaires internationales de l'Université de la Colombie-Britannique. Sur le plan professionnel, il coordonne des projets avec des spécialistes de la justice pénale et des chercheurs juridiques relativement à divers enjeux liés aux politiques, tels que le renforcement des milieux protecteurs dans les collectivités autochtones pour les enfants de parents ayant des démêlés avec la justice et l'accès à la justice pour les femmes des régions rurales et éloignées de la Colombie-Britannique. Dans le cadre du présent projet de recherche, M. Markwei met à contribution son expérience en matière de justice pénale et de politiques de sécurité, ainsi que ses connaissances concernant les répercussions des pratiques institutionnelles sur les collectivités marginalisées.

Voir le compte LinkedIn

Savannah Tuck

Mme Tuck est titulaire d'un baccalauréat en commerce avec spécialisation en comportement organisationnel et en ressources humaines ainsi que d'un certificat d'études supérieures en étude de la paix et des conflits. Le domaine d'études interdisciplinaire a renforcé son désir de résoudre des conflits humains et d'obtenir justice par des moyens pacifiques et constructifs qui favorisent la viabilité dans les sphères sociale, économique et environnementale. La justice et l'égalité sont les principes directeurs sur lesquels Mme Tuck s'appuie pour bâtir sa carrière. Par son expérience de travail et son intérêt à l'égard de l'aspect multidimensionnel de la sécurité, Mme Tuck apporte un point de vue unique en ce qui a trait aux problèmes d'équité entourant les enjeux éthiques et les biais dans les pratiques de gestion des données.

Consulter le compte LinkedIn

Claire Louise Okatch

Mme Okatch est titulaire d'un baccalauréat ès arts en recherche sociale et politiques publiques ainsi que d'une mineure en mandarin de l'Université de New York à Abou Dhabi. Dans le cadre de ses travaux de recherche, elle a notamment cherché comment les décideurs responsables de l'élaboration de politiques peuvent donner voix au chapitre aux femmes, aux jeunes et aux Noirs. Par la suite, elle a participé à plusieurs initiatives dans diverses régions de l'Afrique de l'Est et de l'Afrique australe, au Moyen-Orient et ailleurs dans le monde, tout en menant des activités de recherche primaires et en tenant des consultations avec des groupes communautaires. Tout récemment, Mme Okatch a coécrit un guide de recherche visant à intégrer une optique relative aux sexes plus dans les processus de recherche en général. Son objectif consiste à mettre à profit son expérience en se concentrant sur les communautés marginalisées auxquelles le manque de considération dans les méthodes et les pratiques du secteur du renseignement de sécurité peut causer des préjudices.

Consulter le compte LinkedIn

DESCRIPTION DU CLIENT : GOUVERNANCE DES DONNÉES AU SEIN DU SERVICE CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ

Au sens de l'article 2 de la *Loi sur le Service canadien du renseignement de sécurité* (*Loi sur le SCRS*, 1984), le SCRS est chargé d'enquêter sur les activités qui sont soupçonnées de constituer des menaces envers la sécurité du Canada. Le SCRS est également autorisé à faire enquête sur le terrorisme, l'espionnage et le sabotage, ainsi que sur les activités influencées par l'étranger qui sont préjudiciables aux intérêts du Canada. Les trois axes du mandat de base du SCRS sont les suivants :

1. enquêter sur les activités soupçonnées de constituer des menaces envers la sécurité du Canada;
2. conseiller le gouvernement du Canada à cet égard;
3. prendre des mesures légales pour réduire les menaces envers la sécurité du Canada.

La *Loi sur le SCRS* de 1984 prévoit le cadre législatif nécessaire à la création du SCRS. Elle confère au SCRS le mandat de recueillir des informations sur les activités soupçonnées de compromettre la sécurité nationale, telles que l'espionnage, la violence politique et le terrorisme (Service canadien du

renseignement de sécurité, 2020). Tout récemment, la *Loi de 2017 sur la sécurité nationale* a donné lieu à la création du Bureau du commissaire au renseignement et de l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR), qui ont remplacé un ancien organisme de surveillance. Qui plus est, la *Loi de 2017 sur la sécurité nationale* permet dorénavant la vérification des activités liées à la sécurité nationale et au renseignement dans tous les ministères et organismes fédéraux.

Au cours des dernières années, le SCRS a reconnu que certaines techniques de collecte de renseignements et d'enquête peuvent perpétuer les inégalités et toucher des personnes marginalisées de façon disproportionnée. C'est à la suite de cette reconnaissance que le présent projet a vu le jour. Ce projet visait à trouver et à évaluer les pratiques exemplaires à l'intérieur et à l'extérieur du SCRS afin de s'assurer que l'organisation s'acquitte de son mandat conformément à la *Charte canadienne des droits et libertés*.

Les auteurs ont consulté principalement des représentants de la LRCI, qui joue le rôle de liaison entre le SCRS et la population canadienne. La LRCI collabore avec des intervenants et des leaders d'opinion afin d'établir les enjeux et les priorités en matière de sécurité nationale et d'orienter le processus décisionnel et l'élaboration des politiques au moyen de données probantes. Elle offre un espace multidisciplinaire qui vise à acquérir une meilleure compréhension des questions de sécurité nationale, à collaborer avec des experts aux expériences et aux connaissances très variées, à remettre en question les idées reçues et les préjugés culturels et à affiner les capacités de recherche et d'analyse du SCRS.

Énoncé de la possibilité

L'appareil de la sécurité nationale reconnaît la nécessité d'établir et d'intégrer des pratiques exemplaires de façon à ce que les méthodes et les outils analytiques de gestion des données empêchent la perpétuation de biais. Il reconnaît aussi la nécessité d'agir de façon responsable en démocratie.

Questions :

1. Quelles sont les formes de biais qui pourraient toucher la gestion des données et quelles seraient les répercussions de ces biais dans le secteur de la sécurité nationale?
2. Quels groupes pourraient être touchés de façon disproportionnée par ces formes de biais et comment percevraient-ils ces biais?

3. Quelles sont les pratiques exemplaires susceptibles d'atténuer les biais dans la gestion des données?
4. Comment est-il possible de trouver un équilibre entre la sécurité nationale et la protection des libertés individuelles, deux priorités qui semblent irréconciliables, et de regarder ailleurs pour tirer des leçons?

SOMMAIRE

Compte tenu de l'émergence des mégadonnées, ainsi que des nouvelles technologies et des nouveaux outils analytiques de gestion des données, des organismes de sécurité et de renseignement jettent un regard nouveau sur les répercussions des biais dans les pratiques de gestion de données et cherchent des moyens de les atténuer dans les limites de leur mandat. Ils se trouvent ainsi face à un grand défi, c'est-à-dire qu'ils doivent trouver un équilibre entre la sécurité publique et la reddition de comptes dans un contexte démocratique. Il est donc essentiel de définir les pratiques exemplaires qui assureront une gestion de données exempte de biais et responsable dans un contexte démocratique.

Le présent rapport découle d'une étude à laquelle ont participé des intervenants issus d'organismes fédéraux, d'organisations communautaires, de la société civile et du milieu universitaire. L'étude avait pour but de se pencher sur ce défi dans le secteur de la sécurité nationale et de répondre à quatre questions clés :

1. Quelles sont les formes de biais qui pourraient toucher la gestion des données et quelles seraient les répercussions de ces biais dans le secteur de la sécurité nationale?
2. Quels groupes pourraient être touchés de façon disproportionnée par ces formes de biais et comment percevraient-ils ces biais?
3. Quelles sont les pratiques exemplaires susceptibles d'atténuer les biais dans la gestion des données?
4. Comment est-il possible de trouver un équilibre entre la sécurité nationale et la protection des libertés individuelles, deux priorités qui semblent irréconciliables, et de regarder ailleurs pour tirer des leçons?

Lors de notre étude, nous avons entrepris une analyse thématique axée sur les enjeux endémiques et les enjeux émergents pour structurer nos résultats. Les enjeux endémiques désignent les problèmes systémiques à long terme qui touchent le secteur de la sécurité nationale, mais qui sont également présents dans la société en général. Les enjeux émergents désignent les nouveaux enjeux dans le secteur de la sécurité nationale qui sont jugés les plus urgents et qui sont liés au nouveau contexte de la menace.

De façon générale, notre principale constatation est la suivante : **le SCRS a tout intérêt à se considérer comme une partie d'un grand écosystème fédéral qui travaille à surmonter les problèmes systémiques susceptibles de causer des préjudices non intentionnels aux membres de certains groupes qui demandent à obtenir un service ou une protection du gouvernement ou d'empêcher ces groupes d'en faire la demande**. Le SCRS réaffirme ainsi que son mandat consiste à assurer la sécurité du Canada et qu'il est prêt à collaborer avec d'autres organismes ou ministères pour tirer parti des pratiques existantes, pour autant qu'il puisse les adapter au secteur de la sécurité nationale.

Trois grands thèmes se dégagent de la recherche. Il y a tout d'abord le thème de la reddition de comptes et de la transparence, que nous avons divisé en deux : reddition de comptes interne et reddition de comptes externe. Dans cette section, nous avons voulu montrer comment les dispositions législatives, telles que la *Loi sur le SCRS* et la *Loi sur la protection des renseignements personnels*, définissent le cadre redditionnel du SCRS. Il est toutefois possible d'améliorer les choses en tâchant de comprendre les problèmes endémiques liés aux biais de données et en mobilisant des intervenants de l'extérieur pour étudier ces questions en vue d'élaborer des mesures de reddition de comptes externe.

Le deuxième thème tourne autour de la formation et de l'apprentissage sur l'élimination des préjugés, plus particulièrement le changement de culture et l'alphabétisation numérique. En effet, notre recherche a révélé que la formation sur les biais et l'alphabétisation numérique constitue une composante essentielle des pratiques exemplaires en matière de gestion éthique des données. Par conséquent, nous recommandons que le SCRS adopte une définition élargie de l'alphabétisation numérique qui tient compte des questions éthiques et des cadres exempts de biais, ainsi que des compétences techniques nécessaires.

Le troisième thème traite de l'interopérabilité. Par « interopérabilité », nous entendons la capacité des systèmes à échanger et à traiter des informations. De nombreux répondants ont fait mention d'un besoin accru d'interopérabilité et de collaboration interministérielle en ce qui a trait aux questions de biais et de gestion des données. Notre recherche a révélé que le SCRS peut tirer des leçons de l'expérience de quatre autres organismes ou entités du gouvernement : Statistique Canada, Secrétariat du Conseil du Trésor du Canada, Conseil canadien des normes et Sécurité publique Canada (ce qui comprend toutes les entités qui appartiennent à son portefeuille).

Les recommandations stratégiques suivantes visent à améliorer les pratiques de gestion des données du SCRS, tout en mettant l'accent sur l'atténuation préventive des préjudices pour les groupes

marginalisés de longue date et l'examen proactif des mesures de protection des renseignements personnels.

- s'appuyer sur des mécanismes de reddition de comptes existants en mobilisant les communautés marginalisées à l'interne et à l'externe;
- multiplier les possibilités d'apprentissage interne pour favoriser l'acquisition de compétences numériques et sensibiliser le personnel aux problèmes endémiques liés aux biais de données, de sorte à changer la culture organisationnelle;
- accroître l'interopérabilité en trouvant des moyens plus efficaces d'échanger des informations sur les normes en matière de gouvernance des données et d'atténuation des biais.

INTRODUCTION

Interrelations entre les données, la protection des renseignements personnels et la sécurité nationale

De plus en plus, le monde est aux prises avec des enjeux qui demandent davantage de données. Les plus importants sont la pandémie de COVID-19 et la menace en constante évolution qui pèse sur la sécurité nationale. L'éclosion de la pandémie de COVID-19 et l'importance pour les organismes de santé publique de comprendre comment le virus se propageait ont suscité des débats sur la protection des renseignements personnels, ainsi que sur la collecte et la communication de données personnelles. Au Canada, des initiatives telles que l'Outil d'auto-évaluation de la COVID-19 mis au point par Thrive Health et Santé Canada montrent que des entités publiques et privées collaborent au développement d'outils de collecte de données. Ce type d'outil suscite des questions relatives aux mesures de réglementation et de protection des renseignements personnels compte tenu des obligations redditionnelles distinctes auxquelles sont assujetties les organisations publiques et privées en matière d'utilisation de données. Les mesures de santé publique additionnelles visant à atténuer la propagation de la COVID-19, telles que le traçage des contacts, ont soulevé d'autres questions au sujet de l'équilibre entre la protection de la vie privée et la protection du bien commun.

Tout comme les autorités de santé publique, les organismes chargés du renseignement et de la sécurité nationale ont recours à des outils fondés sur les données pour accroître leur efficacité et renforcer leurs capacités. L'utilisation de données erronées ou biaisées peut mener à des décisions ou à des résultats erronés ou biaisés. Il est important de tenir compte de l'interdépendance des données et de l'analyse. Les données ne sont utiles qu'une fois traitées et analysées, et ce, au regard du contexte.

Pourtant, les outils et les méthodes utilisés pour analyser les données peuvent refléter des biais et, ainsi, entraîner des répercussions disproportionnées pour certains groupes.

Pour comprendre la position du SCRS en ce qui a trait aux biais de données et à la gouvernance des données, il faut d'abord examiner la *Loi sur le SCRS* (1984), dont découle le mandat de l'organisation. Par exemple, les articles 11.01 à 11.25 indiquent que le SCRS est tenu de présenter une demande d'autorisation judiciaire pour conserver un ensemble de données canadien et d'obtenir une autorisation du ministre pour conserver un ensemble de données étranger. Par conséquent, il incombe au SCRS de maintenir des pratiques exemplaires en matière de collecte de données afin de limiter l'intrusion de l'organisation dans la vie privée des Canadiens et de procéder uniquement à la collecte de renseignements si les données sont pertinentes dans le cadre de l'exécution de ses fonctions.

Par ailleurs, l'article 12 de la *Loi sur le SCRS* consacre l'expression « strictement nécessaire » en ce qui concerne la collecte d'informations et de renseignements s'il y a des motifs raisonnables de soupçonner une menace pour la sécurité nationale. La responsabilité qui incombe au SCRS soulève des préoccupations quant à la façon d'assurer la reddition de comptes dans un milieu où les activités se déroulent à un rythme rapide et où les décisions reposent sur des informations incomplètes et entraînent des conséquences. Tel qu'il est mentionné plus loin dans le présent rapport, des initiatives pangouvernementales ont été adaptées à cette obligation redditionnelle accrue. Parmi ces initiatives, citons la mise en œuvre de l'outil d'évaluation de l'incidence algorithmique (EIA) et de l'Analyse comparative entre les sexes plus (ACS+) dans les ministères et organismes fédéraux. Toutefois, un réexamen des stratégies actuelles s'impose étant donné la disponibilité croissante en ligne d'informations qui portent sur les auteurs de menace et d'informations qui émanent de ces derniers.

Contexte actuel : Pourquoi est-ce important que le SCRS se penche sur cette question maintenant?

Depuis le 11 septembre 2001, les organismes de sécurité nationale concentrent leurs efforts stratégiques sur la manière d'anticiper et de contrer les menaces terroristes. Par ailleurs, le meurtre de George Floyd commis par un policier de Minneapolis, Derek Chauvin, au Minnesota en 2020 a marqué un tournant et a fait naître le besoin de réformer les pratiques de gouvernance des organismes publics pour réduire la prévalence des biais et les préjudices disproportionnés à l'égard des communautés de couleur. De plus, des appels ont été lancés pour que les organisations s'engagent à mieux intégrer les principes d'intersectionnalité, d'équité et d'inclusion dans le travail et la structure de la fonction

publique fédérale du Canada, y compris le secteur de la sécurité nationale. Par exemple, en janvier 2021, le greffier du Conseil privé et secrétaire du Cabinet a publié un appel à l'action en faveur de la lutte contre le racisme, de l'équité et de l'inclusion dans la fonction publique fédérale. Dans ce document destiné au public, le greffier abordait le « traitement injuste des Noirs et des Autochtones et d'autres groupes racialisés » et exhortait les dirigeants de la fonction publique à mettre en œuvre des réformes inclusives et à créer davantage de possibilités pour les Noirs, les Autochtones et les autres communautés racialisées au sein des ministères. Comme ces appels en témoignent, les biais structurels dans les fondements institutionnels qui appuient les activités de sécurité nationale peuvent inévitablement mener à des biais dans l'exécution de programmes.

En plus de participer aux vastes débats en la matière, le SCRS prend des mesures pour mieux comprendre les biais et mieux intégrer les principes de diversité, d'équité et d'inclusion. Par exemple, un réseau interne de personnes autochtones, noires et de couleur (PANDC) collabore avec le directeur du SCRS pour aider l'organisation à comprendre ce que vivent les employés racialisés. De plus, il existe un groupe de discussion appelé Femmes en technologie qui encourage les femmes du SCRS à intégrer des bureaux qui mènent des activités dans les secteurs axés sur les données. Des initiatives comme celles-ci découlent d'associations et de réseaux de la fonction publique du Canada. En outre, des technologies novatrices sont en cours de développement à l'interne pour aider les employés à intégrer l'ACS+ dans leur travail en présentant des points décisionnels qui permettent de cerner les préjugés et les biais potentiels. Ces mesures relèvent du **principe de précaution**, qui prône une réflexion approfondie sur les implications des innovations technologiques et des méthodes utilisées en raison du risque de préjudices qu'elles représentent. Lorsque le principe de précaution est appliqué en pareil contexte, il définit un cadre axé sur l'adoption d'une démarche proactive visant à comprendre les répercussions des biais et à prendre des mesures actives pour les atténuer.

L'analyse repose sur le travail du SCRS aux côtés du Groupe consultatif sur la transparence en matière de sécurité nationale (GCT-SN) et la mise sur pied de programmes distincts, dont celui de la LRCI. Sur la base de cette analyse, le présent rapport recommande des moyens d'intégrer de bonnes méthodes de gouvernance de données dans le secteur de la sécurité nationale du Canada et d'atténuer la perpétuation des biais de données, tout en améliorant la transparence, la reddition de comptes et l'obligation de franchise envers la population canadienne.

MÉTHODOLOGIE

La méthode de recherche comportait une analyse documentaire, des entrevues semi-structurées et une analyse thématique. L'analyse documentaire a permis de dégager les tendances et les enjeux liés à la collecte et à l'utilisation des données dans le secteur de la sécurité nationale et dans des domaines connexes, ainsi que les répercussions et les risques qui touchent diverses communautés de façon disproportionnée en raison des biais sous-jacents dans les processus de gestion des données. L'analyse portait notamment sur des études de cas qui montrent en quoi le fait que les services de renseignement utilisent des données biaisées influe sur les communautés dans un contexte démocratique, ainsi que sur des pratiques exemplaires qui permettent d'atténuer les biais, de renforcer les mécanismes redditionnels, d'aborder les enjeux éthiques et d'améliorer la confiance du public à l'égard du traitement des données par les organismes gouvernementaux. Nous avons compilé et examiné plusieurs ressources du milieu universitaire, du secteur public et de la société civile, et nous intégrerons les conclusions pertinentes de notre analyse dans les sections subséquentes.

Nous avons réalisé 16 entrevues semi-structurées avec des répondants issus du milieu universitaire, d'organisations communautaires, ainsi que de ministères et d'organismes fédéraux. Les entrevues, d'une durée maximale de 60 minutes, ont eu lieu virtuellement. Un chargé d'entrevue principal, un chargé d'entrevue secondaire et deux preneurs de notes étaient désignés pour chaque entrevue. Les membres de notre équipe de projet ont assumé ces fonctions à tour de rôle.

Pour commencer, nous avons passé en revue les notes prises lors des entrevues. Ensuite, nous avons analysé nos résultats au moyen d'un processus d'analyse thématique. La première étape consistait à revoir chacune des notes en indiquant nos observations préliminaires, notre interprétation et nos suggestions. À la deuxième étape, nous avons commencé à dégager les tendances et à regrouper les notes selon des thèmes généraux. Par la suite, nous avons affiné les thèmes et compilé nos résultats. Nous avons intégré les thèmes à l'analyse qui figure dans notre rapport de façon à mettre en lumière les enjeux clés, les répercussions, les possibilités, ainsi que les pratiques exemplaires en ce qui concerne le problème des biais dans la gestion des données au sein des organismes responsables de la sécurité nationale.

Nous avons utilisé le cadre d'analyse ci-dessous tout au long de notre processus de recherche.

Enjeux émergents vs enjeux endémiques

Lors de l'élaboration des questions de recherche, nous avons fait une distinction entre les questions structurelles générales touchant les pratiques de gestion des données et ayant une influence sur les biais de données et celles qui pourraient être jugées plus actuelles ou importantes. Pour faciliter cette distinction, nous employons les termes « enjeux émergents » et « enjeux endémiques ». Les « enjeux émergents » sont ceux qui, dans le secteur de la sécurité nationale, sont jugés les plus urgents et sont liés au nouveau contexte de la menace. En revanche, les « enjeux endémiques » désignent les enjeux systémiques à long terme qui sont présents non seulement dans le secteur de la sécurité nationale, mais aussi dans la société en général. Cette terminologie nous permet de mieux cerner les causes profondes des biais dans la gestion des données, de formuler des recommandations réalisables à l'intention du SCRS et d'en arriver à une compréhension globale du problème dans le secteur de la sécurité nationale.

CONSTATATIONS, ANALYSE ET RECOMMANDATIONS

Définition des biais et détermination des groupes touchés

« Ce qui caractérise les services de renseignement, c'est que les biais font partie de leurs activités. En effet, ces services s'intéressent précisément aux caractéristiques qui peuvent leur permettre d'empêcher des personnes de subir des préjudices. »

Ces propos de l'un des répondants résument ce qui rend cette question de biais si difficile à résoudre. D'après ce répondant, les services de renseignement s'efforcent de dégager les tendances et traitent celles qui se répètent comme des biais. Ainsi, on peut se demander si les activités de renseignement peuvent être exemptes de biais alors que c'est justement parce qu'elles sont biaisées qu'elles peuvent empêcher des personnes de subir des préjudices. Comme plusieurs sources nous l'ont indiqué, l'élimination complète des biais de données est peut-être impossible. Nous avons plutôt mis l'accent sur la façon dont nous pouvons réexaminer les pratiques de gestion des données pour comprendre comment elles peuvent causer des préjudices et à qui ces préjudices sont causés, et apprendre comment en atténuer les répercussions. Pour comprendre de façon générale la façon dont les biais se manifestent dans la gestion des données et utiliser des pratiques de gouvernance qui en atténuent efficacement les répercussions, il faut déterminer précisément à quelle étape ils surviennent dans le cycle de vie des données (processus en amont et en aval). Pour répondre à ces questions, nous avons interrogé un large éventail d'intervenants qui ont des connaissances sur les biais de données du point de vue conceptuel et expérimentiel. De notre point de vue, il fallait entamer une analyse qui va au-delà d'un

quelconque manuel des biais dans la gestion des données, en s'inspirant des travaux sur la justice conceptionnelle réalisés par Sasha Chock, Ph.D., qui souligne que le contexte dans lequel les chercheurs posent ce type de questions influe grandement sur le type de réponses qu'ils obtiennent.

Qu'entend-on par « biais de données »?

Il y a un biais de données quand des préjugés subjectifs concernant, entre autres, la race et le genre sont ancrés dans la collecte et l'utilisation des données. Les biais de données peuvent être de niveau individuel et institutionnel. Sur le plan individuel, les personnes qui manipulent des données peuvent, par exemple, avoir des préjugés à l'égard de certains groupes, ce qui influe sur la façon dont elles traitent les données. Au niveau institutionnel, les politiques et les pratiques de gestion des données des organismes et des organisations reflètent parfois des préjugés sociaux. La gestion des données comprend une série de tâches distinctes, et chacune d'entre elles soulève de nouvelles questions sur la façon dont les biais se manifestent lorsque des organismes publics utilisent des données, ainsi que sur les risques de préjudices pour les communautés marginalisées. Nous pouvons ainsi observer la façon dont les biais de données peuvent perpétuer des inégalités structurelles par rapport à des groupes marginalisés de longue date lorsque les biais sont présents au niveau à la fois individuel et institutionnel.

Il existe une croyance populaire qui veut que les données soient neutres et objectives. Cette croyance n'est plus de mise. Il est maintenant reconnu que les données doivent être interprétées dans un contexte donné et qu'elles sont sujettes à des biais. D'après une analyse documentaire, les biais de données peuvent être définis de deux façons. Tout d'abord, en statistique, le biais dans les données provient d'une représentation inexacte d'une population ou d'une étude. Il peut s'agir de données qui n'incluent pas de variables qui rendent compte de manière exacte du phénomène prédit, ou de données produites par des humains qui peuvent contenir des préjugés contre des groupes de personnes (Lopez, 2021). Dans les deux cas, il peut y avoir des répercussions et des préjudices inattendus. L'un des répondants a décrit les biais de la façon suivante : « Il s'agit essentiellement de la différence dans le traitement de personnes ou de situations, de groupes ou de secteurs, en fonction des caractéristiques distinctives de chacun. »

Conséquences des biais de données

L'un des répondants a souligné qu'il importe de sensibiliser le personnel chargé de la sécurité nationale à la façon dont des biais de données peuvent influer sur leurs conclusions. Par exemple, un

répondant a déclaré que les femmes n'ont été prises en compte lors de l'analyse des menaces terroristes ou des menaces à caractère idéologique qu'à compter de 2013-2014.

Dans le secteur de la sécurité nationale, les biais de données se reflètent notamment dans la surveillance policière excessive dont font l'objet certains groupes. Dans le cadre du Programme de protection des passagers du Canada, lequel vise à empêcher des personnes qui représentent une menace pour la sécurité aérienne de monter à bord d'un avion (gouvernement du Canada, 2021), on estime que plus de 100 000 Canadiens sont susceptibles de subir des préjudices non intentionnels à la suite d'un contrôle. Ces personnes peuvent en effet se voir interdire l'embarquement parce qu'elles portent le même nom qu'une personne inscrite sur la liste d'interdiction de vol (Enfants inscrits sur la liste d'interdiction de vol, 2017).

Dans le contexte démocratique occidental, comme beaucoup de documents en témoignent, les organismes d'application de la loi et de sécurité causent des préjudices disproportionnés à des communautés marginalisées et à des gens de couleur en raison de certaines pratiques, comme la surveillance excessive, la détention et la violation des droits constitutionnels. La situation ne date pas d'hier. Bien que les pratiques soient aujourd'hui plus équitables et progressistes qu'elles ne l'étaient par le passé, ces groupes courent toujours un risque disproportionné de subir des préjudices en raison de discrimination structurelle persistante et de préjugés profondément enracinés dans les systèmes institutionnels des organismes de sécurité publique et de sécurité nationale.

En ce qui concerne les biais liés à la race ou à l'ethnicité, par exemple, les entrevues ont fait ressortir un sentiment commun parmi les répondants. En effet, selon ces derniers, les membres des communautés noires et brunes sont souvent pris pour cible par les organismes d'application de la loi et de sécurité en raison d'idées préconçues au sujet, notamment, de leur implication dans des activités criminelles ou terroristes. Au Canada, les membres des communautés noires et autochtones et d'autres communautés racialisées risquent davantage de faire l'objet de profilage racial et d'être interrogés par des policiers. Ils sont également plus susceptibles d'être inscrits dans des banques de données contenant les noms d'individus soupçonnés d'affiliation à un gang ou de personnes d'intérêt, ce qui augmente arbitrairement la probabilité d'une arrestation ou d'une détention en lien avec une activité criminelle soupçonnée (Robertson, Khoo et Song, 2020). Dans d'autres pays démocratiques, dont le Royaume-Uni, l'adoption de nouvelles mesures législatives antiterroristes après les événements du 11 septembre et les attentats du 7 juillet a mené au resserrement de la surveillance dont font l'objet les musulmans et les Sud-Asiatiques britanniques ainsi qu'à l'augmentation de la collecte de

renseignements à leur sujet. Ces nouvelles mesures ont eu pour effet de renforcer la discrimination, la marginalisation et la victimisation de ces communautés (Mythen, Walklate et Khan, 2009). De telles tendances sont préjudiciables aux groupes racialisés, car elles contribuent à propager les perceptions négatives à leur égard. Comme un répondant l'a mentionné, plus ces communautés sont prises pour cible par les services de police et les organismes de sécurité, plus elles risquent d'être perçues comme étant intrinsèquement malintentionnées et suspectes, ce qui a pour effet de les marginaliser davantage.

Les membres de groupes communautaires qui s'identifient comme des personnes de couleur estiment également que les données biaisées ont une incidence sur l'accès à certaines ressources. Par exemple, en Colombie-Britannique, l'aide financière offerte à la communauté noire n'était pas suffisante pour compenser les effets de la pandémie. Le fait de considérer les groupes marginalisés comme un tout homogène compromet l'efficacité des services. Au sein même d'un groupe, les membres risquent d'être marginalisés encore davantage en fonction d'autres indicateurs d'identité tels que l'invalidité, l'orientation sexuelle et la monoparentalité. Les écarts dans la collecte de données désagrégées, comme le montre cet exemple précis, indiquent comment la collecte de telles données crée un effacement systémique. Une marginalisation semblable fait ressortir l'existence d'un problème endémique, à savoir que l'affectation systémique des ressources ne permet pas aux communautés de couleur de recevoir leur juste part.

Cycle de vie des données

Il est essentiel de déterminer comment les biais s'immiscent dans les pratiques de gestion des données et d'établir les conséquences qui en découlent dans le secteur de la sécurité nationale. L'adoption d'une approche axée sur le cycle de vie des données nous permet d'établir à quel moment les biais s'immiscent dans les pratiques et de comprendre que ces technologies sont mises à la disposition des utilisateurs et que leur utilisation est sujette aux biais et aux hypothèses.

ÉTAPE	DÉFINITION	RISQUES	EXEMPLES

Planification	Processus décisionnel pour orienter la collecte et l'exploitation des données.	À cette étape, le manque de consultation avec des communautés externes accroît le risque de perpétuer des résultats préjudiciables pour les étapes en aval. En effet, compte tenu de l'absence de perspectives externes, il est impossible de corriger les biais au sein de l'organisation et de ses dirigeants.	Les membres de différentes communautés (noires, autochtones, sud-asiatiques, etc.) qui font depuis longtemps les frais des technologies axées sur les données indiquent souvent qu'ils ignorent que les organismes de sécurité ou de renseignement recueillent des renseignements à leur sujet ou qu'ils n'y ont pas consenti.
Collecte	Collecte et analyse systématiques de données sur les variables d'intérêt pour évaluer et prévoir les résultats.	Les méthodes utilisées pour recueillir les données (analyse des médias sociaux, reconnaissance faciale, données biométriques, etc.) peuvent donner lieu à des biais et, par conséquent, faire en sorte que divers groupes soient surreprésentés ou sous-représentés dans les bases de données.	Les organismes de sécurité qui exploitent des technologies de surveillance les déploient rarement de façon uniforme, car ils visent principalement les communautés de couleur qui, selon eux, sont susceptibles de représenter une menace. Les membres des communautés de couleur sont plus susceptibles d'être fichés par des services de police. Ces communautés font ainsi l'objet d'une surveillance policière excessive et de mesures de sécurité disproportionnées.
Traitement	Processus de traitement de données qui consiste à transformer des données brutes en données exploitables.	À ce stade, les biais peuvent mener à une interprétation ou à une représentation erronée des données recueillies auprès des communautés. Lorsque les données sont exploitées, les biais peuvent aussi entraîner des mesures préjudiciables contre ces communautés.	Les corrélations stéréotypées et les préjugés sociaux liés notamment à la race et au genre influent souvent sur le traitement des données brutes. Par exemple, les données recueillies auprès des communautés noires ou brunes sont plus susceptibles d'être mises en corrélation avec des activités d'un gang ou des activités terroristes.

Analyse	Étude des données en vue d'en tirer des conclusions pour orienter l'élaboration des politiques.	Les biais individuels ou institutionnels peuvent mener à des interprétations subjectives des données par rapport à divers groupes sociaux et causer des préjudices de façon disproportionnée ou exacerber les inégalités.	Lorsque le gouvernement et des organismes de sécurité élaborent des politiques en matière de sécurité nationale ou de lutte contre la criminalité, ils visent souvent des communautés de couleur en se fondant sur des informations subjectives selon lesquelles ces communautés sont plus susceptibles d'adopter des comportements criminels. Il peut s'agir, par exemple de politiques de lutte antidrogue ou de restrictions en matière d'immigration.
Application	Exploitation des données dans des technologies de pointe ou d'autres applications.	Lorsqu'elles sont utilisées sur le terrain, les technologies alimentées au moyen de données biaisées peuvent causer des préjudices aux communautés.	Il a été démontré que les technologies de lecture biométrique et de reconnaissance faciale utilisées dans les aéroports associent les voyageurs de couleur à un risque éventuel.
Conservation	Protocole mis en place au sein d'une organisation pour assurer la conservation des données pendant une période déterminée aux fins de conformité opérationnelle ou réglementaire.	Plus les données sont conservées longtemps, plus elles risquent d'être compromises et d'être réutilisées dans des applications à des fins autres que celles pour lesquelles elles ont été recueillies. Le problème touche surtout les communautés marginalisées qui communiquent des données à des organismes gouvernementaux sans savoir de quelle façon et à quelles fins leurs données peuvent être utilisées à l'interne.	Des institutions et des organismes recueillent souvent des données auprès de communautés marginalisées sans leur indiquer pendant combien de temps les données seront conservées ni qui y aura accès. Cette situation a mené à des violations de la vie privée et a causé des préjudices aux membres de communautés marginalisées, notamment lorsque des données sensibles ont été rendues publiques dans le cadre de demandes d'accès à l'information.

1. Rôle de la reddition de comptes dans la gestion des données : dimensions internes et externes

Un thème clé qui est ressorti de nos recherches et des entrevues menées sur le terrain est l'importance de la reddition de comptes liée à la collecte et à l'utilisation des données par les services de renseignement. La reddition de comptes liée à la gestion des données s'applique tant à l'interne, dans la structure de l'organisation, qu'à l'externe, en vertu des diverses obligations de l'organisation à l'égard des membres du public dont elle recueille les données personnelles. La reddition de comptes englobe également une notion de transparence quant à la façon dont l'organisation communique des informations au sujet des données recueillies, à la manière dont les données sont exploitées et aux répercussions découlant de leur utilisation. L'adoption de mesures de reddition de comptes efficaces contribue à atténuer la présence de biais et les risques de préjudice découlant de la collecte et de l'utilisation des données, et ce, en contribuant à prévenir l'exploitation des données et à améliorer la qualité des données. Qui plus est, de telles mesures incitent à évaluer soigneusement les risques ou les préjudices pouvant découler de décisions fondées sur les données. Des normes élevées en matière de reddition de comptes et de transparence contribuent en outre à renforcer la confiance du public quant à la capacité des organismes gouvernementaux de traiter les données de façon responsable et éthique et conformément aux principes démocratiques. En l'absence de normes élevées, les citoyens des pays démocratiques sont peu enclins à faire confiance aux organismes gouvernementaux qui ont des données personnelles en leur possession parce qu'ils ne comprennent pas les processus décisionnels entourant la collecte et l'utilisation de leurs renseignements personnels et n'ont pas l'impression d'y avoir consenti. En pareil cas, le public peut se sentir méfiant ou en danger, particulièrement à l'égard des organismes qui mènent des activités de surveillance et qui, tout dépendant de la façon dont ils utilisent leurs données, peuvent causer des préjudices (Parsons, 2020). Lors d'une entrevue, un représentant du SCRS a affirmé que l'organisation devrait avoir un contrat social clair avec la population canadienne. Il a ajouté que ce contrat devrait préciser la façon dont le SCRS collecte les données personnelles ou privées, les pouvoirs qui lui sont conférés à cet égard, ainsi que la manière dont il conserve ou détruit les données. Les propos de ce représentant du SCRS mettent en lumière la volonté de l'organisation de rendre davantage de comptes à la population canadienne et, pour ce faire, de mieux l'informer de la façon dont il utilise les données personnelles, des mesures qui auront pour effet de renforcer la confiance du public.

Le gouvernement du Canada a mis en place de bonnes pratiques en matière de reddition de comptes interne pour régir l'utilisation des données par les organismes publics. Ainsi, il a adopté des dispositions

législatives (*Loi sur la protection des renseignements personnels*, *Loi sur le SCRS,* etc.), créé des organismes de surveillance et mis au point des évaluations de l'incidence algorithmique. Toutefois, les enjeux endémiques englobent la mise en œuvre officielle d'une évaluation du niveau de risque dans les organismes de sécurité, comme le SCRS, pour régir l'utilisation des technologies nouvelles et émergentes, ainsi que le manque de transparence auprès du public concernant les processus et les mesures de protection qui régissent l'utilisation des données.

Reddition de comptes auprès du public en ce qui a trait à la gestion des données : Le cas de l'Estonie

Le gouvernement de l'Estonie peut être considéré comme un cas type qui met en lumière non seulement l'utilité d'adopter des mesures de reddition de comptes efficaces à l'interne pour régir l'utilisation des données, mais aussi la mesure dans laquelle les pratiques axées sur la transparence et la consultation publique favorisent l'utilisation éthique des données et la confiance du public envers les organismes publics. Dans la foulée d'une série de cyberattaques contre l'infrastructure d'information publique, le gouvernement a créé l'« Estonian Information System Authority » afin de s'assurer que les ministères appliquent les mêmes pratiques de sécurité des données. Ces pratiques comprennent l'« Estonian Information Security Standard », une norme obligatoire en matière de sécurité de l'information qui vise à assurer que tous les ministères disposent d'un système de protection de base des données (Republic of Estonia Information System Authority, 2022). Le gouvernement de l'Estonie a également déployé des efforts concertés pour faire preuve de transparence et informer le public au sujet de la portée des cyberattaques contre son infrastructure d'information et de la rétroaction des citoyens concernant les mesures visant à améliorer la sécurité de leurs données. Ces efforts combinés ont permis d'améliorer la cohésion des normes en matière de reddition de comptes au sein du gouvernement et de renforcer la confiance de la population à l'égard de la gestion des données et des processus de gouvernance du gouvernement (Priisalu et Ottis, 2017).

Mécanismes internes de reddition de comptes : cadres juridiques et techniques

Les organismes publics qui traitent des données doivent nécessairement se doter de mécanismes de reddition de comptes interne compte tenu de la vitesse à laquelle les données recueillies se complexifient et de la prolifération des technologies de pointe, des méthodes et des outils axés sur les données. Ces mécanismes sont particulièrement importants pour les organismes de sécurité étant donné la nature sensible des données qu'ils traitent et le rôle qu'ils remplissent, à savoir anticiper et contrer les menaces pour la population et la sécurité nationale. Sous l'angle des enjeux endémiques, à mesure que les technologies axées sur les données telles que l'intelligence artificielle et l'apprentissage machine

gagnent en complexité, le risque de préjudices découlant de l'utilisation de ces technologies s'accroît. Par exemple, un répondant d'un groupe de réflexion universitaire a souligné que le risque de contamination des ensembles de données dans le secteur de la sécurité nationale peut avoir une incidence sur la façon dont sont utilisés les systèmes de défense reposant sur l'intelligence artificielle ou l'apprentissage machine. Une telle contamination peut entraîner des conséquences graves, surtout lorsque ces systèmes sont déployés à grande échelle. Ainsi, il importe que les organismes de sécurité respectent en tout temps les mécanismes internes de reddition de comptes qui favorisent la mise en œuvre de pratiques responsables, éthiques et légales en matière de gestion de données afin de prévenir les préjudices non intentionnels.

Les mécanismes internes de reddition de comptes liés à la gestion des données par les organismes de sécurité comportent habituellement l'utilisation de cadres juridiques et techniques pour réglementer certains facteurs tels que la quantité et le type de données que ces organismes peuvent recueillir, les sources auprès desquelles ils peuvent recueillir des données et les risques liés à l'utilisation de ces données. La *Loi sur le SCRS* stipule les obligations redditionnelles du Service concernant ses pratiques de gestion des données, par exemple la nécessité d'obtenir une autorisation judiciaire pour conserver des ensembles de données canadiens (article 11) et de s'assurer que les mesures prises par le Service pour faire face aux menaces sont « justes et adaptées aux circonstances » et ne causent pas de préjudice inutile à des tiers ou ne portent pas atteinte à leur droit à la vie privée (article 12) (site Web de la législation, 2022).

À mesure que les organismes de sécurité comme le SCRS amélioreront leur capacité de collecte de données en misant sur des technologies émergentes, il faudra se pencher sur les enjeux endémiques et, par exemple, trouver des moyens d'assurer le respect de la vie privée des communautés au Canada. Il faudra notamment établir des façons de garantir le respect des protections que la loi confère aux membres du public. Aux termes de la *Loi sur la protection des renseignements personnels*, les organismes gouvernementaux sont tenus de respecter la vie privée des Canadiens, par exemple en évitant de recueillir des renseignements personnels de façon systématique. Le commissaire à la protection de la vie privée, qui est nommé par le Parlement, veille également à ce les institutions gouvernementales respectent la *Loi sur la protection des renseignements personnels* (Commissariat à la protection de la vie privée, 2015).

L'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR) a mis en place un mécanisme interne de reddition de comptes concernant l'utilisation de données par les organismes responsables de la sécurité nationale au Canada. L'OSSNR a le mandat d'inspecter les activités

du SCRS et du Centre de la sécurité des télécommunications (CST), ainsi que les activités liées à la sécurité nationale et au renseignement de tous les autres ministères et organismes fédéraux. Pour remplir ses fonctions, l'OSSNR a librement accès aux informations classifiées des organismes dont les activités font l'objet d'une surveillance. En vertu des pouvoirs que lui confère la *Loi sur l'OSSNR*, l'Office a librement accès aux informations et mène des vérifications indépendantes (NSIRA, s.d.). L'OSSNR mène des activités de surveillance concernant divers aspects du travail du SCRS : mesures de réduction de la menace, relation avec les services de police lors de la tenue d'enquêtes, rôle de la Direction de la sécurité interne, etc. En 2019, l'OSSNR a publié les résultats d'une vérification portant sur l'utilisation de données de géolocalisation par le SCRS et a souligné un risque de violation de l'article 8 de la *Charte* en ce qui a trait aux perquisitions et aux saisies abusives (OSSNR, 2019). Pour atténuer ce risque, l'OSSNR a recommandé que les organismes de sécurité bénéficient d'un soutien juridique continu de la part du ministère de la Justice pour s'assurer qu'ils se conforment à la loi lorsqu'ils utilisent, entre autres, des technologies visant à recueillir des données de géolocalisation. Il a également recommandé d'élaborer une politique exigeant une évaluation du risque « dans des situations […] où des informations recueillies au moyen de technologies nouvelles et émergentes peuvent contenir des renseignements pour lesquels il peut exister une attente raisonnable en matière de protection de la vie privée » (OSSNR, 2019, p.16).

Le gouvernement du Canada oblige également les organismes gouvernementaux à avoir recours à un outil d'évaluation de l'incidence algorithmique (EIA) lorsqu'ils utilisent des systèmes automatisés de prise de décisions. L'EIA aide les organismes publics à évaluer les risques et à déterminer, à court et à long terme, les répercussions éventuelles des systèmes automatisés. Une telle évaluation est particulièrement utile pour cerner et atténuer les biais dans les processus de gestion des données, car elle fournit aux organismes un cadre qui leur permet d'évaluer le risque que la collecte et l'utilisation de données de différentes communautés entraînent des résultats préjudiciables (Reisman et al., 2018). L'EIA exige notamment des organismes qu'ils réalisent un examen auprès de tiers (membres du public) afin de recueillir leurs commentaires sur la conception et le fonctionnement des systèmes automatisés. L'outil d'EIA du gouvernement canadien, créé par le Conseil du Trésor, contient des questions concernant, par exemple, le profil de risque, le processus décisionnel et la nature des données utilisées dans les systèmes automatisés (gouvernement du Canada, 2021). Lors d'une entrevue, un représentant du Conseil du Trésor a mentionné que l'une des principales faiblesses de l'outil d'EIA est sa portée, c'est-à-dire que, pour le moment, l'outil ne s'applique qu'au processus décisionnel administratif au sein du gouvernement. Par conséquent, l'outil n'est d'aucune utilité actuellement lorsqu'il s'agit de la collecte de données par des organismes comme le SCRS ou l'utilisation de l'intelligence artificielle pour orienter les politiques.

Cependant, le Conseil du Trésor est prêt à fournir un soutien technique et financier aux ministères qui souhaitent intégrer l'EIA à leurs activités.

Mécanismes externes de reddition de comptes : transparence, examen externe et renforcement de la confiance du public

Les mécanismes externes de reddition de comptes concernant la gestion des données englobent la notion de transparence. En effet, les organismes publics doivent révéler comment ils recueillent, utilisent et protègent les données personnelles et privées. Il peut aussi s'agir de mesures permettant au public de consentir à l'utilisation de leurs données, ainsi que de boucles de rétroaction grâce auxquelles les intervenants peuvent formuler des commentaires sur les processus de gestion interne des données par les organismes publics. Ces facteurs contribuent collectivement à favoriser la confiance du public à l'égard de l'utilisation des données personnelles par les organismes gouvernementaux. En ce qui concerne la question du consentement, le Commissariat à la protection de la vie privée du Canada (CPVP) a déclaré que « les organisations doivent généralement obtenir un consentement valable pour la collecte, l'utilisation et la communication de renseignements personnels » (Commissariat à la protection de la vie privée du Canada, 2021). Le CPVP a également énoncé des principes en matière de consentement que les organismes doivent respecter en vertu de différentes lois, dont la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE). L'une des recommandations clés liées à ces principes est la suivante : les organismes devraient toujours être en mesure de démontrer qu'ils respectent les mesures de reddition de comptes, telles que les normes de consentement, en réponse aux demandes d'information des organismes de réglementation ou du grand public. Le CPVP explique également l'importance du consentement compte tenu de la nature sensible de certaines catégories de renseignements personnels et des risques découlant de leur utilisation par des organismes; il peut notamment s'agir de renseignements liés aux origines ethniques ou raciales d'une personne, à ses opinions politiques, à ses données génétiques et biométriques, à son orientation sexuelle et à ses croyances religieuses. Compte tenu du niveau de confidentialité que le SCRS requiert dans le cadre de ses opérations, il est difficile d'obtenir un consentement exprès pour la collecte de données. Or, il peut tout de même être utile pour le SCRS de trouver des moyens d'engager le dialogue avec différentes communautés en tenant des processus de consultation publique et en expliquant ouvertement aux membres de la population comment il protège leurs données.

La prise de mesures qui favorisent un examen externe des processus, des outils et des méthodes de gestion des données peut également contribuer à réduire les biais, tout particulièrement lorsque la

rétroaction provient des groupes qui sont plus à risque de subir de préjudices découlant de l'utilisation de leurs données par des organismes publics. À ce sujet, le secteur de la sécurité nationale occupe une place unique compte tenu des attentes que ses activités suscitent en matière de confidentialité. Cependant, un manque de transparence et d'engagement envers différentes communautés sur le plan de la collecte et de l'utilisation des données par un service de renseignement peut miner la confiance du public quant à la capacité de ce service à traiter les données de manière responsable. En 2020, le CPVP a commandé un sondage pour savoir ce que les Canadiens pensent des enjeux liés à la protection de la vie privée. Le sondage a révélé que 53 % des Canadiens estiment que le gouvernement ne devrait pas avoir le droit de recueillir des informations personnelles dans le cadre de ses activités de renseignement. Par ailleurs, 59 % des Canadiens ont indiqué qu'ils n'accepteraient pas de renoncer, même en partie, à la protection de leur vie privée pour permettre au gouvernement de mener des activités de renseignement (commissaire à la protection de la vie privée, 2020). Ces résultats mettent en évidence le niveau extrêmement élevé de méfiance du public à l'égard des pratiques utilisées par les organismes de sécurité du Canada pour traiter les données. Dans ce cas, il est également utile d'examiner les enjeux émergents pour comprendre les résultats. Pour assurer leur légitimité, les organismes de sécurité devront redoubler d'efforts pour gagner la confiance de la population canadienne puisqu'ils continuent de se servir de méthodes sophistiquées pour recueillir et traiter les données, et ce, afin de contrer les menaces en constante évolution qui pèsent sur la sécurité nationale.

Une importance excessive accordée à la confidentialité, surtout lorsque les raisons sous-jacentes ne sont pas clairement définies, nuit à la relation entre les organismes de sécurité et les communautés qu'ils servent et protègent. Lors des entrevues, des répondants ont indiqué que les gens s'attendent au pire lorsqu'ils ne disposent pas de renseignements suffisants. Selon eux, le fait d'omettre de communiquer des renseignements en raison de préoccupations liées à la protection de la vie privée ou de transmettre des données superficielles sans contexte a pour effet de susciter d'autres questions.

En outre, des répondants ont ajouté que les organismes responsables de la sécurité nationale devraient être plus ouverts à l'idée que des intervenants externes procèdent à un examen de leurs activités et que les résultats soient rendus publics sous forme de synthèse au lieu de bénéficier d'une exemption générale. L'un des répondants a évoqué l'image suivante : au lieu d'entourer leurs activités d'un mur opaque, les organismes responsables de la sécurité nationale pourraient les entourer de fenêtres et de portes pour favoriser la transparence. Des représentants du SCRS partagent cet avis. Ces personnes ont mentionné qu'un certain nombre d'employés sont favorables à l'idée d'accroître la

transparence et de communiquer de plus amples renseignements au public afin de montrer que l'organisme utilise les données de façon responsable. Par ailleurs, plusieurs répondants ont affirmé que les organismes responsables de la sécurité nationale, comme le SCRS, doivent préserver un certain niveau de confidentialité en ce qui concerne les données qu'ils recueillent afin de protéger la vie privée et la sécurité de la population canadienne. Cependant, une solution de compromis consisterait à examiner comment le SCRS peut faire preuve d'une plus grande transparence concernant les politiques et les processus qui orientent la collecte et l'utilisation des données.

L'une des solutions que le SCRS pourrait envisager pour accroître la transparence de ses politiques et de ses processus en matière de gestion de données consisterait à permettre à des intervenants externes issus de diverses communautés de procéder à la vérification de ses systèmes, de ses outils et de ses méthodes internes. Pour éviter les risques éventuels, comme les atteintes à la vie privée ou à la confidentialité, les canaux de vérification pourraient être axés essentiellement sur les étapes en amont de la gestion des données, telles que les processus décisionnels qui déterminent comment les données sont recueillies et utilisées, plutôt que sur la teneur des données elles-mêmes. Dans le cadre des entrevues, plusieurs employés du SCRS et intervenants externes se sont dits favorables à l'augmentation du nombre de vérifications externes des processus qui sous-tendent la collecte de données au sein du Service pour renforcer le système de gouvernance des données.

Encourager la population à signaler les préjudices pouvant être causés par les nouvelles technologies

Aux États-Unis, une boîte à outils pour l'équité algorithmique, connue sous le nom d'Algorithmic Equity Toolkit ou AEkit, a été élaborée dans le cadre d'un processus de conception participative auquel ont pris part des intervenants d'organisations et d'établissements universitaires, comme l'American Civil Liberties Union de Washington, la Digital Life Initiative de l'Université de Cornell University et la School of Information de l'Université du Michigan. La boîte à outils constitue un cadre qui aide les membres de la communauté à déterminer si une technologie donnée repose sur l'intelligence artificielle et à analyser les risques de préjudice algorithmique et de biais dans le système.

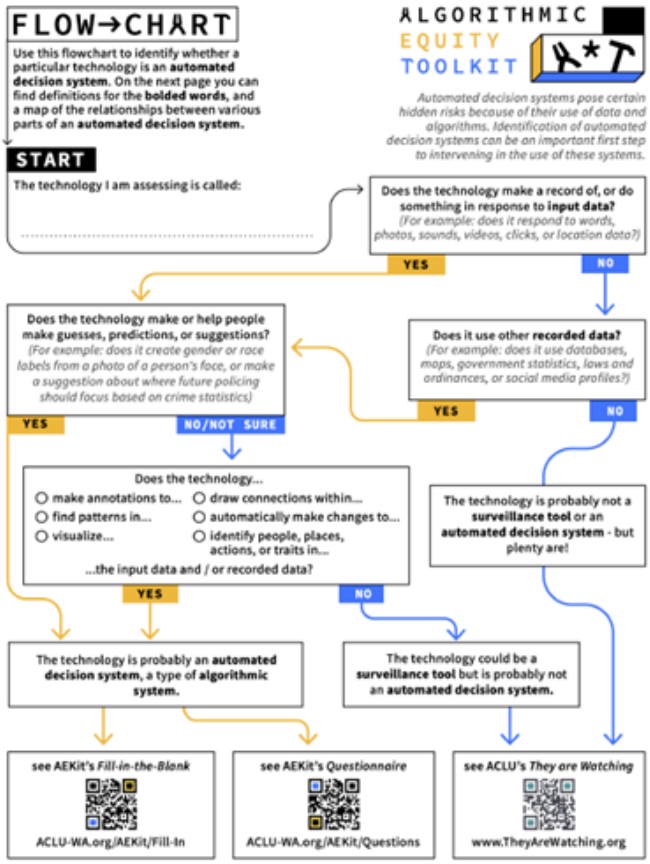

Figure 2. Diagramme de l'AEKit

De par sa souplesse, la boîte à outils incite les utilisateurs à cerner les préjudices potentiels non seulement dans les technologies utilisées par les organismes d'application de la loi ou de sécurité, mais aussi dans celles qui sont utilisées, entre autres, dans les secteurs du transport et du logement (Krafft et al., 2021). L'adoption d'outils tels que l'AEKit a présente un double avantage : d'un côté, elle permet aux communautés de mieux se protéger contre des préjudices éventuels et, de l'autre, elle aide les organismes publics à utiliser des technologies axées sur les données de manière plus éthique. En outre, en recourant à une telle forme de mobilisation publique pour guider leurs pratiques de gestion de données, les organismes gouvernementaux renforcent leurs mesures de transparence et de reddition de comptes externe et améliorent la confiance du public.

Sommaire des recommandations

- Renforcer les obligations redditionnelles internes en mettant en œuvre un processus global d'évaluation des risques semblable à l'outil d'EIA pour régir la collecte et l'utilisation de données, tout particulièrement lorsqu'il s'agit de technologies nouvelles et émergentes.
- Renforcer la reddition de comptes externe et la transparence en communiquant au public davantage d'informations portant notamment sur les politiques applicables à la collecte d'informations personnelles ou privées par le SCRS, les règles concernant l'utilisation des données et les résultats que l'utilisation de ces données permettent d'obtenir.
- Chercher des moyens par lesquels différentes communautés pourraient procéder à une vérification plus poussée des processus relatifs à l'utilisation des données par le SCRS, et ce, au moyen de consultations et d'outils tels que l'Algorithmic Equity Toolkit.

2. Processus d'apprentissage : changement de culture et alphabétisation numérique

Pour atténuer les biais dans la gestion des données, il important d'instaurer une culture organisationnelle interne qui reconnaît les répercussions des biais sur les communautés marginalisées et qui intègre des pratiques d'atténuation de ces biais dans le perfectionnement des compétences en alphabétisation numérique. Nous reconnaissons que les principaux enjeux émergents liés à la gestion des données peuvent avoir un effet unificateur sur les intervenants ou favoriser la mise en place de nouveaux processus d'apprentissage. Si ces enjeux ne se fondent pas sur une compréhension des problèmes endémiques, leur application pourrait être de courte durée et leur incidence sur la culture organisationnelle, de faible envergure. Il faut adopter une approche à long terme pour aborder ces enjeux. Par ailleurs, la compréhension des enjeux endémiques liés aux biais de données permet aux organismes de reconnaître les possibilités de changement organisationnel.

Lors du travail effectué sur le terrain, nous avons mis l'accent sur les façons de se renseigner sur les biais, les moyens de les comprendre et les stratégies visant à les atténuer. Nous savions que les biais étaient définis de différentes façons. À titre d'exemple, un répondant préférait utiliser le terme « écart de rendement » au lieu de « biais », qui met en évidence la nature humaine plutôt que l'aspect technique.

Cette volonté de faire une distinction entre les humains et la technologie suppose deux différentes façons de comprendre d'où viennent les biais de données. Par conséquent, nous jugeons qu'il est important d'examiner de façon plus approfondie la façon dont les gens ont développé leur compréhension des biais et de tâcher d'établir le lien avec la gestion des données. Nous avons cherché les principaux moyens de favoriser la compréhension des biais et avons établi un lien avec les efforts actuellement déployés par le SCRS pour améliorer la diversité, l'équité et l'inclusion.

Voici les trois principaux moyens que nous avons retenus.

Résurgence des initiatives de diversité, d'équité et d'inclusion en raison d'événements politiques importants

Les personnes issues de communautés marginalisées qui ont été rencontrées en entrevue ont associé les questions relatives aux biais de données à des enjeux endémiques et ont affirmé que la prise de conscience sociale de 2020 aurait dû survenir il y a longtemps. Il serait fort utile d'exploiter cette vision à long terme dans la conception des processus d'apprentissage liés aux biais de données.

L'analyse des répercussions de 2020 du point de vue des enjeux émergents montre comment le rôle prépondérant de la sphère politique pendant cette période a mis à l'avant-plan la marginalisation de la communauté noire. Ce qui est préoccupant, toutefois, c'est que cela laisse croire que le débat sur les biais raciaux dans les données a commencé à un moment précis, alors que les communautés avec lesquelles nous nous sommes entretenus ne considèrent pas ce moment comme le point de départ. Dans son ouvrage *Design Justice*, Sasha Chock examine comment les discours relatifs aux mouvements sociaux influent sur les processus de conception et fait remarquer que la formulation du problème représente l'un des principaux résultats de l'interaction entre ces concepts (Constanza-Chock, 2020). Le fait de considérer la prise de conscience de 2020 comme un événement ponctuel sans reconnaître qu'elle témoigne d'une marginalisation endémique à long terme peut changer notre perspective quant à l'importance du problème. Par exemple, si les enjeux relatifs à la marginalisation sont jugés endémiques, les intervenants concernés peuvent décider d'approfondir leur enquête sur les processus de gestion des données et les d'atténuation des biais.

Lors des entrevues, cinq répondants sur seize ont indiqué que la prise de conscience raciale de 2020 ou l'affaire George Floyd avait incité leur organisme ou ministère à effectuer des changements pour remédier aux problèmes d'équité et d'inclusion. Lors d'une entrevue, un formateur en ACS+ a mentionné que la même tendance était observée dans la formation tenant compte des genres et a expliqué qu'il y avait eu

un regain d'intérêt à l'égard de l'ACS+ après 2020, même s'il s'agissait déjà d'un outil exigé par le gouvernement. À notre avis, d'un point de vue politique, il s'agissait du moment tout indiqué pour réexaminer comment les biais de données intensifient la marginalisation. Il est impératif que les connaissances acquises sur les communautés marginalisées de longue date soient utilisées dans la conception du processus de gestion des données dans le secteur de la sécurité nationale.

Réseaux d'employés et de dirigeants

Des répondants ont indiqué que la création du Réseau des PANDC et du Réseau des femmes du SCRS favorisait l'inclusion des groupes marginalisés en plus de leur offrir du soutien. Le rôle du Réseau des femmes du SCRS consiste à fournir des informations sur le genre et la diversité, ainsi qu'à conseiller ses membres sur leur cheminement professionnel. Pour leur part, de petits groupes du Réseau des PANDC ont rencontré le directeur du SCRS afin de discuter de leurs expériences de travail au sein du Service (Tsalikis, 2020). En outre, ces réseaux favorisent un sentiment d'appartenance parmi leurs membres et leur apportent du soutien.

Dans certains ministères, les dirigeants rencontrent régulièrement les représentants des réseaux d'employés, ce qui témoigne de l'importance que la direction accorde à ces enjeux clés. Les dirigeants jouent un rôle important lorsqu'il s'agit de soutenir les initiatives et les plans de formation sur l'élimination des biais au sein du SCRS et des autres organismes fédéraux. Par exemple, les ministres ont apparemment joué un rôle clé lorsqu'il a été demandé de réexaminer comment les données désagrégées peuvent aider à mieux comprendre les difficultés rencontrées par les communautés marginalisées. De plus, les dirigeants peuvent influer sur les parcours d'apprentissage des employés en mettant l'accent sur la compréhension des biais, de la marginalisation et de la gestion des données. Une façon d'y parvenir consisterait à créer des plans d'apprentissage individuels qui comprendraient des cours de formation obligatoires et optionnels offerts par le gouvernement du Canada et qui feraient l'objet de discussion entre les gestionnaires et les employés.

Bien que les dirigeants semblent jouer un rôle essentiel dans l'affectation des ressources et la priorisation des questions d'équité, les initiatives telles que les plans d'apprentissage ou les approches diversifiées en matière d'embauche ne nous fournissent que peu d'informations sur la façon dont les dirigeants s'y prennent pour approfondir leur apprentissage des biais de données endémiques. Par exemple, il a toujours été indiqué que les plans d'apprentissage devaient faire l'objet d'une discussion avec un

gestionnaire ou un supérieur. Puisque les dirigeants jouent un rôle essentiel dans l'organisation des réseaux d'équité ou l'adaptation des plans d'apprentissage, il faut porter une attention particulière aux moyens que prennent les dirigeants pour se tenir au courant des enjeux relatifs aux biais dans la gestion des données et s'y adapter, et ce, de façon à continuer de créer des milieux de travail qui favorisent l'apprentissage.

Formation sur l'élimination des biais en tant que composante de l'alphabétisation numérique

La définition de l'alphabétisation numérique demeure complexe et continue d'évoluer au rythme des avancées technologiques et de la numérisation mondiale (Bejaković et Mrnjavac, 2020). Au lieu d'être définie comme un ensemble de compétences techniques, l'alphabétisation numérique fait généralement référence à la maîtrise et à la compréhension des systèmes par rapport à la technologie et au monde numérique, ainsi qu'au fonctionnement de ces systèmes suivant les contraintes légales et éthiques (Bejaković et Mrnjavac, 2020). Par conséquent, l'alphabétisation numérique doit être interprétée de manière élargie, c'est-à-dire qu'elle doit englober la maîtrise et la compréhension des systèmes, et non seulement les compétences techniques. Cette définition élargie de l'alphabétisation numérique comprendrait donc l'atténuation des biais et les valeurs que sont la diversité, l'équité et l'inclusion.

Approche globale à l'égard de l'alphabétisation numérique

Le Cadre de référence des compétences numériques de la Commission européenne, par exemple, tient compte du bien-être social, de la protection de la vie privée et de l'inclusion. Ce cadre repose sur les cinq compétences ci-dessous :

1. *information et littératie des données;*
2. *communication et collaboration;*
3. *création de contenu numérique;*
4. *sécurité;*
5. *résolution de problèmes.*

Le cadre offre une approche globale pour enseigner l'alphabétisation numérique puisqu'il rassemble les considérations éthiques et les compétences techniques nécessaires. Par exemple, la compétence « Sécurité » fait référence à la protection de la vie privée, à la sensibilisation au mieux-être et à l'inclusion sociale. Par ailleurs, la compétence « Résolution de problèmes » désigne la faculté de réflexion et la capacité à adopter une attitude constructive, soit des caractéristiques qui aideraient une personne à

comprendre les répercussions des données qui ne sont peut-être pas évidentes à première vue. Ces principes sont transférables au SCRS puisqu'ils visent à atténuer les biais dans la gestion des données. L'accroissement des compétences en alphabétisation numérique constitue une préoccupation dans l'ensemble de la fonction publique fédérale et restera un sujet d'actualité au cours des prochaines années (gouvernement du Canada, 2017).

Lors des entrevues, de nombreux répondants ont indiqué qu'une formation individuelle ou ministérielle sur les biais de données et l'alphabétisation numérique était essentielle pour le poste qu'ils occupent. Beaucoup d'entre eux ont mentionné qu'il serait important de mettre en place une politique de formation sur l'ACS+ pour créer une compréhension interministérielle commune des différents moyens permettant de tenir compte de la spécificité des sexes dans les processus décisionnels et de planification.

Le gouvernement canadien a pris des mesures pour intégrer l'ACS+ dans tous les ministères, programmes et processus de planification, et ce, à tous les niveaux (Femmes et Égalité des genres Canada, 2021). Au départ, le cadre de l'ACS reposait sur le mouvement de défense des droits des femmes. En 2012, on y a ajouté la mention « plus » pour inclure une approche intersectionnelle (Christoffersen et Hankivsky, 2021). Toutefois, il y a encore beaucoup de chemin à faire pour tirer des leçons du courant dominant et intégrer pleinement la notion de « plus » (une approche intersectionnelle) dans les processus décisionnels (Christoffersen et Hankivsky, 2021). En outre, des représentants de l'ensemble des ministères ont affirmé qu'ils connaissaient bien l'ACS+, mais ont laissé entendre que l'intégration d'un cadre intersectionnel était peu avancée. Par exemple, plusieurs facteurs d'identité seraient analysés en fonction de considérations et de catégories distinctes. La façon dont les répondants discutaient de la marginalisation, tout en faisant souvent la distinction entre les initiatives sur l'égalité entre les sexes et celles sur l'égalité entre les races, en témoigne.

En revanche, un groupe communautaire qui offrait une aide financière dans le cadre de la pandémie et collaborait déjà avec des personnes marginalisées a adopté sciemment une approche intersectionnelle pour analyser la ventilation de ses services d'aide en fonction des caractéristiques des personnes qui y recouraient (sexe, âge, incapacité ou classe). Le groupe jugeait cette approche intersectionnelle importante puisqu'elle lui permettait de cerner les personnes qui subissaient peut-être une double marginalisation et qui avaient peut-être besoin d'aide et de ressources supplémentaires pendant la pandémie. Une telle approche est utile pour les intervenants dans les processus de gestion des données, car elle leur permet de mieux comprendre la façon dont les groupes sont touchés et d'intervenir de façon plus efficace.

Il est important d'adopter une approche intersectionnelle dans l'évaluation de l'incidence des processus de gestion des données. Par exemple, en ce qui concerne le principe de « Sécurité » tel qu'il est défini ci-dessus dans le cadre de référence des compétences en alphabétisation numérique, il est essentiel d'adopter une approche intersectionnelle pour comprendre l'inclusion sociale et évaluer les répercussions sur plusieurs facteurs d'identité.

Au SCRS, des progrès sont réalisés à cet égard grâce à la mise en œuvre de diverses initiatives, telles que l'Appel à l'action en faveur de la lutte contre le racisme, de l'équité et de l'inclusion, et à la tenue d'ateliers et d'événements. Le SCRS a contribué à instaurer un milieu propice à la réflexion lorsqu'il a tenu, en 2020, son premier Colloque d'experts sur les préjugés inconscients, la diversité et l'inclusion dans le domaine de la sécurité nationale, un événement appelé à se répéter tous les ans. Lors de ce colloque, des experts ont analysé en détail la notion du « plus » dans l'ACS+ afin d'aider à mieux faire comprendre l'intersectionnalité. Il est important de poursuivre sur cette lancée et d'intégrer l'atténuation des biais aux compétences en alphabétisation numérique.

Information et littératie des données

Création de contenu numérique

Sécurité

Résolution de problèmes

Le cadre offre une approche globale pour enseigner l'alphabétisation numérique puisqu'il rassemble les considérations éthiques et les compétences techniques nécessaires. Par exemple, la compétence « Sécurité » fait référence à la protection de la vie privée, à la sensibilisation au mieux-être et à l'inclusion sociale. Par ailleurs, la compétence « Résolution de problèmes » désigne la faculté de réflexion et la capacité à adopter une attitude constructive, soit des caractéristiques qui aideraient une personne à comprendre les répercussions des données qui ne sont peut-être pas évidentes à première vue. Ces principes sont transférables au SCRS puisqu'ils visent à atténuer les biais dans la gestion des données. L'accroissement des compétences en alphabétisation numérique constitue une préoccupation dans l'ensemble de la fonction publique fédérale et restera un sujet d'actualité au cours des prochaines années (gouvernement du Canada, 2017).

Lors des entrevues, de nombreux répondants ont indiqué qu'une formation individuelle ou ministérielle sur les biais de données et l'alphabétisation numérique était essentielle pour le poste qu'ils occupent. Beaucoup d'entre eux ont mentionné qu'il serait important de mettre en place une politique

de formation sur l'ACS+ pour créer une compréhension interministérielle commune des différents moyens permettant de tenir compte de la spécificité des sexes dans les processus décisionnels et de planification.

Le gouvernement canadien a pris des mesures pour intégrer l'ACS+ dans tous les ministères, programmes et processus de planification, et ce, à tous les niveaux (Femmes et Égalité des genres Canada, 2021). Au départ, le cadre de l'ACS reposait sur le mouvement de défense des droits des femmes. En 2012, on y a ajouté la mention « plus » pour inclure une approche intersectionnelle (Christoffersen et Hankivsky, 2021). Toutefois, il y a encore beaucoup de chemin à faire pour tirer des leçons du courant dominant et intégrer pleinement la notion de « plus » (une approche intersectionnelle) dans les processus décisionnels (Christoffersen et Hankivsky, 2021). En outre, des représentants de l'ensemble des ministères ont affirmé qu'ils connaissaient bien l'ACS+, mais ont laissé entendre que l'intégration d'un cadre intersectionnel était peu avancée. Par exemple, plusieurs facteurs d'identité seraient analysés en fonction de considérations et de catégories distinctes, et le fait qu'ils s'entrecoupent ne serait pas compris.

En revanche, un groupe communautaire qui offrait une aide financière dans le cadre de la pandémie et collaborait déjà avec des personnes marginalisées a adopté sciemment une approche intersectionnelle pour analyser la ventilation de ses services d'aide en fonction des caractéristiques des personnes qui y recouraient (sexe, âge, incapacité ou classe). Une telle approche intersectionnelle aidait grandement à déterminer les répercussions des services et à identifier les personnes qui avaient peut-être besoin d'une aide supplémentaire pendant la pandémie.

En ce qui concerne les processus de gestion des données, une approche intersectionnelle peut aider à mieux comprendre la façon dont les groupes sont touchés et à intervenir de façon plus efficace. Par exemple, en ce qui concerne le principe de « Sécurité » tel qu'il est défini ci-dessus dans le cadre de référence des compétences en alphabétisation numérique, il est essentiel d'adopter une approche intersectionnelle pour comprendre l'inclusion sociale et évaluer les répercussions sur plusieurs facteurs d'identité.

Au SCRS, des progrès sont réalisés à cet égard grâce à la mise en œuvre de diverses initiatives, telles que l'Appel à l'action en faveur de la lutte contre le racisme, de l'équité et de l'inclusion, et à la tenue d'ateliers et d'événements. Le SCRS a contribué à instaurer un milieu propice à la réflexion lorsqu'il a tenu, en 2020, son premier Colloque d'experts sur les préjugés inconscients, la diversité et l'inclusion dans le domaine de la sécurité nationale, un événement appelé à se répéter tous les ans. Lors de ce colloque, des experts ont analysé en détail la notion du « plus » dans l'ACS+ afin d'aider à mieux faire

comprendre l'intersectionnalité. Il est important de poursuivre sur cette lancée et d'intégrer l'atténuation des biais aux compétences en alphabétisation numérique.

Sommaire des recommandations

- Faire preuve de transparence en ce qui concerne la formation des dirigeants sur les biais dans la gestion des données afin de s'assurer qu'ils sont à même d'offrir du soutien aux réseaux d'employés en matière d'équité ainsi que d'aider à élaborer les plans d'apprentissage personnalisés des employés.
- Mobiliser des représentants de communautés marginalisées pour aider à instaurer un milieu propice à la réflexion dans lequel les intervenants cherchent à corriger les biais, intègrent une approche intersectionnelle et tirent des leçons pour tenter de régler les problèmes endémiques.
- Faire de la mobilisation et de l'apprentissage des communautés marginalisées des objectifs à long terme ou permanents afin de mettre l'accent sur l'engagement à l'égard d'un changement de la culture organisationnelle et l'adoption d'approches systémiques, plutôt que sur des interventions ponctuelles.
- Alphabétisation numérique : Se servir de plans d'apprentissage individuels pour approfondir les connaissances sur la diversité, l'équité et l'inclusion liées à la gestion de données. Il faudrait également que le SCRS examine s'il pourrait aller jusqu'à offrir un soutien ministériel, car un représentant du SCRS a indiqué qu'un « soutien organisationnel individuel » était nécessaire pour veiller à ce que les ministères respectent les normes et les directives. Il s'agit d'un changement que le SCRS pourrait envisager d'apporter à ses processus internes.
- L'intégration, aux plans d'apprentissage individuels, de cours sur l'alphabétisation numérique offerts par l'entremise de GCApprentissage favoriserait une compréhension fondamentale commune à l'échelle du SCRS.

3. Fragmentation dans l'ensemble des ministères – Moyens d'accroître l'interopérabilité

Les données de plus en plus nombreuses recueillies sur les citoyens sont conservées par le gouvernement fédéral et les administrations provinciales et municipales. Plusieurs répondants ont affirmé que le modèle de système de gouvernement britannique – un modèle repris par le Canada – permet aux ministères et organismes de fonctionner en vase clos et de jouir d'une certaine flexibilité dans la création

de normes relatives à la collecte et à la communication des données. Or, une telle approche ne favorise pas la collaboration interministérielle ni l'échange d'informations sur les enjeux liés aux biais et à la gestion éthique des données. Lors de neuf entrevues, les répondants ont fait état de la nécessité d'accroître l'interopérabilité. À l'origine, le terme « interopérabilité » désignait la capacité des *systèmes informatiques* d'échanger et d'utiliser des informations, mais le terme a évolué : aujourd'hui, il prend en compte des facteurs sociaux, politiques et organisationnels. Par conséquent, nous interprétons l'interopérabilité comme la capacité des *systèmes* d'échanger et d'utiliser des informations (Leal et al., 2019).

Des représentants du gouvernement ont indiqué qu'il fallait améliorer les voies de communication entre les ministères afin d'accroître l'échange d'informations sur les questions entourant la gestion des données et de favoriser la tenue d'un dialogue sur la façon d'éliminer les biais qui sont ancrés dans le système. Le fait d'améliorer l'échange d'informations entre les ministères peut également contribuer à l'adoption de normes officielles et compatibles en matière de saine gestion des données dans l'ensemble des ministères.

Le SCRS exerce ses activités dans le secteur de la sécurité nationale, lequel dispose d'exemptions spéciales, et ne contribue manifestement pas aux opérations et services des autres ministères et organismes. Cela dit, les discussions que nous avons eues avec divers représentants gouvernementaux ont révélé que les difficultés découlant des enjeux endémiques définis précédemment surviennent dans l'ensemble du gouvernement. Le Secrétariat du Conseil du Trésor a tenu des consultations au sujet de la Directive sur la prise de décisions automatisées avec d'autres organismes qui relèvent du portefeuille de la Sécurité publique, tels que l'Agence des services frontaliers du Canada (ASFC) et la Gendarmerie royale du Canada (GRC), mais le SCRS n'y a pas participé. **Ainsi, le SCRS a tout intérêt à se considérer comme une partie d'un grand écosystème fédéral qui travaille à surmonter les problèmes systémiques susceptibles de causer des préjudices non intentionnels aux membres de certains groupes qui demandent à obtenir un service ou une protection du gouvernement ou d'empêcher ces groupes d'en faire la demande.** Le SCRS réaffirme ainsi que son mandat consiste à assurer la sécurité du Canada et qu'il est prêt à collaborer avec d'autres organismes ou ministères pour tirer parti des pratiques existantes, pour autant qu'il puisse les adapter au secteur de la sécurité nationale.

Interopérabilité en Nouvelle-Zélande

(https://www.digital.govt.nz/digital-government/about-digital-government/introduction-to-nzs-digital-transformation/)

En Nouvelle-Zélande, l'intendant principal des données, le dirigeant principal du numérique et l'agent principal de la sécurité de l'information collaborent dans le cadre d'un partenariat lancé par le dirigeant principal du numérique en 2015. Le partenariat regroupe plus de 20 organismes gouvernementaux et 55 hauts dirigeants. Un partenariat qui englobe les fonctions liées aux données, à la sécurité et à la numérisation permet aux parties prenantes d'amorcer une discussion intersectorielle non seulement sur la façon dont on peut tirer parti des données, mais aussi sur les préoccupations et les risques pour l'avenir.

Des répondants ont attiré l'attention sur plusieurs initiatives qui ont été mises en œuvre à l'échelle du gouvernement et dont le SCRS pourrait tirer parti pour intensifier ses efforts de rapprochement avec les autres ministères et organismes et régler les problèmes liés aux enjeux endémiques. Nous croyons qu'il est possible pour le SCRS d'envisager une interopérabilité accrue avec les organismes ci-dessous.

Première possibilité : Statistique Canada

À notre avis, Statistique Canada pourrait jouer un rôle clé pour accroître l'interopérabilité. Cette possibilité est apparue lorsqu'un répondant a déclaré que Statistique Canada est sous-utilisé dans le contexte de la gestion des données. En effet, Statistique Canada applique des normes, des pratiques et des mécanismes rigoureux en matière de gestion éthique des données. Plus particulièrement, un représentant de Statistique Canada a mentionné qu'il est essentiel d'appliquer le Cadre de nécessité et de proportionnalité pour assurer un haut niveau d'éthique dans la gestion des données. Ce cadre est directement lié à l'article 12 de la *Loi sur le SCRS*, lequel stipule que le SCRS recueille des informations et des renseignements dans la mesure strictement nécessaire. Un autre point important souligné par un représentant de Statistique Canada est le fait que les données doivent être analysées en fonction du contexte. Ce principe peut aider à comprendre comment déterminer la qualité à la fois des données et de leur source. De toute évidence, il existe des possibilités de synergie entre Statistique Canada et le SCRS : les deux organismes peuvent s'allier pour renforcer ces définitions et ces cadres et s'assurer que, dans sa gestion des données, le SCRS applique les pratiques de gestion des données qui visent à réduire les biais tout au long du cycle de vie des données. Une telle collaboration permettrait de réduire les préjudices envers les groupes marginalisés de longue date.

Deuxième possibilité : Secrétariat du Conseil du Trésor

D'après nos constatations, deux directives montrent la possibilité d'accroître l'interopérabilité entre le SCRS et le Secrétariat du Conseil du Trésor.

Premièrement, il y a la Directive sur la prise de décisions automatisée. Cette directive vise à atténuer les biais en surveillant et en assurant la qualité des données, c'est-à-dire veiller à ce que les données soient exactes, récentes et examinées par des pairs. L'un des répondants a indiqué que la Directive ne s'applique pas forcément au SCRS qui, de par sa nature, s'emploie à recueillir des données plutôt qu'à prendre des décisions. Cependant, comme le SCRS s'apprête à adopter des outils de prise de décisions automatisée et d'analyse de pointe pour l'aider à mener ses opérations, il pourrait intégrer certains principes de cette directive à ses activités. Comme il a été mentionné précédemment, l'EIA aide à déterminer le degré d'incidence d'un système automatisé en tenant compte de sa conception, ainsi que de l'algorithme, du type de décision, des répercussions et des données. Il est essentiel que le SCRS prenne en considération chacun des facteurs, à tous les niveaux, pour déterminer la façon dont des biais peuvent s'immiscer. L'instauration officielle d'un tel processus d'analyse et de vérification permettrait de s'assurer que des précautions sont prises pour réduire le risque de préjudice envers des personnes et des communautés, atténuant ainsi les enjeux endémiques. Qui plus est, un tel processus cadre avec les Principes de bonne pratique de l'Organisation de coopération et de développement économiques (OCDE) en matière d'éthique des données dans le secteur public. Ces principes réitèrent les objectifs que visent expressément l'utilisation des données et les outils d'autoévaluation et de réflexion pour aider à définir les limites des divers aspects du cycle de vie des données (OCDE, 2021).

Boîte de dialogue : Principes de bonne pratique de l'OCDE en matière d'éthique des données dans le secteur public

La transition vers un gouvernement numérique, l'augmentation des flux de données et la difficulté de créer des structures de gouvernance transfrontalières pour les données mettent en évidence la nécessité d'élaborer une orientation stratégique détaillée concernant les conséquences, sur le plan de l'éthique, de l'accès aux données, ainsi que de leur communication et de leur utilisation (OCDE, 2021). L'apparition de nouvelles technologies peut contribuer à l'augmentation exponentielle de la production et de l'utilisation de données dans un contexte où il y a numérisation des informations dans les différentes sphères de la société. Les possibilités en matière d'analyse de données se multiplient, les gouvernements cherchant à tirer parti des technologies numériques pour améliorer et simplifier leurs fonctions, orienter la conception

et la mise en œuvre de politiques et de services améliorés, et automatiser les processus décisionnels au moyen d'algorithmes (OCDE, 2021).

Les Principes de bonne pratique ont été élaborés par un groupe de travail de l'OCDE formé de hauts fonctionnaires de l'administration numérique (OCDE, 2021). Ces dix principes, que tous les membres de l'OCDE sont tenus d'appliquer, placent les valeurs humaines et les droits de la personne au cœur des politiques, des stratégies, des initiatives et des projets liés au gouvernement numérique et aux données (OCDE, 2021). Grâce à l'élaboration de documents d'orientation fondés sur les valeurs, les gouvernements sont en mesure :

- *d'adopter des approches axées sur l'inclusion et la collaboration pour concevoir des politiques, des stratégies et des initiatives qui renforcent l'utilisation éthique des données dans la fonction publique;*
- *d'établir un consensus sur la façon de renforcer la confiance du public dans le contexte de la gestion des données;*
- *de convenir de pratiques de gestion des données fiables en se fondant sur des valeurs communes.*

Deuxièmement, il y a la Directive sur l'évaluation des facteurs relatifs à la vie privée. Cette directive oriente les institutions gouvernementales quant à la façon d'évaluer les incidences sur la vie privée des activités ou des programmes liés au traitement de renseignements personnels. Elle oblige les ministères et organismes fédéraux à effectuer une évaluation des facteurs relatifs à la vie privée pour tout programme ou service qui peut avoir une incidence sur le respect des droits à la vie privée, ainsi qu'à la documenter et à la publier. Le dédale de plus en plus complexe de données et de technologies suscite des préoccupations en matière de vie privée, surtout l'utilisation des technologies de surveillance. Plus particulièrement, la complexité du travail lié à la sécurité nationale et la nécessité de recueillir des renseignements sur des menaces peuvent mener à une intrusion dans la vie privée de personnes ou d'entités suspectes. Si les biais ne sont pas atténués avant la collecte de données sur certaines personnes suspectes, il est possible que des groupes marginalisés de longue date subissent des préjudices de façon disproportionnée.

L'intégration d'une évaluation des facteurs relatifs à la vie privée avant l'utilisation d'outils d'analyse de pointe dans le secteur de la sécurité nationale, sur le plan individuel et communautaire, peut contribuer à atténuer de façon préventive les préjudices auxquels sont exposées les communautés

marginalisées de longue date. Le fait d'officialiser l'évaluation des facteurs relatifs à la vie privée assure la tenue d'un examen proactif avant que ne soient entreprises les activités de collecte de données (Cavoukian, 2012, tel que cité dans Strauss, 2019).

Troisième possibilité : normes

La normalisation permet d'accroître l'interopérabilité et constitue un excellent moyen pour faciliter les interactions entre les systèmes. Les données et les technologies évoluent rapidement, ce qui représente un défi sur le plan des lois et des règlements liés à la vie privée. Toutefois, un répondant a mentionné que la normalisation aide à faire le lien entre le monde de l'innovation et celui de la législation. En effet, l'établissement de normes aide à déterminer ce qui doit absolument être réglementé et favorise les discussions sur ce qui constitue une bonne pratique. Un point à prendre en considération lors de la mise en œuvre de normes est la possibilité de réduire les écarts entre les différentes expériences vécues.

La conformité à certaines normes peut aider à bâtir la confiance, tout particulièrement lorsque ces normes sont fondées sur les valeurs que sont la confiance, la collaboration et le consensus. L'établissement d'une relation de confiance avec les communautés dans le cadre d'une collaboration significative et inclusive en vue de l'élaboration de normes permet de surmonter les défis liés aux enjeux endémiques. Un représentant du Conseil canadien des normes a décrit le travail que l'organisme accomplit avec les collectivités autochtones dans le cadre de la Feuille de route canadienne sur la normalisation en matière de gouvernance des données. Comme la souveraineté des données est un sujet délicat pour les collectivités autochtones, il est important d'inclure ces dernières dans les cercles de discussion afin de créer des normes qui tiennent compte des points de vue des communautés marginalisées de longue date. Ainsi, l'établissement de normes constitue un mécanisme qui favorise des liens de confiance entre les ministères et les intervenants concernés. En matière de saine gouvernance des données, l'élaboration de normes qui tiennent compte des valeurs et de la diversité de la population canadienne au moyen de processus de collaboration avec diverses communautés permet d'établir un langage commun dans le cadre des discussions interministérielles sur les biais dans les pratiques de gestion des données.

Sommaire des recommandations

- Plaider en faveur d'un changement dans la culture organisationnelle qui serait axé sur la réflexion, la collaboration, l'inclusion et l'apprentissage continu. Ces principes constituent un point de

départ critique pour l'adoption de toutes les autres recommandations formulées dans le présent rapport.

- Créer des groupes de travail interministériels (Statistique Canada, Secrétariat du Conseil du Trésor, Commissariat à la protection de la vie privée, Conseil canadien des normes) afin de discuter de l'efficacité des approches et des principes d'atténuation de biais que chacun des organismes a mis en place jusqu'à présent pour assurer une gestion éthique des données et de déterminer comment ces approches et principes peuvent être adaptés au secteur de la sécurité nationale. Les autres intervenants qui exercent des activités dans le secteur de la sécurité nationale pourraient être intégrés à ces groupes de travail interministériels; il s'agit notamment des intervenants des organismes qui relèvent du portefeuille de Sécurité publique Canada, tels que le Service correctionnel Canada, le CST, la GRC, l'ASFC et le ministère de la Défense nationale, qui ont mis en place les principes directeurs de cadres relatifs à l'éthique et à l'analyse des données.
- Accroître l'interopérabilité en trouvant d'autres moyens d'échanger des informations sur la façon dont les normes en matière de saine gouvernance des données et d'atténuation des biais sont intégrées.

CONCLUSION

La présente étude montre que les organismes de sécurité et de renseignement doivent souvent maintenir un équilibre fragile entre leur mandat – à savoir protéger la population – et leurs obligations redditionnelles envers les structures de gouvernance dont ils relèvent, tout particulièrement dans un contexte démocratique. Notre recherche a démontré que la situation est encore plus délicate compte tenu de la complexité du cycle de vie des données et des biais endémiques qui touchent différentes étapes du processus de gestion des données. Dans le même ordre d'idées, nous avons également démontré que différents groupes d'intervenants reconnaissent dorénavant la nécessité d'atténuer les répercussions des biais.

Le SCRS doit d'abord comprendre la situation dans son ensemble s'il veut atténuer les répercussions des biais dans la gestion des données. En prenant conscience de sa place dans le grand écosystème, il sera mieux à même de tirer parti des efforts des autres ministères et organismes qui cadrent avec le mandat que lui confère la *Loi sur le SCRS*. Qui plus est, il est possible de repenser ce que la protection de la population canadienne signifie selon le mandat du SCRS. Il s'agirait notamment d'inclure au « devoir de

protéger » la compréhension des divers facteurs de vulnérabilité des communautés marginalisées ainsi que les répercussions que les biais dans les pratiques de gestion des données entraînent pour ces communautés.

Nous nous sommes fondés sur notre examen des pratiques exemplaires dans d'autres contextes, notre analyse documentaire et nos entrevues pour formuler les recommandations suivantes :

- s'appuyer sur des mécanismes de reddition de comptes existants en mobilisant les communautés marginalisées à l'interne et à l'externe;
- multiplier les possibilités d'apprentissage interne pour favoriser l'acquisition de compétences numériques et sensibiliser le personnel aux problèmes endémiques liés aux biais de données, de sorte à changer la culture organisationnelle.
- accroître l'interopérabilité en trouvant des moyens plus efficaces d'échanger des informations sur les normes en matière de gouvernance des données et d'atténuation des biais.

À notre avis, ces recommandations offrent au SCRS des points de départ solides pour poursuivre ses efforts en vue d'atténuer les biais, et ce, grâce à la compréhension des biais endémiques et des stratégies déjà mises en œuvre dans divers contextes.

GLOSSAIRE

Direction de la liaison-recherche et de la collaboration avec les intervenants (LRCI)

Intelligence artificielle (IA)

Évaluation de l'incidence algorithmique (EIA)

Personnes autochtones, noires et de couleur (PANDC)

Agence des services frontaliers du Canada (ASFC)

Centre de la sécurité des télécommunications (CST)

Service canadien du renseignement de sécurité (SCRS)

Analyse comparative entre les sexes plus (ACS+)

Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR)

Organisation de coopération et de développement économiques (OCDE)

Gendarmerie royale du Canada (GRC)

Secrétariat du Conseil du Trésor du Canada (SCTC)