ACCÈS LÉGAL, DROIT À LA VIE PRIVÉE ET CONFIANCE

RAPPORT DESTINÉ AU

COMITÉ DES PARLEMENTAIRES SUR LA SÉCURITÉ NATIONALE

ET LE RENSEIGNEMENT

NOVEMBRE 2023

BENJAMIN J. GOOLD

FACULTÉ DE DROIT PETER A. ALLARD

UNIVERSITÉ DE LA COLOMBIE-BRITANNIQUE

CONTENU

INTRODUCTION

Au cours des vingt dernières années, le chiffrement, le droit à la vie privée et les pouvoirs d'enquête de la police et des services de sécurité ont fait l'objet d'un débat continu au Canada[1]. Depuis les consultations sur l'accès légal en 2002, suivies de la publication du *Livre vert sur la sécurité nationale* en 2016 et, plus récemment, du rapport du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (Comité ETHI), en 2022, les gouvernements successifs ont été confrontés au problème de savoir comment veiller à ce que les pouvoirs juridiques et les techniques d'enquête utilisées par la police et les services de sécurité – ce qui est souvent appelé « accès légal » – suivent l'évolution de la technologie tout en respectant le droit à la vie privée et les autres droits garantis par la *Charte canadienne des droits et libertés*.

Face à ce que l'on appelle souvent le problème « going dark », les officiers supérieurs de la Gendarmerie royale du Canada (GRC) ont à maintes reprises demandé des pouvoirs supplémentaires qui leur permettraient d'accéder légalement aux données et aux communications chiffrées au Canada[2]. En 2016, Bob Paulson, qui était alors commissaire à la GRC, a déclaré à CBS News qu'il y avait [TRADUCTION] « chaque jour des activités criminelles qui [étaient] facilitées par la technologie et pour lesquelles aucune mesure n'[était] prise », et il a attiré l'attention sur ce que la GRC considérait comme des obstacles numériques aux enquêtes criminelles et des menaces pour la sécurité nationale[3]. Dans les années qui ont suivi, et en l'absence de la réforme du droit souhaitée par la GRC[4], la police a continué de chercher des

---

[1] Pour un compte rendu récent de ce débat au Canada et ailleurs, consulter Diab, R. « The Road Not Taken: Missing Powers to Compel Decryption in Bill C-59, Ticking Bombs, and the Future of the Encryption Debate », *Alberta Law Review,* vol. 57, 2019, p. 267-96.

[2] Seglins, D., Cribb, R. et Gomez, C. « RCMP Boss Bob Paulson Says Force Needs Warrantless Access to ISP User Data », *CBC News*, 2016 (15 novembre 2016), https://www.cbc.ca/news/investigates/police-power-privacy-paulson-1.3851955 (consulté le 24 août 2023); Tunney, T. « RCMP's Ability to Police Digital Realm 'Rapidly Declining,' Commissioner Warned », *CBC News*, 2018 (5 octobre 2018), https://www.cbc.ca/news/politics/lucki-briefing-binde-cybercrime-1.4831340 (consulté le 13 août 2023).

[3] Seglins, D., Cribb, R. et Gomez, C. « RCMP Boss Bob Paulson Says Force Needs Warrantless Access to ISP User Data », *CBC News*, 2016 (15 novembre 2016).

[4] Dans le sillage du *Livre vert sur la sécurité nationale* de 2016, la GRC a publiquement soutenu la mise en place de divers nouveaux pouvoirs dans la *Loi antiterroriste* du Canada (projet de loi C-51). Consulter Seglins, D., Cribb, R. et Gomez, C. « RCMP Want New Powers to Bypass Digital Roadblocks in Terrorism, Major Crime

moyens de relever les défis posés par le chiffrement. Plus récemment, soit au milieu de 2022, il a été révélé que la GRC avait utilisé des logiciels espions (« outils d'enquête sur appareil ») pour accéder aux téléphones mobiles et aux ordinateurs portables de suspects dans le cadre de plusieurs enquêtes menées pendant la période de 2018 à 2020[5]. Il est frappant de constater que le recours à cette technologie par la police a été caché pas seulement au public, mais également au Commissariat à la protection de la vie privée du Canada (CPVP). Lorsqu'il s'est adressé au Comité ETHI, en août 2022, le commissaire Philippe Dufresne a fait observer que son bureau n'avait pas été consulté ni même informé au sujet de l'utilisation d'outils d'enquête sur appareil par la GRC et qu'il n'avait eu connaissance de cette pratique qu'à la suite de la parution d'articles dans les médias[6]. Malgré ces révélations, la GRC a continué de soutenir qu'il fallait en faire davantage pour l'aider à surmonter les défis posés par le chiffrement. Au moment de la rédaction du présent rapport, par exemple, l'Association canadienne des chefs de police (ACCP) était toujours d'avis qu'il fallait modifier la loi pour obliger le détenteur d'une clé de chiffrement ou d'un mot de passe à les mettre à la disposition des organismes d'application de la loi (pour autant qu'une autorisation judiciaire ait été obtenue[7]).

Contrairement à la position adoptée par la GRC et l'Association canadienne des chefs de police, les défenseurs de la vie privée, les groupes de la société civile et le milieu universitaire ont exprimé de vives inquiétudes quant à l'éventualité où il serait plus facile pour la police et les

Cases », *CBC News*, 2016 (15 novembre 2016), https://www.cbc.ca/news/investigates/rcmp-digital-roadblocks-1.3850018 (consulté le 24 août 2023); et Seglins, D., Cribb, R. et Gomez, C. « Inside 10 Cases Where the RCMP Hit a Digital Wall », *CBC News*, 2016 (15 novembre 2016), https://www.cbc.ca/news/investigates/police-power-privacy-rcmp-cases-1.3850783 (consulté le 24 août 2023).

[5] Forrest, M. « Canada's National Police Force Admits Use of Spyware to Hack Phones », *Politico*, 2022 (29 juin 2022), https://www.politico.com/news/2022/06/29/canada-national-police-spyware-phones-00043092 (consulté le 23 août 2023). En réponse à une question posée par le député conservateur Tako Van Popta le 6 mai 2022, la GRC a admis avoir utilisé des outils d'enquête sur appareil pour accéder à des données et prendre le contrôle des caméras et des microphones de téléphones mobiles. Consulter Chambre des Communes. Ordre/adresse de la Chambre des Communes, Q-566, document parlementaire 8555-441-566 (22 juin 2022). À la suite du dépôt de cette réponse, le Comité ETHI a adopté une motion visant à étudier l'utilisation d'outils d'enquête sur appareil par la GRC. Consulter Chambre des communes (Canada). Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique. *Outils d'enquête sur appareil utilisés par la Gendarmerie royale du Canada et enjeux liés,* rapport (novembre 2022), 44e législature, 1re session [ci-après « Rapport du Comité permanent sur les outils d'enquête sur appareil »].

[6] Rapport du Comité permanent sur les outils d'enquête sur appareil (idem), p. 12.

[7] Association canadienne des chefs de police. *Résolutions adoptées à la 111e Conférence annuelle*, 2016 (août 2016), p. 19-20 (Résolution no 03), https://www.cacp.ca/r_solution.html (consulté le 11 septembre 2023).

services de sécurité d'accéder aux données et aux communications chiffrées des Canadiens. Dans un rapport indépendant complet de 2018 sur le chiffrement au Canada, intitulé *Shining a Light on the Encryption Debate: A Canadian Field Guide*, Citizen Lab et la Clinique d'intérêt public et de politique d'Internet du Canada (CIPPIC) ont fait valoir que la police ne cessait d'exagérer l'ampleur du problème « going dark » et qu'elle disposait de sources d'information plus que suffisantes pour relever les défis posés par le chiffrement :

> [TRADUCTION] Le chiffrement protège inévitablement certaines données des organismes gouvernementaux, mais les organismes d'application de la loi et de renseignement ne manquent généralement pas de renseignements pour effectuer leur travail. Or, non seulement on est loin du problème « going dark », mais on dispose également aujourd'hui de plus de renseignements au sujet de la vie privée des individus qu'à n'importe quel moment de l'histoire de l'humanité. Les mesures d'aide aux entreprises continuent de favoriser la création et l'agrégation de données dans des formats qui restent accessibles aux fournisseurs de services, aux agents de l'État et à d'autres tierces parties dans des formats non chiffrés […]. Une analyse holistique et contextuelle du débat sur le chiffrement montre clairement que les coûts d'enquête et de renseignement imposés par un accès public illimité à une technologie de chiffrement solide sont souvent surestimés[8].

Les auteurs du rapport ont déployé des efforts considérables pour décrire les enjeux des mesures visant à affaiblir ou à contourner le chiffrement. Ils ont précisé que, outre les avantages économiques découlant d'opérations commerciales et financières privées et sécurisées, le chiffrement [TRADUCTION] « se rattach[ait] de très près » à plusieurs droits fondamentaux, les plus importants étant celui à la vie privée et celui à la liberté d'expression. De plus, ils ont fait valoir que la disponibilité du chiffrement – et le droit à la vie privée qu'il procure – représentait un contrepoids essentiel aux capacités de surveillance croissantes de l'État canadien :

---

[8] Gill, L., Israel, T. et Parsons, C. *Shining a Light on the Encryption Debate*: *A Canadian Field Guide*, Citizen Lab et Clinique d'intérêt public et de politique d'Internet du Canada Samuelson-Glushko, 2018, https://citizenlab.ca/wp-content/uploads/2018/05/Shining-A-Light-Encryption-CitLab-CIPPIC.pdf (consulté le 24 août 2023), iv. L'argument selon lequel la police a surestimé les défis en matière d'enquête posés par le chiffrement a été repris par Ann Cavoukian, ancienne commissaire à la protection de la vie privée de l'Ontario. Selon Mme Cavoukian, la police dispose généralement de plus de renseignements qu'il ne lui en faut pour enquêter sur la criminalité et la prévenir, et bien que le chiffrement puisse constituer un obstacle, il est loin d'être insurmontable. Le défi consiste plutôt à relier les points et à assembler [TRADUCTION] « toutes les pièces du puzzle ». Consulter Seglins, Cribb et Gomez. « RCMP Want New Powers », 2016 (nº 4 ci-dessus). Des commentateurs ont également soulevé un point semblable dans le contexte américain. Consulter Swire, P. et Ahmad, K. « 'Going Dark' Versus a 'Golden Age for Surveillance », Center for Democracy and Technology, 2011, https://cdt.org/insights/going-dark-versus-a-golden-age-for-surveillance/ (consulté le 24 août 2023).

> [TRADUCTION] À une époque où les organismes de renseignement d'origine électromagnétique exercent leurs activités alors qu'un minimum de restrictions sont exercées sur leurs activités de surveillance à l'étranger, le chiffrement reste l'une des rares limites pratiques à la surveillance de masse […]. Le simple fait d'être conscient de la surveillance de masse a un effet dissuasif important sur la liberté d'expression. Les groupes vulnérables et marginalisés sont soumis de manière disproportionnée au regard scrutateur de l'État et peuvent être particulièrement vulnérables à ces effets dissuasifs. Les démocraties paient un prix particulièrement élevé lorsque les voix minoritaires et les opinions dissidentes sont poussées à s'autocensurer ou à s'abstenir de participer à la vie publique […]. Le recours à des systèmes de chiffrement non compromis peut donc favoriser la sécurité nécessaire à une intégration importante, à une mobilisation démocratique et à l'égalité d'accès dans la sphère numérique[9].

Cinq ans se sont écoulés depuis la publication du rapport *Shining a Light on the Encryption Debate*, mais ces arguments clés – à savoir que la police surestime régulièrement l'ampleur du problème « going dark » et que le chiffrement est essentiel à la protection de la vie privée, à la liberté d'expression et à diverses valeurs démocratiques – restent au cœur du débat sur l'accès légal au Canada. En même temps, des données probantes démontrent que le sentiment du public à l'égard de la police et des services de sécurité – qui est généralement positif au Canada – pourrait être en train de changer[10]. Selon les résultats des trois dernières enquêtes auprès des clients et des partenaires de la GRC, la confiance du public envers cette dernière n'a cessé de diminuer, en passant de 69 % en 2019-2020 à 60 % en 2020-2021, puis à 53 % en 2021-2022[11]. Des baisses semblables ont été signalées pour un certain nombre de services de police provinciaux, en particulier depuis mars 2020 et la pandémie de COVID-19[12]. La perception du Service canadien du renseignement de sécurité (SCRS) demeure largement positive, mais un

[9] Gill, Israel et Parsons. *Shining a Light on the Encryption Debate*, 2018 (nº 8 ci-dessus), i.

[10] Ruddell, R. « The Changing Context of Canadian Policing: An Examination of the Public's Perceptions after 2020 », *Journal of Community Safety and Well-Being*, vol. 7, nº 2, 2022, p. 47–52.

[11] Gendarmerie royale du Canada. *Résultats des sondages d'opinion auprès des clients et des partenaires 2019-2020*, 2020; Gendarmerie royale du Canada. *Résultats des sondages d'opinion auprès des clients et des partenaires 2020-2021*, 2021; Gendarmerie royale du Canada. *Résultats des sondages d'opinion auprès des clients et des partenaires 2021-2022*, 2022. Tous les documents sont disponibles sur le site https://www.rcmp-grc.gc.ca/fr/rapports-recherche-et-publications/resultats-des-sondages-dopinion-aupres-des-clients-et-des-partenaires (consulté le 11 septembre 2023).

[12] Ruddell. 2022 (nº 10 ci-dessus), p. 48-49.

rapport récent commandé par le SCRS a révélé que seulement 63 % des personnes interrogées se fiaient « un peu » à l'organisation pour la protection des droits et des libertés des Canadiens[13].

C'est dans le contexte du problème « going dark » et de l'évolution de la perception des organismes d'application de la loi que le présent rapport propose quelques réflexions sur le chiffrement et le débat sur l'accès légal au Canada. Plus précisément, il vise à attirer l'attention sur deux volets souvent négligés de ce débat, à savoir les dimensions publiques de la vie privée et l'importance du maintien de la confiance envers la police et les services de sécurité. Il est important d'approfondir notre compréhension à l'égard du type d'intérêt en matière de vie privée en jeu dans les discussions sur le chiffrement – de manière à intégrer non seulement la vie privée individuelle, mais également les volets publics et collectifs de la vie privée – si nous devons évaluer correctement les coûts de l'élargissement des pouvoirs de la police en vue de l'accès légal aux communications et aux données chiffrées. De même, il est dans l'intérêt de la police et des services de sécurité d'examiner les répercussions possibles de cet élargissement des connaissances sur la confiance institutionnelle. Étant donné que les organismes d'application de la loi au Canada dépendent grandement du soutien du public pour réaliser bon nombre de leurs tâches, toute perte de confiance découlant des efforts visant à mettre en péril le chiffrement ou à en venir à bout doit être mise en balance avec les prétendus avantages de l'élargissement de l'accès légal et de la lutte contre le problème « going dark ».

D'emblée, il est important de mentionner que le présent rapport n'examine pas la question de savoir si l'accès légal au Canada doit être réformé pour faciliter (ou compliquer) la prise de mesures d'intervention par la police et les services de sécurité à l'égard des défis posés par le chiffrement. De même, il n'aborde pas les déclarations des organismes d'application de la loi, des défenseurs de la vie privée, de la société civile ou du milieu universitaire sur la nature, l'étendue ou l'avenir du problème « going dark ». Il existe déjà une abondante documentation sur le paysage juridique de l'accès légal au Canada et sur la question de savoir si la police et les

[13] Les Associés de recherche EKOS. « Attitudes à l'égard du Service canadien du renseignement de sécurité (SCRS) : Rapport », 2021, https://publications.gc.ca/collections/collection_2021/scrs-csis/PS74-8-2-2021-fra.pdf (consulté le 31 octobre 2023). Consulter également Marhnouj, S. « CSIS survey finds majority of Canadians leery of giving more powers to police, intelligence agencies », *The Globe and Mail*, 2022 (16 janvier 2022), https://www.theglobeandmail.com/politics/article-csis-survey-finds-canadians-leery-of-giving-more-powers-to/ (consulté le 14 novembre 2023).

services de sécurité ont besoin de pouvoirs supplémentaires pour faire face à l'utilisation croissante du chiffrement[14]. L'objectif du présent rapport est de placer la relation entre le public et l'État canadien au cœur du débat sur l'accès légal.

Jusqu'à présent, le problème « going dark » au Canada a été largement encadré en fonction de l'existence d'une tension entre les biens publics (sûreté et sécurité) d'une part et des droits individuels (à la vie privée et à la liberté d'expression) d'autre part[15]. La réalité est cependant beaucoup plus complexe. L'élargissement de l'accès légal est clairement susceptible d'affaiblir les droits et libertés individuels, mais dans la mesure où ces derniers englobent un volet public, il peut également porter atteinte à des intérêts et valeurs *collectifs* qui sont importants pour le bon fonctionnement de la démocratie constitutionnelle du Canada. De même, il peut être tentant pour la police et les services de sécurité de considérer les pouvoirs étendus d'enquête comme un bien incontestable face aux défis posés par le chiffrement, mais l'utilisation de ces pouvoirs peut saper considérablement la confiance du public et éroder leurs relations avec les collectivités qu'ils cherchent à protéger.

Les sections qui suivent du présent rapport sont axées sur le rôle que la vie privée joue dans la définition des limites de l'exercice des pouvoirs de l'État ainsi que sur la dynamique complexe de la confiance lorsqu'il s'agit de l'utilisation de ce pouvoir par des agents de l'État tels que la police et les services de sécurité. Ainsi, elles visent à démontrer que le débat actuel sur l'accès

[14] Outre les travaux cités précédemment, consulter Penney, S. et Gibbs, D. « Law Enforcement Access to Encrypted Data: Legislative Responses and the Charter », *Revue de droit de McGill Law*, vol. 63, nº 2, 2017, p. 201-45; Dheri, P. et Cobey, D. *Lawful Access & Encryption in Canada; A Policy Framework Proposal*, 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3470957 (consulté le 11 septembre 2023); Parsons, C. « Canada's New and Irresponsible Encryption Policy How the Government of Canada's New Policy Threatens Charter Rights, Cybersecurity, Economic Growth, and Foreign Policy », Citizen Lab (Université de Toronto), 2019, https://citizenlab.ca/2019/08/canadas-new-and-irresponsible-encryption-policy-how-the-government-of-canadas-new-policy-threatens-charter-rights-cybersecurity-economic-growth-and-foreign-policy/ (consulté le 11 septembre 2023); West, L. et Forcese, C. « Twisted into Knots: Canada's Challenges in Lawful Access to Encrypted Communications », *Common Law World Review*, vol. 49, nºs 3 et 4, 2020, p. 182-98; et Masoodi, M.J. et Rand, A. *Why Canada Must Defend Encryption*, 2021, https://static1.squarespace.com/static/5e9ce713321491043ea045ef/t/61401f669251e7128c8bf757/1631592298920/WhyCanadaMustDefendEncryption_V5.pdf (consulté le 11 septembre 2023).

[15] À cet égard, les discussions de ce genre font écho à des débats élargis et de longue date sur l'équilibre à atteindre entre la sécurité et les droits de la personne dans les démocraties constitutionnelles comme le Canada, la question centrale étant celle de savoir dans quelle mesure nous sommes prêts à laisser l'État enfreindre ou affaiblir certains droits (tel que celui à la vie privée) en échange de la promesse d'une sûreté et d'une sécurité accrues.

légal porte autant sur la manière dont nous envisageons la relation entre le public et l'État que sur les défis posés par le chiffrement et le respect des droits individuels.

ACCÈS LÉGAL ET VALEUR DE LA VIE PRIVÉE

Jusqu'à présent, les préoccupations liées aux répercussions de l'élargissement de l'accès légal au Canada – en particulier en ce qui concerne l'utilisation du chiffrement pour sécuriser les données en transit et au repos – se sont largement concentrées sur deux volets connexes de la vie privée, à savoir l'importance du droit à la vie privée en tant que droit individuel et la relation entre le droit à la vie privée et les autres droits protégés par la *Charte* (comme ceux à la liberté d'expression et à la liberté d'association). En ce qui concerne le premier point, la société civile et les défenseurs des droits de la personne ont à plusieurs reprises attiré l'attention sur le rôle important que le chiffrement joue dans la protection de la vie privée. À une époque où les activités quotidiennes se déroulent de plus en plus en ligne et où les capacités de surveillance de l'État et du secteur privé ne cessent de s'élargir, les Canadiens se sont à juste titre tournés vers le chiffrement comme moyen relativement accessible d'obtenir un certain degré de protection de leur vie privée dans leur vie numérique. Comme les auteurs du rapport *Shining a Light* l'ont fait observer :

> [TRADUCTION] Le chiffrement est essentiel pour préserver la confidentialité et l'intégrité d'innombrables interactions numériques à une époque où la communication s'effectue sur des flux de trafic mondialisés qui font régulièrement l'objet d'une surveillance massive et non ciblée de la part d'un éventail d'organismes gouvernementaux à l'échelle mondiale. Le chiffrement constitue de plus en plus l'une des seules mesures de protection fiables et pragmatiques contre cette surveillance étatique non ciblée, car il crée des espaces privés qui seraient autrement impossibles en ligne[16].

Ces espaces privés sont virtuels, mais il ne faut pas sous-estimer leur importance. Grâce aux communications numériques et à la consommation de médias électroniques, et en tant que membres de collectivités virtuelles, les Canadiens peuvent explorer certains volets de leur identité, nouer des relations personnelles et intimes, et échanger des opinions et des renseignements avec d'autres personnes. La facilité d'accès aux applications de communication chiffrées – comme Signal, Telegram et WhatsApp – et l'intégration du chiffrement sur appareil

[16] Gill, Israel et Parsons. *Shining a Light on the Encryption Debate*, 2018 (nº 8 ci-dessus), p. 12.

par des sociétés comme Apple et Microsoft ont permis aux individus de maintenir un certain degré de confidentialité dans leurs activités en ligne et d'éviter les effets dissuasifs du regard scrutateur du gouvernement, des entreprises privées et d'autres personnes.

Comme l'ont fait remarquer de nombreux commentateurs, la valeur de la vie privée va toutefois au-delà des justifications fondées sur les notions d'autonomie personnelle, d'identité et d'autodétermination[17]. Également, le droit à la vie privée est important parce qu'il constitue le fondement de l'exercice d'autres libertés et droits fondamentaux, au premier rang desquels figurent la liberté d'expression et la liberté d'association. En permettant aux individus de limiter l'accès à leurs communications – et d'établir à qui ils transmettent leurs idées et leurs renseignements –, le droit à la vie privée favorise la création d'espaces dans lesquels les opinions et croyances différentes peuvent s'épanouir. Comme le souligne la National Academy of Sciences des États-Unis :

> [TRADUCTION] Depuis l'explosion de l'accès à Internet et des capacités de communication électronique dans le monde, l'exercice des libertés d'expression et de croyance, y compris le droit d'obtenir des renseignements, dépend de plus en plus de la capacité d'accéder à Internet et de communiquer par voie électronique. Étant donné que les communications électroniques et l'accès à Internet font l'objet d'une surveillance électronique, le droit à la vie privée pour les communications, opinions et activités politiques et religieuses, entre autres choses, est devenu encore plus important […]. Ces faits nouveaux ont mené à la conclusion selon laquelle le chiffrement, qui protège la confidentialité des communications et des renseignements de nature délicate, fait maintenant partie intégrante des droits à la liberté d'expression et de croyance[18].

Sous cet angle, il est clair que le droit à la vie privée a une dimension politique indubitable. Dans la mesure où la liberté d'expression, la liberté d'association et la liberté de croyance sont essentielles au bon fonctionnement de toute démocratie saine, le droit à la vie privée est d'une importance fondamentale. En l'absence du droit à la vie privée, il est plus difficile pour les

[17] Consulter Regan, P.M. *Legislating Privacy: Technology, Social Values, and Public Policy*, University of North Carolina Press, 1995; Solove, D.J. *Understanding Privacy*, Harvard University Press, 2002; Solove, D.J. *The Digital Person: Technology and Privacy in the Information Age*, New York University Press, 2004; et Nissenbaum, H. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press, 2009.

[18] National Academies of Sciences, Engineering, and Medicine. *Decrypting the Encryption Debate: A Framework for Decision Makers*, National Academies Press, 2018, p. 34.

individus et les collectivités de s'organiser politiquement ou de se mobiliser dans des formes de résistance politique. C'est particulièrement le cas pour les populations vulnérables et les personnes politiquement marginalisées qui sont confrontées à un État antagoniste :

> Le chiffrement et l'anonymat, qu'ils soient utilisés séparément ou conjointement, instaurent un espace de confidentialité qui sert à protéger les opinions et les convictions. Par exemple, ils rendent possibles les communications privées et sont capables de mettre les opinions à l'abri de la curiosité extérieure, ce qui est particulièrement important dans les environnements politiques, sociaux, religieux ou juridiques hostiles. Lorsque les États imposent une censure illégale en imposant des techniques telles que le filtrage, le chiffrement et l'anonymat peuvent permettre aux citoyens de contourner ces obstacles et d'accéder à l'information et aux idées sans que les autorités ne s'en mêlent[19].

Nous sommes réticents à l'idée de considérer l'environnement politique, social, religieux et juridique canadien comme hostile lorsque nous examinons les questions liées à l'accès légal et les pouvoirs de la police et des services de sécurité, mais il est important que ces examens aillent au-delà du présent. Une fois accordés, les pouvoirs conférés aux agents de l'État comme la police sont rarement retirés ou réduits. Bien que nous ne nous préoccupions pas de l'utilisation abusive de ces pouvoirs dans le climat politique actuel, la situation pourrait changer. De même, avant d'étendre les capacités de surveillance de l'État pour permettre à la police et aux services de sécurité d'utiliser des outils d'enquête sur appareil ou d'autres formes de piratage légal, les législateurs et le public doivent prendre en compte le risque que ces capacités soient utilisées à mauvais escient à l'avenir. Autrement dit, la protection de la vie privée et le maintien des limites de l'accès légal visent autant à [TRADUCTION] « protéger l'avenir » des droits politiques essentiels qu'à les garantir actuellement[20].

Comme il a déjà été mentionné, ces deux volets de la vie privée – personnel et politique – ont été évoqués à maintes reprises dans les discussions sur l'accès légal et le chiffrement au Canada au cours des vingt dernières années. Il existe cependant un autre volet de la vie privée qui mérite

[19] Kaye, D. *Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression*, Conseil des droits de l'homme des Nations Unies (CDHNU), 29e session, Doc. NU A/HRC/29/32, 2015, p. 6 (para 12).

[20] Sur ce point et plus généralement sur la relation entre la surveillance et la répression, consulter Haggerty, K. « What's Wrong with Privacy Protections? Provocations from a Fifth Columnist », dans A. Sarat (éd.), *A World without Privacy: What Law Can and Should Do?* Oxford University Press, 2014, p. 190-222.

d'être pris en compte dans ce contexte. Il s'agit de l'idée selon laquelle la vie privée est essentielle à la primauté du droit et qu'elle limite considérablement les pouvoirs de l'État. Cet argument a été présenté par la professeure Lisa Austin, qui a fait observer que l'approche actuelle en matière de droit à la vie privée au Canada – particulièrement en ce qui concerne les questions de surveillance de l'État – était trop restrictive :

> [TRADUCTION] Mon argument est que ces volets fondamentaux de la primauté du droit ont implicitement façonné notre définition juridique de la vie privée, mais qu'ils l'ont fait de manière partielle et d'une manière qui soutient une facette étroite de la vie privée. La conséquence ironique est que le discours juridique sur la vie privée contribue maintenant souvent à appuyer l'élargissement du pouvoir discrétionnaire des agents de l'État plutôt qu'à le limiter, ce qui met en péril la primauté du droit plutôt que de la maintenir. Afin de mieux répondre aux nouvelles formes de surveillance, notre jurisprudence concernant le droit à la vie privée doit être plus explicite et mieux comprendre les exigences de ces principes fondamentaux de la primauté du droit[21].

Selon Austin, le droit à la vie privée établi par la *Charte* – qui découle de l'interdiction des perquisitions et saisies abusives prévue à l'article 8 – n'est pas fondé sur des idées de propriété, mais plutôt sur un engagement à l'égard de la primauté du droit et la nécessité de limiter le pouvoir de l'État[22]. Sous cet angle, la vie privée joue un rôle important dans la réglementation (et la restriction) du pouvoir discrétionnaire de la police et des services de sécurité en contribuant à voir à ce que ceux qui ont un pouvoir sur nous l'exercent d'une manière compatible avec les valeurs de la primauté du droit, notamment la responsabilité et la transparence.

Pour mieux comprendre la vision d'Austin, il est utile de revenir sur les récentes révélations faites au sujet de l'utilisation d'outils d'enquête sur appareil par la GRC. Même si la GRC doit obtenir une autorisation judiciaire avant d'avoir recours à une telle technologie, le manque de transparence par rapport à l'utilisation de ces outils soulève d'importantes questions en matière de primauté du droit, notamment en ce qui concerne la notification équitable. Étant donné qu'il était impossible pour les individus de savoir avant 2022 que la GRC utilisait des outils d'enquête

[21] Austin, L. « Getting Past Privacy? Surveillance, the Charter, and the Rule of Law », *Revue canadienne de droit et société*, vol. 27, p. 381-98, 383.

[22] Austin, L. « Enough about Me: Why Privacy Is about Power, not Consent (or Harm) » dans A. Sarat (éd.), *A World without Privacy: What Law Can and Should Do?* Cambridge University Press, 2014.

sur appareil, ils n'étaient pas en mesure de prendre des décisions éclairées au sujet de leurs appareils personnels et des renseignements qui y étaient stockés. Comme l'a souligné Austin :

> [TRADUCTION] Il existe une forte tradition quant à la compréhension de la valeur de la primauté du droit au chapitre de sa capacité d'orienter la prise de mesures. Dans cette optique, l'élément central de la primauté du droit est la capacité des individus de planifier leurs activités à la lumière de leur responsabilité juridique potentielle. Des valeurs telles que la prévisibilité des attentes sont essentielles à cette compréhension. On a établi un lien entre ce rôle de planification et l'idée de liberté juridique, mais aussi les idées d'autonomie et de dignité[23].

Sous cet angle, l'utilisation d'outils d'enquête sur appareil par la GRC était problématique non seulement sur le plan du droit à la vie privée des individus – et des droits connexes à la liberté d'expression et d'association –, mais également sur celui de la primauté du droit. Bien qu'elle soit importante, la responsabilité légale par le biais de la surveillance judiciaire ne permet qu'en partie de voir à ce que la police soit assujettie convenablement à la primauté du droit. En outre, il doit y avoir une transparence de l'éventail des pouvoirs et des techniques d'enquête dont elle dispose. C'est un point qui a été souligné par le commissaire à la protection de la vie privée, Philippe Dufresne, dans son témoignage récent au Comité ETHI :

> [L]es répercussions de la révélation de ce type d'information par des reportages ou des questions des médias peuvent susciter des interrogations et des inquiétudes. Je pense que, du point de vue de la confiance, il serait de loin préférable que des évaluations des facteurs relatifs à la protection de la vie privée soient effectuées en amont, que mon bureau soit consulté et que cette information puisse être transmise d'une manière ou d'une autre aux Canadiens, afin qu'ils soient rassurés sur le fait qu'il existe des institutions, comme mon bureau, qui fournissent des conseils et s'assurent que la protection de la vie privée est une priorité[24].

Il est important d'intégrer les questions relatives à la primauté du droit dans les discussions sur l'accès légal et le chiffrement, car cela nous rappelle que le droit à la vie privée ne consiste pas seulement à protéger des intérêts individuels ou à faciliter l'exercice d'autres droits. Il s'agit également d'imposer des contraintes importantes au pouvoir de l'État. En fait, Jed Rubenfeld et d'autres intervenants ont fait valoir que le fait de se concentrer exclusivement sur les volets de

[23] Austin. 2012 (nº 21 ci-dessus), p. 386-87 (note de bas de page originale omise).

[24] *Rapport du Comité permanent sur les outils d'enquête sur appareil* (nº 5 ci-dessus), p. 13.

[TRADUCTION] « l'identité individuelle » de la vie privée était une erreur et que nous devions plutôt placer l'État au cœur de notre analyse :

> [TRADUCTION] Le droit à la vie privée est une doctrine politique. Il n'existe pas parce que les individus ont une sphère de vie « privée » avec laquelle l'État n'a rien à voir. L'État a tout à voir avec notre vie privée, et la liberté que protège le droit à la vie privée s'étend également, comme nous l'avons vu, aux questions « publiques » comme aux questions « privées ». Le droit à la vie privée existe parce que la démocratie doit imposer des limites à l'étendue du contrôle et de la direction que l'État exerce sur la manière dont les individus mènent leur vie de tous les jours[25].

L'idéologie « antitotalitaire » de la vie privée de Rubenfeld a été critiquée, mais son idée clé selon laquelle la vie privée peut jouer un rôle important en limitant les tendances expansionnistes de l'État est importante dans le contexte de l'accès légal[26]. Si bien intentionnés que soient la police et les services de sécurité, leurs appels à disposer de plus d'outils pour résoudre le problème « going dark » et les défis du chiffrement nous obligent à nous poser une question fondamentale : jusqu'où sommes-nous prêts, en tant que membres d'une démocratie constitutionnelle, à laisser l'État s'immiscer dans nos vies dans le but d'assurer la sûreté et la sécurité publique? Les préoccupations relatives à la vie privée, à la liberté d'expression, à la liberté d'association et à la primauté du droit nous permettent de répondre en partie à cette question, mais nous devons également nous pencher sur des questions plus vastes concernant le rôle de l'État et les limites de son pouvoir.

Nous apportons une perspective différente au débat sur le problème « going dark », mais nous plaçons aussi l'État au cœur de notre analyse, ce qui est également utile lorsqu'il s'agit d'aborder l'une des caractéristiques uniques du chiffrement, à savoir la possibilité d'une protection absolue de la vie privée. Comme le soulignent souvent les organismes d'application de la loi, le recours au chiffrement est différent d'autres formes de protection de la vie privée – comme les mécanismes de verrouillage, les mots de passe et les codes – en ce sens qu'il ne rend pas l'accès de l'État à certains types de renseignements personnels seulement plus difficile; dans certains cas, le chiffrement rend cet accès à peu près impossible. Dans l'optique de l'État canadien

[25] Rubenfeld, J. « The Right to Privacy », *Harvard Law Review*, vol. 102, 1989, p. 737-807 et 804-5 (la note de bas de page originale a été omise).

[26] Solove, D.J. « Conceptualizing Privacy », *California Law Review*, vol. 90, nº 4, 2002, p. 1087-155 et 1120.

moderne – qui n'a cessé d'étendre ses pouvoirs de surveillance au cours du siècle dernier –, l'idée que les individus puissent désormais empêcher facilement les organismes d'application de la loi d'accéder à leurs renseignements est inquiétante. Cependant, pour ceux qui s'inquiètent de la portée de plus en plus grande de la surveillance étatique, l'avènement du chiffrement est une bonne nouvelle, notamment parce qu'il nous oblige à nous demander si une vie privée absolue devrait être possible dans une démocratie comme le Canada. Autrement dit, si le seul moyen de lutter contre le problème « going dark » est de restreindre l'utilisation du chiffrement – ou de permettre aux organismes d'application de la loi d'avoir recours à des moyens trompeurs pour le contourner –, nous sommes obligés de nous poser la question suivante : « Y a-t-il des choses que l'État ne peut tout simplement pas savoir sur nous[27]? »

Enfin, lorsqu'on réfléchit à l'accès légal et au droit à la vie privée, il est utile de se pencher sur d'autres contextes dans lesquels la loi impose des contraintes importantes pour les personnes qui participent à l'administration de la justice pénale. L'analogie est loin d'être parfaite, mais un engagement fort à l'égard du droit à la vie privée dans le contexte du maintien de l'ordre contribue à uniformiser les règles du jeu entre les individus et l'État d'une manière qui n'est pas différente des droits à l'application régulière de la loi dans le contexte des procès criminels. Tout comme la loi place délibérément des obstacles devant la police et les procureurs par le biais de règles de procédure et de preuve qui tiennent compte du vaste déséquilibre du pouvoir entre les personnes accusées d'une infraction pénale et la Couronne, les restrictions à l'accès légal servent à limiter le pouvoir de surveillance de l'État. Autrement dit, il *devrait* être difficile pour la police et les services de sécurité d'accéder aux renseignements chiffrés, ne serait-ce que parce que les individus sont déjà fortement désavantagés lorsqu'il s'agit de maintenir un certain degré de confidentialité à l'égard de l'État.

SURVEILLANCE, TRANSPARENCE ET CONFIANCE

À l'extérieur du cadre du droit à la vie privée, les discussions sur l'accès légal au Canada ont soulevé des préoccupations au sujet des répercussions éventuelles sur la confiance du public – à

[27] Je remercie Robert Diab pour ses réflexions sur la relation entre le chiffrement et la protection absolue de la vie privée.

l'égard de la sécurité offerte par les technologies de chiffrement et envers les organismes d'application de la loi et les autres institutions de l'État. En ce qui concerne le premier type de confiance du public, il suffit peut-être de reconnaître ici que les technologies de chiffrement sont fondamentales pour le commerce (en particulier le marché numérique) et qu'il y a des coûts économiques assez évidents qui découleraient de l'affaiblissement de la confiance du public à l'égard de ces technologies. C'est le deuxième type de confiance du public – la confiance envers la police, les services de sécurité et l'État en général – qui sera examiné dans la présente section, particulièrement en ce qui touche sa relation avec l'accès légal, la surveillance et le chiffrement.

Le maintien de la confiance envers le gouvernement et les institutions de l'État est souvent cité comme une raison de limiter l'accès légal pour la police et les services de sécurité, mais ce que l'on entend par confiance et la raison pour laquelle elle est importante dans ce contexte ne sont pas toujours clairs. Dans certains cas, la confiance est simplement présentée comme un bien *en soi*, et la nécessité de maintenir la confiance du public sert en tant que motif justifiant la transparence et la responsabilité accrues en matière de maintien de l'ordre et de surveillance de l'État. Cependant, plus récemment, la confiance a été définie en fonction de son rôle dans la promotion de la participation démocratique et de la mobilisation publique. Par exemple, dans le témoignage qu'il a livré au Comité ETHI lors de son enquête sur l'utilisation d'outils d'enquête sur appareil par la GRC, le commissaire à la protection de la vie privée du Canada a établi un lien direct entre le droit à la vie privée, la confiance et l'engagement du public envers le gouvernement :

> La protection de la vie privée comme moyen d'accentuer la confiance des Canadiens envers leurs institutions et en tant que citoyens de la société numérique signifie que lorsque des organismes comme la GRC tiennent compte de l'incidence sur la vie privée dès le départ et que les Canadiens le voient, ces derniers se sentent confiants et rassurés quant à la nécessité des outils et des mesures mis en place pour atténuer l'incidence sur la vie privée et veiller à ce que les mesures et les objectifs soient proportionnels[28].

Dans la même veine, le ministre de la Sécurité publique, Marco Mendicino, a signalé le même jour que « la confiance [était] l'une des clés de l'ouverture et de la transparence », après quoi il a

[28] Témoignage au Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, 44e législature, 1re session, numéro 030 (lundi 8 août 2022), p. 2.

ajouté que « [n]ous devons maintenir la confiance partout pour pouvoir utiliser cet outil d'une façon qui respecte la *Charte* et tous les droits qu'elle prévoit[29] ».

Le fait de lier ainsi la confiance et la transparence – où la promotion de la confiance sert de motif justifiant une transparence accrue – peut sembler ne poser aucun problème, mais l'hypothèse selon laquelle une plus grande transparence est toujours et inévitablement une bonne chose mérite d'être examinée de plus près. C'est particulièrement le cas lorsqu'il s'agit de l'utilisation de technologies de surveillance par la police et les services de sécurité. Bien que la transparence soit souvent citée comme une condition préalable nécessaire à la responsabilité institutionnelle, elle peut également jouer un rôle dans la normalisation des activités qui devraient être considérées comme exceptionnelles. Dans la présentation d'un récent recueil de rapports universitaires sur la confiance, la transparence et la surveillance, les éditeurs ont fait remarquer que si nous considérons [TRADUCTION] « la transparence comme une pratique politique plutôt que comme la simple communication de renseignements, nous pouvons commencer à comprendre comment la transparence peut finir par avoir des effets contre-intuitifs, comme la légitimation, voir l'élargissement, des pouvoirs de surveillance de l'État[30] ». Dans un chapitre du même ouvrage, Lora Anne Viola affirme que, dans certains cas, la transparence – particulièrement lorsqu'elle fait suite à des révélations au sujet d'activités de surveillance de l'État non divulguées auparavant – peut avoir ce qu'elle appelle un *effet de cautionnement* :

> [TRADUCTION] [Cet effet] est déclenché lorsque des niveaux élevés de non-conformité révélée réduisent l'opprobre social perçu pour l'infraction à la norme et engendrent plutôt des demandes de normalisation ou de légitimation du comportement. Les révélations qui découlent de la transparence offrent l'occasion non seulement de condamner le comportement, comme pourrait le préconiser une approche de responsabilité, mais également d'en discuter et de le normaliser. Dans le cas de la surveillance, la divulgation d'une surveillance illégale a suscité l'indignation dans l'opinion publique et des débats sur la manière de la légaliser. Ainsi, sous l'apparence de dispositions législatives de réforme, de nombreuses pratiques de surveillance illégale dévoilées par Snowden se sont vu accorder un statut légal et, par conséquent, ont été légitimées. Il est permis de penser que les révélations généralisées sur la surveillance – non seulement par la NSA [National Security Agency], mais également par des entreprises privées comme Facebook – ont normalisé l'idée de la collecte et de l'utilisation de données de masse. L'exposition et la

[29] Témoignage au Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, 44e législature, 1re session, numéro 031 (lundi 8 août 2022), p. 5.

[30] Viola, L.A. et Laidler, P. *Trust and Transparency in an Age of Surveillance* (Routledge), 2022, p. 7.

> divulgation donnent à penser que le comportement est plus répandu que prévu, ce qui lève le tabou[31].

Pour revenir aux révélations de 2022 concernant l'utilisation d'outils d'enquête sur appareil par la GRC, il est facile de constater cet effet de cautionnement. Malgré les préoccupations initiales, le débat sur l'utilisation de cette technologie est rapidement passé de la question de savoir s'il fallait l'autoriser à celle de savoir comment on pouvait mieux la réglementer; les discussions sur la nécessité d'une transparence et d'une responsabilité accrues se sont retrouvées au cœur du débat. Dans cette optique, on peut faire valoir que les décideurs politiques et les législateurs doivent faire preuve de prudence lorsqu'ils reviennent sur des appels de longue date à un élargissement des pouvoirs d'accès légal; en effet, l'examen de nouvelles techniques d'enquête policière et technologies de surveillance, même lorsqu'elles s'accompagnent d'appels à une plus grande transparence et à une réglementation plus claire, peut avoir pour effet de les normaliser.

En présumant que les avantages d'une transparence accrue l'emportent sur les risques de tout effet de cautionnement potentiel en matière d'accès légal, on doit encore s'interroger sur l'objectif ultime, à savoir la promotion et le maintien de la confiance du public, dans le cadre des discussions sur le chiffrement et les pouvoirs de la police. Bien qu'elle soit rarement énoncée explicitement, l'importance accordée à la confiance dans les discussions sur l'accès légal repose sur une hypothèse clé : il existe une relation directe entre la surveillance, le droit à la vie privée et la confiance, et toute modification du régime d'accès légal – surtout les modifications qui portent atteinte à la vie privée des individus – peut entraîner l'érosion de cette confiance. En 2019, Dheri et Cobey se sont appuyés sur cette hypothèse pour plaider en faveur de l'élaboration et de la publication par les organismes d'application de la loi de leurs propres lignes directrices sur les pratiques exemplaires de contournement du chiffrement :

> [TRADUCTION] En ce moment, le public ne sait pas comment les organismes d'application de la loi et le portefeuille de Sécurité publique Canada dans son ensemble traitent le chiffrement. […] [L]a non-divulgation des politiques internes [au sujet du contournement du chiffrement] permet aux critiques de combler le vide par des spéculations, aussi exactes ou inexactes soient-elles. Or, les spéculations peuvent avoir

[31] Viola, L. A. « The Limits of Transparency as a Tool for Regulating Surveillance: A Comparative Study of the United States, United Kingdom, and Germany », dans Viola et Laidler (éd.) (2022) (idem), p. 21-46 et 28 (note de bas de page originale omise).

> des conséquences négatives sur la réputation d'un organisme et la confiance du public à son endroit, et elles peuvent même nuire aux objectifs légitimes d'application de la loi. Étant donné que les organismes canadiens d'application de la loi exercent leurs activités dans une période où règnent la méfiance et les « fausses nouvelles », et où les démocraties du monde entier sont menacées, les facteurs liés à la perception du public revêtent une importance encore plus grande. La mise en place et la communication de pratiques exemplaires de chiffrement constitueraient une étape importante en vue d'une plus grande transparence et d'une démocratie plus saine[32].

Cette même hypothèse étaye une grande partie de la discussion sur les outils d'enquête sur appareil au chapitre 1 du rapport de 2022 du Comité permanent. La nécessité de maintenir la confiance envers les institutions publiques – comme la police et les services de sécurité – est évoquée par plusieurs témoins en tant que motif justifiant une plus grande transparence de l'utilisation de ces technologies ainsi qu'une surveillance accrue de la part des autorités de protection de la vie privée et des tribunaux. Ce qui n'est pas abordé, en revanche, c'est la nature de la relation entre la surveillance, le droit à la vie privée et la confiance ou les raisons pour lesquelles une surveillance accrue entraîne une perte de confiance.

Il peut sembler évident que l'utilisation de technologies de surveillance par l'État est susceptible de miner la confiance du public – tant envers les institutions particulières chargées de la surveillance qu'envers l'État en général –, mais l'image qui se dégage de la documentation de recherche est moins claire. Comme l'a fait observer Björklund, il existe des éléments de preuve empiriques qui permettent de penser que [TRADUCTION] « des niveaux élevés de confiance prédisent un sentiment positif à l'égard de la surveillance[33] ». De façon plus précise, elle a fait référence à des sondages menés récemment en Europe qui ont démontré que le niveau de confiance envers les institutions de l'État, surtout les organismes de sécurité, pouvait avoir des répercussions positives sur la volonté du public d'accepter certains types de pratiques et technologies de surveillance. Par exemple, selon une étude réalisée en 2015 en Europe, il semble

[32] Dheri, P. and Cobey, D. *Lawful Access & Encryption in Canada: A Policy Framework Proposal*, 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3470957 (consulté le 11 septembre 2023), p. 29.

[33] Björklund, F. « Trust and Surveillance: An Odd Couple or a Perfect Pair? » dans Viola et Laidler (éd.), 2022 (nº 30 ci-dessus), p. 183. Björklund a également attiré l'attention sur des études de cas précises, dont un certain nombre portent sur la surveillance des collectivités musulmanes aux États-Unis et au Royaume-Uni, où il a été démontré que la surveillance avait l'effet inverse, ce qui a entraîné une perte de confiance envers les organismes d'État.

y avoir une relation claire entre la façon dont les gens perçoivent les services de sécurité et leur volonté d'accepter certains types de technologies de sécurité axées sur la surveillance :

> [TRADUCTION] Plus les gens font confiance aux institutions scientifiques et politiques, en l'occurrence les agents de sécurité, plus le recours à une technologie serait acceptable. Notre étude confirme clairement cette hypothèse. Cela signifie concrètement que, sur le plan des technologies de sécurité axées sur la surveillance, les organismes et institutions de sécurité devraient se préoccuper beaucoup plus du degré de confiance à leur endroit que de la question de savoir dans quelle mesure le public connaît les technologies. Si nous voulions en savoir plus sur les répercussions de chaque sous-dimension de la fiabilité institutionnelle sur l'acceptabilité, nous pourrions examiner d'autres analyses de ces données figurant dans d'autres publications et nous constaterions que la capacité, l'intégrité et la bienveillance des agents de sécurité jouent un rôle plus ou moins important dans le cas de chaque technologie précise de sécurité axée sur la surveillance[34].

Comme le soulignent les auteurs de cette étude, de nombreux autres facteurs peuvent influencer la manière dont le public réagit aux technologies de surveillance, notamment le caractère intrusif perçu, l'efficacité perçue et les préoccupations relatives à la protection de la vie privée. Ces résultats et d'autres conclusions semblables donnent à penser que les niveaux de confiance existants sont importants lorsqu'il s'agit de la volonté (ou de la réticence) du public d'accepter un élargissement des pouvoirs de surveillance de l'État. Étant donné que la confiance envers la GRC a chuté au cours des dernières années, toute mesure visant à étendre la portée de l'accès légal au Canada risque de se heurter à une résistance considérable de la part du public et de ne faire qu'exacerber les problèmes de confiance existants.

Si l'on revient au travail de Björklund sur la confiance, elle a souligné que les idées institutionnelles de confiance – telles que celles qui sous-tendent l'enquête citée ci-dessus – étaient problématiques parce que le public n'est souvent pas en mesure de juger de l'efficacité de pratiques de surveillance particulières ou du rendement d'organismes comme la police ou les services de sécurité. C'est pour cette raison que Björklund plaide en faveur d'études qui englobent également ce qu'elle appelle une perspective socioculturelle :

[34] Pavone, V., Degli-Esposti, S. et Santiago, E. *Key Factors Affecting Public Acceptance and Acceptability of SOSTs* (Institut Universitaire Européen), 2015, p. 136. Consulter également Degli-Esposti, S. et Santiago Gómez, E. « Acceptable Surveillance-Orientated Security Technologies: Insights from the SurPRISE Project », *Surveillance & Society*, vol. 13, nos 3 et 4), 2015, p. 437–454.

> [TRADUCTION] Le véritable mérite d'une perspective socioculturelle sur la confiance et la surveillance est qu'elle peut rendre compte de mouvements ascendants qui illustrent ce qui se passe dans la vie quotidienne des gens. Les normes ne sont pas faciles à modifier, mais d'un point de vue socioculturel, la confiance en tant que norme trouve son origine dans les expériences que nous vivons avec les personnes qui font partie de nos contacts quotidiens et de nos réseaux personnels. Par conséquent, une perspective socioculturelle tient compte de la possibilité que la surveillance mine la confiance telle que nous la connaissons. Si la confiance est une question de socialisation et découle d'expériences vécues dans des relations étroites, les expériences négatives vécues par exemple avec la police locale peuvent miner la confiance par le bas et avoir des effets à long terme sur d'autres types de confiance et sur les normes de confiance au sein d'une société. Ainsi, les études sociales révèlent l'existence d'une relation positive entre la confiance et l'acceptation de la surveillance, mais les études de cas plus qualitatives mentionnées ci-dessus, qui font état d'une association négative, peuvent nous renseigner sur ce que nous devrions attendre de l'avenir[35].

Ce qui est sous-entendu ici, c'est que la confiance fonctionne à différents niveaux et peut aller dans différentes directions. Un niveau élevé de confiance envers la police en tant qu'institution pourrait amener le public à accepter plus facilement certains types de surveillance, mais en même temps, les expériences réelles vécues par les individus et les collectivités exposés à cette surveillance peuvent entraîner une perte de confiance ultérieure, à la fois envers la police et envers l'État de manière plus générale. Si l'on revient au contexte de l'accès légal et du chiffrement, il laisse supposer que la *manière* dont la police et les services de sécurité utilisent les nouvelles technologies et les nouveaux pouvoirs visant à lutter contre le problème « going dark » jouera probablement un rôle dans le renforcement (ou l'érosion) de la confiance. Par exemple, si l'utilisation des techniques d'accès légal s'accroît – et si ces dernières servent principalement à enquêter sur des individus et des collectivités qui subissent déjà des excès de zèle de la part des policiers –, la confiance du public risque d'en pâtir. Dans l'ensemble, les perspectives institutionnelles et socioculturelles sur la confiance montrent que, dans le contexte de la surveillance à tout le moins, la confiance est une *ressource* qui peut être utilisée lors de la mise en place de nouvelles mesures de surveillance, mais elle peut facilement se perdre en fonction de la manière dont ces mesures sont mises en œuvre et vécues par le public.

Avant d'aborder les questions de transparence et de confiance, il est important de s'attaquer aux questions de portée par rapport à l'accès légal et au débat sur le problème « going dark ».

[35] Björklund. 2022 (nº 33 ci-dessus), p. 194.

D'abord, on peut affirmer que les efforts que la police et les services de sécurité déploient pour venir à bout du chiffrement sont plus susceptibles d'être de portée limitée et de viser un très petit nombre d'individus et d'organisations criminelles[36]. Par conséquent, il convient d'être prudent lors de l'examen des répercussions probables de ces mesures sur la confiance du public envers la police et les services de sécurité. Cela dit, il est également important de tenir compte de deux facteurs connexes, à savoir l'omniprésence du chiffrement et les risques du détournement de fonction. Étant donné que le chiffrement des données au repos et en transit est désormais très répandu, les organismes d'application de la loi pourraient avoir davantage recours à l'avenir à des techniques comme le piratage légal et les outils d'enquête sur appareil, dont l'utilisation est actuellement limitée, notamment parce que la technologie connexe nécessaire devient moins coûteuse et plus facile à déployer. C'est certainement le cas pour d'autres formes de surveillance policière au Canada, y compris l'écoute électronique et la vidéosurveillance. Par conséquent, toute discussion sur l'élargissement de l'accès légal doit partir du principe que l'utilisation du contournement du chiffrement pourrait devenir courante au fil du temps.

Dans le même ordre d'idées, l'argument selon lequel le piratage légal et l'utilisation d'outils d'enquête sur appareil ne serviront probablement que dans le cadre d'enquêtes sur des crimes graves ou sur le terrorisme est fort sujet à caution. Les technologies de surveillance sont caractérisées par une tendance bien établie au détournement de fonction et sont souvent utilisées d'une manière qui n'était pas prévue à l'origine au moment de leur élaboration ou de leur déploiement[37]. En outre, cette tendance est souvent accentuée par des événements qui suscitent une crainte par rapport à la criminalité, à la sûreté et à la sécurité publique, comme on l'a constaté dans les années qui ont suivi les attentats du 11 septembre 2001 et, plus récemment, lors de la pandémie de COVID-19[38]. Une fois que le recours à des pouvoirs exceptionnels d'accès légal a été autorisé par la loi et normalisé par des efforts visant à garantir la transparence et la

[36] Consulter, par exemple, les déclarations faites au Comité ETHI dans le cadre de son enquête sur l'utilisation d'outils d'enquête sur appareil. Rapport du Comité permanent sur les outils d'enquête sur appareil (nº 5 ci-dessus), p. 21.

[37] Koops, B. J. « The concept of function creep », *Law, Innovation and Technology*, vol. 13, nº 1, 2021, p. 29–56.

[38] Consulter Lyon, D. et Haggerty, K. D. « The surveillance legacies of 9/11: Recalling, reflecting on, and rethinking surveillance in the security era », *Canadian Journal of Law and Society*, vol. 27, nº 3, 2012, p. 291-300; et Newell, B. « Introduction: surveillance and the COVID-19 pandemic: views from around the world », *Surveillance & Society*, vol. 19, nº 1, 2021, p. 81–84.

responsabilité, il devient relativement facile de les utiliser dans des contextes qui vont bien au-delà du problème « going dark ». Comme il est mentionné ci-dessus, la perspective d'un élargissement de l'accès légal à l'avenir – particulièrement en ce qui concerne l'utilisation du chiffrement – ne devrait pas nécessairement empêcher les décideurs politiques, les législateurs, les organismes d'application de la loi et le public de discuter du mérite des nouvelles technologies et de l'élargissement des pouvoirs. Cependant, nous devons être lucides sur le fait que, comme l'histoire l'a démontré à maintes reprises, une fois qu'elles ont été autorisées par la loi et que leur utilisation est devenue normalisée, les pratiques et technologies de surveillance sont rarement, voire jamais, réexaminées, suspendues ou abandonnées de quelque manière que ce soit.

CONCLUSION

Au cours des vingt dernières années, les discussions sur le chiffrement, les pouvoirs de la police et l'accès légal au Canada ont été axées sur une série de questions liées au droit à la vie privée, à la transparence et à la confiance. Le présent rapport a cherché à mettre en lumière certains volets négligés de chacune de ces questions, notamment les suivants :

(1) La relation entre le droit à la vie privée, la primauté du droit et les limites du pouvoir de l'État;

(2) Le rôle que la transparence peut jouer dans l'approbation ou la légitimation des formes de surveillance de l'État;

(3) La nature complexe de la confiance à l'égard du contexte de la surveillance, particulièrement en ce qui concerne le sentiment du public envers la police et les services de sécurité.

En tentant de démontrer que la valeur du droit à la vie privée va au-delà de son statut de droit individuel – et que la relation entre la transparence, la confiance et la surveillance est intrinsèquement complexe et multidirectionnelle –, le présent rapport vise à offrir aux membres du Comité des parlementaires sur la sécurité nationale et le renseignement des points de vue supplémentaires sur le débat relatif au problème « going dark ». En particulier, le présent rapport doit être considéré comme un appel à placer notre vision de l'État au centre de toute discussion sur l'accès légal, les pouvoirs de la police et les défis du chiffrement. Trop souvent, les débats sur

les nouvelles formes de surveillance partent du principe qu'il incombe aux individus et aux collectivités d'expliquer pourquoi l'État ne devrait pas être en mesure d'étendre ses pouvoirs de surveillance en réponse à une menace nouvellement détectée pour la sûreté ou la sécurité publique. À cet égard, le public joue presque toujours un rôle de « défenseur », car il doit expliquer pourquoi le droit à la vie privée est encore important et pourquoi des limites doivent être imposées aux nouvelles technologies de surveillance policière. Toutefois, si nous partons d'un point différent, c'est-à-dire si nous admettons qu'il peut y avoir des choses que l'État ne peut pas savoir et des endroits où il ne peut pas aller, la discussion prendra alors une tournure différente.

Le chiffrement représente clairement un défi important pour la police et les services de sécurité. Que le problème « going dark » ait été surestimé ou non par les organismes d'application de la loi au Canada, il ne fait aucun doute que le chiffrement rend les enquêtes sur les crimes graves plus difficiles. Mais le chiffrement, pour la première fois peut-être, offre également aux individus la possibilité de jouir d'une vie privée absolue, car il fixe des limites réelles aux pouvoirs de surveillance croissants de l'État. Par conséquent, les débats sur l'avenir de l'accès légal au Canada doivent aller au-delà de la tension entre les droits individuels et la recherche de la sécurité, et s'inscrire plutôt plus largement dans le cadre d'une discussion permanente sur la relation fondamentale entre l'État canadien et la population à qui il offre des services.

RÉFÉRENCES

Austin, L. « Getting Past Privacy? Surveillance, the Charter, and the Rule of Law », *Revue canadienne de droit et société*, vol. 27, 2012, p. 381-98.

—— « Enough about Me: Why Privacy Is about Power, not Consent (or Harm) » dans A. Sarat (éd.), *A World without Privacy: What Law Can and Should Do?* Cambridge University Press, 2014.

Björklund, F. « Trust and Surveillance: An Odd Couple or a Perfect Pair? » dans L.A. Viola et P. Laidler, *Trust and Transparency in an Age of Surveillance* (Taylor & Francis), 2022.

Association canadienne des chefs de police. « Résolutions adoptées à la 111e Conférence annuelle », 2016 (août 2016), https://www.cacp.ca/r_solution.html (consulté le 31 octobre 2023).

Degli-Esposti, S. et Santiago Gómez, E. « Acceptable Surveillance-Orientated Security Technologies: Insights from the SurPRISE Project », *Surveillance & Society*, vol. 13, nos 3 et 4), 2015, p. 437-454.

Dheri, P. et Cobey, D. « Lawful Access and Encryption in Canada: A Policy Framework Proposal », 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3470957 (consulté le 11 septembre 2023).

Diab, R. « The Road Not Taken: Missing Powers to Compel Decryption in Bill C-59, Ticking Bombs, and the Future of the Encryption Debate », *Alberta Law Review*, vol. 57, 2019, p. 267-96.

Les Associés de recherche EKOS. « Attitudes à l'égard du Service canadien du renseignement de sécurité (SCRS) : Rapport », 2021, https://publications.gc.ca/collections/collection_2021/scrs-csis/PS74-8-2-2021-fra.pdf (consulté le 31 octobre 2023).

Chambre des communes (Canada). Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique. Témoignages : numéro 030 (lundi 8 août 2022), 44e législature, 1re session, 2022, https://publications.gc.ca/collections/collection_2022/parl/xc73-1/XC73-1-2-441-30-fra.pdf (consulté le 15 novembre 2023).

—— Témoignages : numéro 031 (lundi 8 août 2022), 44e législature, 1re session, 2022, https://publications.gc.ca/collections/collection_2022/parl/xc73-1/XC73-1-2-441-31-fra.pdf (consulté le 15 novembre 2023).

—— Témoignages : numéro 032 (mardi 9 août 2022), 44e législature, 1re session, 2022, https://publications.gc.ca/collections/collection_2022/parl/xc73-1/XC73-1-2-441-32-fra.pdf (consulté le 15 novembre 2023).

—— Témoignages : numéro 033 (mardi 9 août 2022), 44e législature, 1re session, 2022, https://publications.gc.ca/collections/collection_2022/parl/xc73-1/XC73-1-2-441-33-fra.pdf (consulté le 15 novembre 2023).

Forrest, M. « Canada's National Police Force Admits Use of Spyware to Hack Phones », *Politico*, 2022 (29 juin 2022), https://www.politico.com/news/2022/06/29/canada-national-police-spyware-phones-00043092 (consulté le 23 août 2023).

Gill, L., Israel, T. et Parsons, C. *Shining a Light on the Encryption Debate*: *A Canadian Field Guide*, Citizen Lab et Clinique d'intérêt public et de politique d'Internet du Canada Samuelson-Glushko, 2018, https://citizenlab.ca/wp-content/uploads/2018/05/Shining-A-Light-Encryption-CitLab-CIPPIC.pdf (consulté le 24 août 2023).

Gouvernement du Canada. *Notre sécurité, nos droits* : *Livre vert sur la sécurité nationale de 2016*, 2016, https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/ntnl-scrt-grn-ppr-2016-bckgrndr/index-fr.aspx (consulté le 11 septembre 2023).

—— *Réponse du gouvernement au septième rapport du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique*, 2022, https://www.ourcommons.ca/content/Committee/441/ETHI/GovResponse/RP12299295/441_ETHI_Rpt07_GR/TreasuryBoardOfCanada-f.pdf (consulté le 15 novembre 2023).

Haggerty, K. « What's Wrong with Privacy Protections? Provocations from a Fifth Columnist », dans A. Sarat (éd.), *A World without Privacy: What Law Can and Should Do?* Cambridge University Press, 2014.

Chambre des communes. Ordre/adresse de la Chambre des communes, Q-566, document parlementaire 8555-441-566 (22 juin 2022).

Chambre des communes (Canada). Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique. *Outils d'enquête sur appareil utilisés par la Gendarmerie royale du Canada et enjeux liés*, rapport (novembre 2022), 44e législature, 1re session, 2022, https://www.ourcommons.ca/Content/Committee/441/ETHI/Reports/RP12078716/ethirp07/ethirp07-f.pdf (consulté le 31 octobre 2023).

Chambre des communes (Canada). Comité permanent de la sécurité publique et nationale. *Protéger les Canadiens et leurs droits* : *une nouvelle feuille de route pour la sécurité nationale du Canada*, rapport (mai 2017), 42e législature, 1re session, 2017, https://publications.gc.ca/collections/collection_2017/parl/xc76-1/XC76-1-1-421-9-fra.pdf (consulté le 31 octobre 2023).

Koops, B. J. « The concept of function creep », *Law, Innovation and Technology*, vol. 13, no 1, 2021, p. 29-56.

Kaye, D. *Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression*, CDHNU, 29e session, Doc. NU A/HRC/29/32, 2015.

Lyon, D. et Haggerty, K. D. « The surveillance legacies of 9/11: Recalling, reflecting on, and rethinking surveillance in the security era », *Canadian Journal of Law and Society*, vol. 27, nº 3, 2012, p. 291-300.

Marhnouj, S. « CSIS survey finds majority of Canadians leery of giving more powers to police, intelligence agencies », *The Globe and Mail*, 2022 (16 janvier 2022), https://www.theglobeandmail.com/politics/article-csis-survey-finds-canadians-leery-of-giving-more-powers-to/ (consulté le 14 novembre 2023).

Masoodi, M.J. et Rand, A. *Why Canada Must Defend Encryption*, 2021, https://static1.squarespace.com/static/5e9ce713321491043ea045ef/t/61401f669251e7128c8bf757/1631592298920/WhyCanadaMustDefendEncryption_V5.pdf (consulté le 11 septembre 2023).

National Academies of Sciences, Engineering and Medicine. *Decrypting the Encryption Debate: A Framework for Decision-Makers*, National Academies Press, 2018.

Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR). « La relation entre le SCRS et la GRC vue sous l'angle d'une enquête en cours », examen de l'OSSNR nº 2019-04, 2019, https://nsira-ossnr.gc.ca/wp-content/uploads/CSIS-RCMP_RRCLOI_FR.pdf (consulté le 31 octobre 2023).

Newell, B. « Introduction: surveillance and the COVID-19 pandemic: views from around the world », *Surveillance & Society*, vol. 19, nº 1, 2021, p. 81-84.

Nissenbaum, H. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press, 2009.

Parsons, C. « Canada's New and Irresponsible Encryption Policy: How the Government of Canada's New Policy Threatens Charter Rights, Cybersecurity, Economic Growth, and Foreign Policy », Citizen Lab (Université de Toronto), 2019, https://citizenlab.ca/2019/08/ canadas-new-and-irresponsible-encryption-policy-how-the-government-of-canadas-new-policy-threatens-charter-rights-cybersecurity-economic-growth-and-foreign-policy/ (consulté le 11 septembre 2023).

Pavone, V., Degli-Esposti, S. et Santiago, E. *Key Factors Affecting Public Acceptance and Acceptability of SOSTs*, Institut Universitaire Européen, 2015.

Penney, S. et Gibbs, D. « Law Enforcement Access to Encrypted Data: Legislative Responses and the Charter », *Revue de droit de McGill Law*, vol. 63, nº 2, 2017, p. 201-45.

Regan, P.M. *Legislating Privacy: Technology, Social Values, and Public Policy*, University of North Carolina Press, 1995.

Gendarmerie royale du Canada. *Résultats des sondages d'opinion auprès des clients et des partenaires 2019-2020*, 2020, disponible à l'adresse https://www.rcmp-grc.gc.ca/fr/rapports-recherche-et-publications/resultats-des-sondages-dopinion-aupres-des-clients-et-des-partenaires (consulté le 11 septembre 2023).

—— *Résultats des sondages d'opinion auprès des clients et des partenaires 2020-2021*, 2021, disponible à l'adresse https://www.rcmp-grc.gc.ca/fr/rapports-recherche-et-publications/resultats-des-sondages-dopinion-aupres-des-clients-et-des-partenaires (consulté le 11 septembre 2023).

—— *Résultats des sondages d'opinion auprès des clients et des partenaires 2021-2022*, 2022, disponible à l'adresse https://www.rcmp-grc.gc.ca/fr/rapports-recherche-et-publications/resultats-des-sondages-dopinion-aupres-des-clients-et-des-partenaires (consulté le 11 septembre 2023).

—— « Réponse de la Gendarmerie royale du Canada au document parlementaire Q-566, 23 juin 2022 », 2022, https://www.priv.gc.ca/fr/protection-de-la-vie-privee-et-transparence-au-commissariat/divulgation-proactive/cpvp-parl-bp/ethi_20220808/grc_reponse/ (consulté le 22 juin 2023).

Rubenfeld, J. « The Right to Privacy », *Harvard Law Review*, vol. 102, 1989, p. 737-807.

Ruddell, R. « The Changing Context of Canadian Policing: An Examination of the Public's Perceptions after 2020 », *Journal of Community Safety and Well-Being*, vol. 7, nº 2, 2022, p. 47-52.

Seglins, D., Cribb, R. et Gomez, C. « Inside 10 Cases Where the RCMP Hit a Digital Wall », *CBC News*, 2016 (15 novembre 2016), https://www.cbc.ca/news/investigates/police-power-privacy-rcmp-cases-1.3850783 (consulté le 24 août 2023).

—— « RCMP Boss Bob Paulson Says Force Needs Warrantless Access to ISP User Data », *CBC News*, 2016 (15 novembre 2016), https://www.cbc.ca/news/investigates/police-power-privacy-paulson-1.3851955 (consulté le 24 août 2023).

—— « RCMP Want New Powers to Bypass Digital Roadblocks in Terrorism, Major Crime Cases », *CBC News*, 2016 (15 novembre 2016), https://www.cbc.ca/news/investigates/rcmp-digital-roadblocks-1.3850018 (consulté le 24 août 2023).

Solove, D.J. « Conceptualizing Privacy », *California Law Review*, vol. 90, nº 4, 2002, p. 1087-155.

Solove, D.J. *Understanding Privacy*, Harvard University Press, 2002.

Solove, D.J. *The Digital Person: Technology and Privacy in the Information Age*, New York University Press, 2004.

Swire, P. et Ahmad, K. « Going Dark' Versus a 'Golden Age for Surveillance' », Center for Democracy and Technology, 2011, https://cdt.org/insights/going-dark-versus-a-golden-age-for-surveillance/ (consulté le 24 août 2023).

Tunney, T. « RCMP's Ability to Police Digital Realm 'Rapidly Declining,' Commissioner Warned », *CBC News*, 2018 (5 octobre 2018), https://www.cbc.ca/news/politics/lucki-briefing-binde-cybercrime-1.4831340 (consulté le 13 août 2023).

Viola, L. A. « The Limits of Transparency as a Tool for Regulating Surveillance. A Comparative Study of the United States, United Kingdom, and Germany » dans L.A. Viola et P. Laidler (éd.), 2022. *Trust and Transparency in an Age of Surveillance*, Routledge, 2022.

Viola, L. A. et Laidler, P. (éd.). *Trust and Transparency in an Age of Surveillance*, Routledge, 2022.

West, L. et Forcese, C. « Twisted into Knots: Canada's Challenges in Lawful Access to Encrypted Communications », *Common Law World Review*, vol. 49, n^{os} 3 et 4, 2020, p. 182-98.