L'interception des communications et les perquisitions numériques à l'ère du chiffrement et des logiciels espions : Les lois canadiennes sont-elles adéquates?

Rapport destiné au Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR)

Vivek Krishnamurthy[1]
Version provisoire – 30 août 2023

INTRODUCTION

Le présent document évalue l'adéquation des lois canadiennes encadrant l'emploi d'outils d'enquête sur appareil (OEA – communément appelés « logiciels espions ») pour intercepter des communications chiffrées et extraire des données d'appareils chiffrés, cela à des fins de sécurité et de renseignement.

Les développements technologiques récents, notamment l'essor des communications chiffrées de bout en bout et du chiffrement « complet du disque » sur les ordinateurs et les portables, ont amené les organismes de sécurité et de renseignement et les organismes d'application de la loi à s'en remettre aux OEA pour remplir le rôle autrefois assuré par les écoutes téléphoniques et les perquisitions physiques. Le rôle joué par les OEA dans la collecte de renseignements et les enquêtes criminelles va sans doute s'intensifier

[1] Je tiens à remercier Daniella Febbraro, diplômée de la Section de common law à la Faculté de droit de l'Université d'Ottawa (2023), et Leonhard Knebel, étudiant en droit de la Ludwig-Maximillian University de Munich, en Allemagne, ayant passé le First State Examination in Law en Bavière, pour leur aide dans les recherches.

dans les années à venir, le chiffrement étant de plus en plus répandu et les technologies de communication quantique, de plus en plus utilisées.

Toutefois, les OEA présentent des dangers beaucoup plus graves pour les droits de la personne des Canadiens et des citoyens étrangers que les techniques qu'ils remplacent. Les lois du Canada qui régissent l'utilisation de ces outils par les organismes gouvernementaux ne suivent pas le rythme de ces développements technologiques.

Le présent document débute par un aperçu des tendances technologiques qui entraînent un accroissement de l'utilisation des OEA par les organismes gouvernementaux et se poursuit avec une évaluation du cadre juridique du Canada régissant l'autorisation d'utiliser ces outils redoutables. L'analyse juridique examinera les dispositions pertinentes du *Code criminel* du Canada, de la *Loi sur le Service canadien du renseignement de sécurité* (*Loi sur le SCRS*) et de la *Loi sur le Centre de la sécurité des télécommunications* (*Loi sur le CST*), en considérant le lien étroit qui existe entre les organismes d'application de la loi et les organismes de sécurité et de renseignement dans de nombreux contextes. Le document se termine par un examen des réformes juridiques récentes en Allemagne, lesquelles peuvent servir d'exemple au Canada pour sa mise à jour des lois ayant pour but de surmonter les défis posés par un environnement technologique changeant rapidement.

1. CONTEXTE TECHNOLOGIQUE ET HISTORIQUE

Un peu de contexte historique sur la capacité des organismes gouvernementaux à intercepter les communications nous sera utile pour évaluer si les lois du Canada régissant ces activités sont adaptées à la réalité technologique actuelle. Aujourd'hui, il est plus facile pour les organismes gouvernementaux d'intercepter les communications en temps réel et d'accéder aux données de communications stockées, plus facile qu'à tout autre moment du siècle dernier, ou presque. Toutefois, la généralisation du chiffrement fait qu'il est un peu plus difficile pour ces organismes de mener des enquêtes numériques qu'il y a dix ans.

L'une des principales raisons pour lesquelles le chiffrement est plus répandu aujourd'hui qu'il y a dix ans est la dénonciation par Edward Snowden des activités de surveillance de masse illégales par la National Security Agency des États-Unis, et la réaction qu'elle a entraînée[2]. Toutefois, il est exagéré de dire que les choses

[2] FINLEY, Klint, *« Encrypted Web Traffic More Than Doubles After NSA Revelations »*, Wired, consulté le 28 août 2023, https://www.wired.com/2014/05/sandvine-report/; CUTHBERSON, Anthony,

« vont en s'aggravant » pour les organismes gouvernementaux, en raison de l'essor du chiffrement[3]. Comme il est expliqué plus loin, ces organismes ont un plus grand accès aux métadonnées des communications qu'à tout autre moment du siècle dernier. De plus, la disponibilité répandue et alarmante de « logiciels espions » capables de supplanter la plupart des technologies de chiffrement fait que les organismes gouvernementaux sont toujours capables de pratiquer une surveillance numérique ciblée[4]. Nous sommes confrontés à un défi : celui de réglementer adéquatement l'utilisation de ces nouvelles technologies de surveillance terrifiantes, étant donné que celles-ci risquent de devenir de plus en plus importantes avec le temps avec l'essor attendu des technologies de communications quantiques.

1.1. « Bienvenue dans les années 80 »

Un moyen pour comprendre pourquoi les organismes gouvernementaux ont plus de facilité à intercepter et analyser les données des communications aujourd'hui qu'à tout autre moment depuis l'invention du télégraphe, ou presque, consiste à remonter aux années 80, où le téléphone était la technologie de communication en temps réel dominante.

Avec l'architecture du réseau téléphonique traditionnel, il était facile pour les organismes gouvernementaux d'intercepter les appels téléphoniques et de recueillir ce que nous appelons aujourd'hui des métadonnées de communications[5]. Le réseau

---

« Snowden 'Sped Up Encryption' by Seven Years », Newsweek, 26 avril 2016, https://www.newsweek.com/snowden-sped-encryption-seven-years-452688.

[3] ZITTRAIN, Jonathan *et al.*, *« Don't Panic: Making Progress on the Going Dark Debate* », Berkman Center, publication de recherche, 2016-1, 2016, https://dash.harvard.edu/handle/1/28552576.

[4] LUBIN, Asaf, *« Selling Surveillance »*, travail universitaire du SSRN (Rochester, NY, 2023), https://doi.org/10.2139/ssrn.4323985.

[5] La Electronic Frontier Foundation, une organisation importante défendant les droits numériques basée à San Francisco, décrit les métadonnées comme suit :

> Les métadonnées sont souvent décrites comme étant tout à l'exception du contenu de vos communications. On peut s'imaginer les métadonnées comme étant l'équivalent numérique d'une enveloppe. Une enveloppe referme des renseignements sur l'expéditeur, le destinataire et la destination d'un message. Il en va de même pour les métadonnées.
> Les métadonnées sont des renseignements sur les communications numériques transmises et reçues. Voici quelques exemples de métadonnées : – la ligne d'objet de vos courriels
> – la durée de vos conversations – la période au cours de laquelle une conversation a eu lieu – votre emplacement géographique quand vous communiquez (et avec qui)

Electronic Frontier Foundation, *« Voici pourquoi les métadonnées sont importantes »*, consulté le 30 août 2023, https://ssd.eff.org/fr/module/voici-pourquoi-

téléphonique traditionnel a une architecture centralisée où chaque ligne est connectée à un central téléphonique[6]. De l'équipement d'interception pouvait être installé facilement à ces centraux. Tous les grands fabricants d'équipement de commutation intégraient dans leurs produits des capacités d'« interception légale[7] ». Ils le faisaient pour aider leurs clients (les anciens monopoles téléphoniques détenus par l'État) à respecter la loi, qui les obligeait à avoir ces capacités[8,9]. De plus, le fait que les compagnies de téléphone facturaient le montant à leurs clients en fonction des numéros composés (appels locaux *vs* appels interurbains) et de la durée des conversations générait des registres, que les organismes gouvernementaux pouvaient obtenir auprès d'entités centralisées pour savoir qui appelait qui[8].

Toutefois, des contraintes logistiques importantes affectaient la capacité des organismes gouvernementaux à intercepter et analyser des communications téléphoniques en grande quantité. Les appels téléphoniques devaient être enregistrés sur ruban magnétique et des analystes humains devaient écouter les enregistrements pour déterminer leur contenu[10]. Tout au long des années 80, l'ancêtre du Service canadien du renseignement de sécurité (SCRS) a maintenu la pratique d'effacer les enregistrements de conversations téléphoniques sur ruban qu'il avait interceptées – probablement pour pouvoir réutiliser les rubans – et pour cette raison, il a détruit des enregistrements de conversations entre les conspirateurs de l'attentat Air India survenu en 1985[10].

Par contraste, le stockage numérique est si abordable aujourd'hui

---

les-m%C3%A9tadonn%C3%A9es-sont-importantes.

[6] PSTN Network Topology, dans Wikipedia, 19 avril 2023, https://en.wikipedia.org/w/index.php?title=PSTN_network_topology&oldid=1150624186, What Is PSTN and How It Works | Complete Guide [2022], Telnyx, consulté le 28 août 2023, https://telnyx.com/resources/what-is-pstn.

[7] *« Lawful Interception (LI) »*, ETSI, consulté le 28 août 2023, https://www.etsi.org/technologies/lawful-interception.

[8] Commissariat à la protection de la vie privée du Canada, « Réponse à la consultation du gouvernement sur l'accès légal (5 mai 2005) », 8 juillet 2005, https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/memoires-presentes-dans-le-cadre-de-consultations/sub_la_050505.

[9] Remarque : dans le contexte national de l'application de la loi, ces renseignements pourraient être recueillis par la police au moyen d'une ordonnance de communication, plutôt qu'avec un mandat. Voir Société *Télé-Mobile c. Ontario*, 2008 CSC 12.

[10] Le film allemand « La vie des autres » (« Das Leben der Anderen ») sorti en 2006 dépeint, entre autres, l'ampleur des ressources humaines et matérielles requises pour la Stasi, le tant méprisé service de renseignement de l'Allemagne de l'Est, pour soumettre ses citoyens à une surveillance téléphonique à grande échelle dans les années 80.

que n'importe quelle donnée recueillie pour une enquête peut être conservée indéfiniment[11].

De plus, les outils numériques tels que la reconnaissance vocale, la traduction automatique et les analyses alimentées par l'intelligence artificielle peuvent éplucher automatiquement pour les organismes gouvernementaux des tonnes de données numériques interceptées et relever les éléments qui vaudraient la peine d'être analysés par leur personnel[12].

En effet, du point de vue de la logistique et des coûts, un organisme gouvernemental peut aujourd'hui intercepter chaque communication numérique en provenance ou à destination d'un pays donné, et analyser ces communications au moyen d'outils automatisés à la recherche de tout élément présentant un intérêt pour les autorités d'enquête. Pour toutes ces raisons, notre époque est appelée « l'âge d'or de la surveillance » par le professeur Peter Swire du Georgia Institute of Technology, qui a été directeur du National Intelligence Review Group on Intelligence and Communications Technologies sous le gouvernement Obama[13], et par Bruce Schneier de la Harvard Kennedy School, qui est l'un des technologues en sécurité les plus réputés mondialement[14].

Cette évaluation est toujours valide malgré que la généralisation du chiffrement ait légèrement réduit la capacité des organismes gouvernementaux à intercepter et analyser les données numériques.

[10] *« Erasing Wiretap Evidence Was 'default' CSIS Policy, Air India Inquiry Told »*, CBC News, 19 septembre 2007, https://www.cbc.ca/news/canada/erasing- wiretap-evidence-was-default-csis-policy-air-india-inquiry-told-1.631443.

[11] Le coût d'une heure de stockage de la qualité audio d'un CD est passé de 20 150 $ en 1985 à seulement 0,91 ¢ aujourd'hui. Calculs de l'auteur basés sur l'article *« Historical Cost of Computer Memory and Storage »*, Our World in Data, consulté le 30 août 2023, https://ourworldindata.org/grapher/historical-cost-of-computer-memory-and- storage.

[12] KRISHNAMURTHY, Vivek, *« With Great (Computing) Power Comes Great (Human Rights) Responsibility: Cloud Computing and Human Rights »*, Business and Human Rights Journal 7, nº 2 (juin 2022) : 226 48, https://doi.org/10.1017/bhj.2022.8.

[13] SWIRE, Peter, *« The FBI Doesn't Need More Access: We're Already in the Golden Age of Surveillance »*, Just Security, 17 novembre 2014, https://www.justsecurity.org/17496/fbi-access-golden-age-surveillance/.

[14] SCHNEIER, Bruce, *« Internet Has Delivered a 'Golden Age of Surveillance' »*,

Schneier on Security (blogue), 11 avril 2014, https://www.schneier.com/news/archives/2014/04/schneier_internet_ha.html.

1.2. L'essor du chiffrement

Dans certains milieux, on craint de plus en plus que la généralisation du chiffrement affaiblisse la capacité des organismes gouvernementaux en application de la loi et en renseignement et sécurité à mener à bien leurs missions[15].

Pour savoir si ces craintes sont fondées, il faut comprendre comment le chiffrement fonctionne. Il faut aussi examiner dans quelle mesure le chiffrement fait obstacle à la capacité des organismes gouvernementaux à accomplir leurs missions, compte tenu de la disponibilité de nouvelles technologies puissantes qui peuvent saper le chiffrement.

Les technologies de chiffrement actuelles se divisent en deux grandes catégories. Les technologies de la première catégorie chiffrent les données « au repos », c.-à-d. lorsqu'elles sont stockées sur un support numérique[16].

Par exemple, les technologies FileVault et Data Protection d'Apple chiffrent les données stockées sur les ordinateurs Macintosh et les appareils iOS par défaut[17]. De ce fait, lorsque les organismes gouvernementaux saisissent de tels appareils, ils sont incapables d'accéder aux données qui y sont stockées, sauf s'ils peuvent obtenir le mot de passe de chiffrement ou utiliser des OEA pour contourner les protections par chiffrement[18].

Les technologies de la deuxième catégorie chiffrent les « en mouvement », c.-à-d. pendant que celles-ci sont transférées d'un expéditeur à un destinataire[19].

La forme de chiffrement de « données en mouvement » la plus courante est connue sous le nom de « sécurité au niveau du transport » (SNT). C'est ce type de chiffrement qui est utilisé pour protéger la sécurité des banques en ligne ou des services fondés sur l'infonuagique tels que Gmail ou Microsoft Office 365. Avec la SNT, la mise sur écoute d'une connexion Internet (qu'elle soit par câble, par fibre optique ou cellulaire) ne permet d'intercepter aucunes données intelligibles : seulement des données brouillées.

[15] BAKER, Stewart, *« How Long Will Unbreakable Commercial Encryption Last? »*, Lawfare, 20 septembre 2019, https://www.lawfaremedia.org/article/how-long- will-unbreakable-commercial-encryption-last.

[16] Cette courte description du fonctionnement du chiffrement est basée sur l'excellent guide d'introduction de la Electronic Frontier Foundation. Voir l'article *« What*

Should I Know About Encryption? » de la Electronic Frontier Foundation, consulté le 30 août 2023, https://ssd.eff.org/module/what-should-i-know-about-encryption.

[17] *« Encryption and Data Protection Overview »*, Apple Support, consulté le 30 août 2023, https://support.apple.com/guide/security/encryption-and-data- protection-overview-sece3bee0835/web.

[18] NAKASHIMA, Ellen, et Reed Albergotti, *« The FBI Wanted to Unlock the San Bernardino Shooter's iPhone. It Turned to a Little-Known Australian Firm »*, Washington Post, 14 avril 2021, https://www.washingtonpost.com/technology/2021/04/14/azimuth-san- bernardino-apple-iphone-fbi/.

[19] Electronic Frontier Foundation, *« What Should I Know About Encryption? »*

données qu'il est pratiquement impossible de déchiffrer, même avec les superordinateurs les plus puissants[20].

La SNT est importante pour protéger la sécurité et la vie privée des utilisateurs d'Internet contre l'écoute électronique. Toutefois, les organismes gouvernementaux peuvent obtenir les données transmises par SNT autrement. Par exemple, la police peut obtenir un mandat de perquisition visant Google pour exiger de celui-ci qu'il remette le contenu de mon compte de courriel si je suis soupçonné d'un crime[21].

De la même manière, la police peut se rendre à ma banque pour obtenir mes documents financiers même si ma session de services bancaires en ligne est protégée par SNT.

L'autre forme courante de chiffrement des « données en mouvement » est connue sous le nom de « chiffrement de bout en bout ». Avec cette forme de chiffrement, les intermédiaires entre les deux parties ne peuvent accéder au contenu des communications de celles-ci[22].

Par exemple, un message échangé entre deux personnes au moyen de Signal, une plateforme de messagerie de bout en bout populaire, est rendu inintelligible et pour les exploitants du réseau de Signal et pour les nombreuses entreprises de télécommunications interviennent dans le transfert des messages électroniques entre deux parties[23].

Le chiffrement de bout en bout pose une difficulté beaucoup plus importante que la SNT pour les organismes gouvernementaux : ceux-ci ne sont pas en mesure d'obtenir une copie de ces messages auprès d'un fournisseur de services comme dans le cas d'un service infonuagique tel Gmail ou Dropbox.
En fonction de l'architecture, les organismes gouvernementaux peuvent être en mesure d'obtenir les métadonnées sur les utilisateurs auprès de l'exploitant ou d'un fournisseur de services Internet. Toutefois, comme nous le verrons plus loin, les messages

eux-mêmes ne peuvent être obtenus qu'au moyen d'un « logiciel espion ».

[20] Selon une estimation, il faudrait un milliard d'un milliard d'années à un superordinateur pour décoder l'algorithme de chiffrement AES-128, algorithme largement utilisé, au moyen de techniques de « force brute ». ARORA, Mohit, *« How Secure Is AES Against Brute Force Attacks? »*, EE Times, consulté le 30 août 2023, https://www.eetimes.com/how- secure-is-aes-against-brute-force-attacks/.

[21] Google, *« Requests for User Information FAQs – Transparency Report Help Center »*, consulté le 30 août 2023, https://support.google.com/transparencyreport/answer/9713961.

[22] Electronic Frontier Foundation, *« What Should I Know About Encryption? »*

[23] SNOW, John, *« Signal Is Secure, as Proven by Hackers »*, Kaspersky Daily, 24 août 2022, https://usa.kaspersky.com/blog/signal-hacked-but-still-secure/26949/.

Les métadonnées sont des « données sur des données ». Elles sont extrêmement utiles pour n'importe quelle enquête. À la différence du contenu d'une communication, qui consiste en ce qui est dit (avec la voix ou par texte), les métadonnées comprennent des renseignements tels que l'identité des interlocuteurs, leur numéro de téléphone ou adresse IP, la durée de la communication et d'autres renseignements tels que la ligne d'objet d'un courriel ou le nombre de messages texte échangés entre les deux parties[24].

Les métadonnées peuvent révéler ce qu'il y a de plus confidentiel à votre sujet. Par exemple, une liste des adresses courriel des personnes avec qui vous avez échangé révèle l'identité des personnes que vous fréquentez. Dans la mesure où ces personnes ont certaines caractéristiques communes (p. ex. même nationalité ou même identité sexuelle), beaucoup de choses peuvent être déduites sur votre identité.

Il arrive que des enquêteurs doivent accéder aux données stockées sur un appareil ou au contenu d'une communication chiffrée à des fins d'enquête légitimes. À titre d'exemple, une enquête criminelle portant sur du matériel d'exploitation sexuelle d'enfants (MESE) peut nécessiter l'accès au matériel sous-jacent dans un format non chiffré, pour déposer des accusations criminelles et s'en servir comme éléments de preuve dans un procès. Non seulement ces enquêteurs doivent avoir accès aux métadonnées qui démontrent qu'un suspect échange des fichiers avec d'autres trafiquants de MESE connus, mais ils ont parfois besoin d'accéder aux données sous-jacentes. Cela nous amène à examiner les options stratégiques dont le législateur dispose pour faire face aux défis posés par l'essor

du chiffrement.

2. PRISE EN CHARGE DU CHIFFREMENT : LE MENU DES OPTIONS STRATÉGIQUES

Les gouvernements disposent de trois options stratégiques pour faire face aux défis que présente le chiffrement des « données au repos » et des « données en mouvement » pour les opérations de sécurité et de renseignement et les opérations d'application de la loi.

2.1. Interdire le chiffrement

La première option consiste à restreindre de manière importante l'utilisation des technologies de chiffrement avancées. Quelqu'un pourrait imposer un retour au statu quo d'avant les révélations d'Edward Snowden, où le chiffrement des données au repos et en mouvement était l'exception plus que la règle. Par exemple, le gouvernement indien a récemment interdit 14 applications de messagerie chiffrée, sous prétexte que celles-ci étaient utilisées par des « terroristes » dans le territoire disputé de Jammu-et-Cachemire.

[24] Electronic Frontier Foundation, *« Why Metadata Matters »* [25]

Malgré les problèmes constitutionnels majeurs réels associés à l'interdiction de cette catégorie de technologies, même en restreignant de façon importante leur utilisation[26], il est peu probable que des restrictions légales sur le chiffrement serviraient le travail de renseignement, de sécurité et d'application de la loi. La technologie du chiffrement est maintenant répandue, et il est impossible de revenir en arrière. Quiconque souhaite protéger la sécurité et le caractère privé de ses données et de ses communications fera fi des restrictions sur le chiffrement pour atteindre ses objectifs.

De plus, les gains pour les organismes d'enquête gouvernementaux qui mènent des enquêtes sont largement annulés par les risques liés à la cybersécurité que pose la restriction du chiffrement pour la société canadienne[27].

Les technologies de chiffrement avancées sont essentielles pour protéger le caractère privé et la sécurité des communications cruciales et l'intégrité des données d'établissements importants tels que les banques, les hôpitaux et les établissements d'enseignement. De ce fait, la notion d'interdiction du chiffrement visant à améliorer la sécurité du public est, à juste titre, qualifiée de remède pire que le mal.

2.2. Rendre obligatoire l'accès exceptionnel

Une deuxième option, moins extrême, consiste à obliger certaines entreprises de technologie à créer des « points d'accès exceptionnel » et à intégrer ceux-ci dans leurs communications chiffrées et leurs systèmes de stockage de données de manière à faciliter le travail des organismes gouvernementaux[28].

Leurs partisans présentent ces mesures comme un « passe-partout » qui puisse ouvrir les verrous numériques pour les organismes gouvernementaux qui en ont le mandat légal[29],

[25] *« Govt Bans 14 Messaging, Calling Apps »*, Hindustan Times, 1er mai 2023, https://www.hindustantimes.com/india-news/indian-government-bans-14- mobile-messaging-and-calling-apps-over-terrorist-communication-concerns-101682964848626.html.

[26] PENNEY, Steven, et Dylan Gibbs, *« Law Enforcement Access to Encrypted Data: Legislative Responses and the Charter »*, McGill Law Journal 63, nº 2 (n.d.) : 201 45). [27] EOYANG, Mieke, et Michael Garcia, *« Weakened Encryption: The Threat to America's National Security »*, Third Way, consulté le 30 août 2023, https://www.thirdway.org/report/weakened-encryption-the-threat-to-americas- national-security. KRISHNAMURTHY, Vivek, Devony Schmidt et Amy Lehr, *« Cybersecurity and Human Rights: Understanding the Connection* , dans *« Human Rights Responsibilities in the Digital Age: States, Companies, and Individuals »*, éd. Jonathan Andrew et Frédéric Bernard (Gordonsville : Hart Publishing, impression de Bloomsbury Publishing, 2021). 28 ABELSON, Harold *et al.*, *« Keys under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications »*, *Journal of* 29

tandis que leurs détracteurs les qualifient de « trappes » susceptibles d'engendrer des vulnérabilités qui compromettent la vie privée et la cybersécurité de tous les utilisateurs de ces services[30].

Bien qu'il semble raisonnable à première vue de fournir aux organismes gouvernementaux les moyens techniques nécessaires pour déjouer le chiffrement lorsque cela est dûment autorisé par la loi, rendre obligatoire les « points d'accès exceptionnel » dans les systèmes chiffrés risque fortement d'ébranler notre sécurité nationale et de nuire à la vie privée et à la cybersécurité de tous les Canadiens[31].

Chaque fois qu'un point faible est créé dans un système électronique dans le but de fournir un accès aux organismes de sécurité et de renseignement et aux organismes d'application de la loi qui mènent leurs activités avec des autorisations légales appropriées, ce point peut être exploité par des adversaires, qui vont d'États étrangers à des cybercriminels, pour des activités qui iraient de l'espionnage à la guerre électronique. Comme l'a dit Jack Goldsmith, professeur à la Harvard Law School, « toute cyberarme offensive constitue une faille potentielle dans notre cyberdéfense[32] ».

Cybersecurity, 17 novembre 2015, tyv009, https://doi.org/10.1093/cybsec/tyv009.
KOUVAKAS, Ioannis, *« Changes to UK Surveillance Regime May Violate International Law »*, Just Security, 22 août 2023, https://www.justsecurity.org/87615/changes-to-uk-surveillance-regime-may- violate-international-law/.

[29] Comité éditorial *« Opinion | Compromise Needed on Smartphone Encryption »*, Washington Post, 3 octobre 2014, https://www.washingtonpost.com/opinions/compromise-needed-on- smartphone-encryption/2014/10/03/96680bf8-4a77-11e4-891d- 713f052086a0_story.html.

[30] *« Issue Brief: A 'Backdoor' to Encryption for Government Surveillance »*, Center for Democracy and Technology (blogue), 3 mars 2016, https://cdt.org/insights/issue-brief-a-backdoor-to-encryption-for-government- surveillance/.

[31] Abelson *et al.*, *« Keys under Doormats ».* Eoyang et Garcia, *« Weakened Encryption »*. GILL, Lex, Tamir Israel et Christopher Parsons, *« Shining a Light on the Encryption Debate: A Canadian Field Guide »*, mai 2018, https://tspace.library.utoronto.ca/handle/1807/94803. 32

GOLDSMITH, Jack, *« Cyber Paradox: Every Offensive Weapon Is a (Potential) Chink in Our Defense -- and Vice Versa »*, Lawfare, 12 avril 2014, https://www.lawfaremedia.org/article/cyber-paradox-every-offensive-weapon- potential-chink-our-defense-and-vice-versa.

Le paradoxe de Goldsmith est d'autant plus vrai que la diversité fait défaut dans les écosystèmes matériels et logiciels actuels. Tout comme nos adversaires de l'étranger et les organisations criminelles et terroristes que nous souhaitons ébranler, nous utilisons tous le même matériel informatique et les mêmes logiciels pour atteindre nos objectifs. Les chefs d'État et les dirigeants des organisations terroristes communiquent tous sur la plateforme WhatsApp de Meta, et les ordinateurs du gouvernement canadien utilisent Microsoft Windows, tout comme ceux des groupes cybercriminels organisés. De ce fait, les risques pour la sécurité que comporte l'introduction de « points d'accès exceptionnel » dans ces systèmes dépassent de loin les bénéfices qui accompagnent cette action.

2.3. Les OEA : un moindre mal?

Cela nous amène à la troisième option stratégique, qui consiste à élaborer un cadre juridique approprié pour gérer l'utilisation, par les organismes de sécurité, de renseignement et d'application de la loi, des outils numériques couramment appelés « logiciels espions » afin de contourner le chiffrement et d'obtenir les données directement à partir des appareils numériques où elles sont stockées.

Les OEA utilisent une gamme de moyens, qui vont des « enregistreurs de frappe » qui suivent chaque frappe entrée par un utilisateur dans un ordinateur[33] aux outils terrifiants et controversés comme la tristement célèbre suite logicielle Pegasus du NSO Group, qui permet à ses utilisateurs d'extraire chaque bit de données d'un téléphone intelligent infecté et de transformer le

microphone, la caméra ou le système GPS du téléphone en appareil de surveillance en temps réel redoutable[34].

Les OEA ont tous un point en commun : ils exploitent les erreurs et les faiblesses présentes dans la programmation et la conception du matériel informatique et des logiciels modernes pour permettre à leurs utilisateurs de saper une multitude de précautions de sécurité, notamment le chiffrement[35]. Il est pratiquement impossible d'utiliser des techniques « de force brute » pour déchiffrer un message ayant été sécurisé au moyen de techniques de chiffrement modernes. L'erreur est humaine, et chaque appareil informatique vendu sur le marché comporte des vulnérabilités qui permettent à des auteurs de menace disposant de moyens sophistiqués de contourner les mesures de protection de la cybersécurité les plus poussées.

[33] *« Keyloggers: How They Work & How to Detect Them – CrowdStrike »*, crowdstrike.com, consulté le 30 août 2023, https://www.crowdstrike.com/cybersecurity-101/attack-types/keylogger/.

[34] SHANKLAND, Stephen, *« Pegasus Spyware and Citizen Surveillance: Here's What You Should Know »*, CNET, consulté le 30 août 2023, https://www.cnet.com/tech/mobile/pegasus-spyware-and-citizen-surveillance- what-you-need-to-know/.

[35] Dans le jargon de la cybersécurité, ces faiblesses sont appelées « vulnérabilités de jour zéro ». *« What Is a Zero-Day Attack? –* Definition and *Explanation »*, usa.kaspersky.com, 30 juin 2023, https://usa.kaspersky.com/resource- center/definitions/zero-day-exploit; LAKSHMAMAN, Ravie, *« NSO Group Used 3 Zero-Click iPhone Exploits Against Human Rights Defenders »*, The Hacker News, 20 avril 2023, https://thehackernews.com/2023/04/nso-group-used-3-zero-click-iphone.html.

De la même manière, les copies de messages ayant été envoyées avec un chiffrement de bout en bout et qui sont stockées dans un appareil chiffré peuvent être extraites directement à partir d'un appareil au moyen de ces OEA sophistiqués[36].

Certains de ces outils nécessitent que les enquêteurs aient physiquement avec eux un appareil chiffré. C'est le cas par exemple du logiciel obtenu par le FBI auprès d'une entreprise australienne du nom d'Azimuth pour contourner le chiffrement d'un iPhone ayant été utilisé par le suspect (décédé) à l'origine d'une attaque terroriste à San Bernardino en Californie (2015[37]).

Par contraste, des outils tels que Pegasus de NSO Group et la suite Galileo de Hacking Team (qui n'existe plus) permettent à leurs utilisateurs d'accéder à distance au contenu d'un appareil numérique[38].

De plus, il est prouvé que Pegasus permet d'actionner à distance le microphone et la caméra d'un appareil, et

d’en surveiller les communications en temps réel[39].

Les capacités des outils tels que Pegasus sont beaucoup plus invasives que celles des outils d’écoute traditionnels. Pour revenir à notre exemple tiré des années 80, un dispositif d’écoute de la Gendarmerie royale du Canada (GRC) pouvait surveiller les conversations téléphoniques d’une personne, mais non pas ses conversations à la maison ou dans un parc public par exemple. De la même manière, l’écoute électronique ne pouvait pas être utilisée pour fouiller chaque document présent chez un suspect, pour lire son courrier ni pour prendre des photos ou tourner des vidéos de lui à son insu jour et nuit. Mais les OEA les plus puissants regroupent toutes ces techniques d’enquête en un seul outil.

36 MANANCOURT, Vincent, et Mark Scott, *« Spyware Scandal Revives Push against Government Access to Encrypted Messages »*, POLITICO (blogue), 19 juillet 2021, https://www.politico.eu/article/spyware-scandal-revives-push-against- government-access-to-encrypted-messages/.

37 Nakashima et Albergotti, *« The FBI Wanted to Unlock the San Bernardino Shooter’s iPhone. It Turned to a Little-Known Australian Firm. »* 38 COX, Joseph, *« The FBI Spent $775K on Hacking Team’s Spy Tools Since 2011 »*, Wired, consulté le 30 août 2023, https://www.wired.com/2015/07/fbi-spent-775k- hacking-teams-spy-tools-since-2011/.

39 LOVEJOY, Ben, *« Pegasus Screenshots Show It Secretly Activating Mic and Camera »*, 9to5Mac, 5 août 2022, https://9to5mac.com/2022/08/05/pegasus- screenshots/.

Les OEA comme Pegasus ont été impliqués dans de graves abus commis par des gouvernements nationaux aux antécédents aussi variés, pour le respect des droits de la personne, que l’Espagne et l’Arabie saoudite. En Espagne, les services de renseignement ont utilisé Pegasus sans autorisation légale pour surveiller les communications de représentants élus de la Catalogne qui militent pour l’indépendance de cette région[40]. Pendant ce temps, les autorités saoudiennes utilisaient Pegasus pour espionner le journaliste dissident Jamal Khasoggi. Ce dernier a été brutalement assassiné puis démembré par une équipe d’agents du renseignement saoudiens dans le consulat du royaume à Istanbul[41].

De nombreux autres abus de ces outils ont été mis au jour, notamment leur utilisation par des gouvernements autoritaires pour espionner des journalistes, des dissidents, et même des chefs d’État de pays détenant l’arme nucléaire[42].

Les OEA possèdent des capacités redoutables. Il est urgent de réglementer le commerce international pour une vaste variété d'OEA vendus par des entités privées[43].

Néanmoins, à l'heure actuelle, les OEA représentent la moins mauvaise des trois options disponibles face aux défis que pose le chiffrement systématique pour les capacités d'enquête des organismes gouvernementaux.

Comparativement à une restriction des capacités de chiffrement ou à une obligation d'inclure des points d'accès exceptionnel dans les systèmes chiffrés, l'utilisation des OEA engendre moins de risques systémiques pour la cybersécurité – du moins dans le contexte technologique actuel. Les OEA sont dangereusement omniprésents et peuvent être mal utilisés. Cela va de soi. Toutefois, leur nature oblige que leur activité soit ciblée. En effet, l'utilisateur d'un OEA doit choisir la personne ciblée avec la technologie, tandis que les deux premières options engendrent des vulnérabilités dans les systèmes utilisés par tous les utilisateurs pour permettre aux organismes de sécurité, de renseignement et d'application de la loi d'atteindre leurs objectifs d'enquête.

Également, on peut parler d'une course aux armements puisque des entreprises telles que Apple, Meta et Microsoft – conceptrices du matériel et des logiciels informatiques les plus utilisés sur la planète – s'efforcent de corriger les vulnérabilités exploitables plus vite que les développeurs d'OEA n'arrivent à les trouver[44].

Cette « course aux armements » limite quelque peu la prévalence des OEA et de l'ampleur de leur déploiement, comparativement aux cyberrisques à grande échelle qu'impliquerait l'affaiblissent du chiffrement.

[40] AARUP, Sarah Anne, *« Pegasus Spyware Targets Top Catalan Politicians and Activists »*, POLITICO (blogue), 18 avril 2022, https://www.politico.eu/article/pegasus-spyware-targets-top-catalan-politicians- and-activists/.

[41] BERGMAN, Ronen, et Mark Mazzetti, *« Israeli Companies Aided Saudi Spying Despite Khashoggi Killing »*, The New York Times, 17 juillet 2021, sec. World, https://www.nytimes.com/2021/07/17/world/middleeast/israel-saudi-khashoggi- hacking-nso.html.

[42] *« Pegasus: French President Macron Identified as Spyware Target – BBC News »*, consulté le 30 août 2023, https://www.bbc.com/news/world-europe-57907258.

[43] Lubin, *« Selling Surveillance »*

[44] ARMERDING, Taylor, *« Apple's $1 Million Bug Bounty Could Launch Arms Race For Zero Days »*, Forbes, consulté le 30 août 2023, https://www.forbes.com/sites/taylorarmerding/2019/08/15/bug-bounties-go-big/.

L'utilisation des OEA par les organismes gouvernementaux va sans doute s'intensifier si l'utilisation des technologies de communication quantiques connaît une expansion. Les systèmes de communication quantique utilisent un principe de physique des particules appelé « intrication », qui rend impossible pour quiconque l'interception en cachette des communications acheminées d'un expéditeur à un destinataire[45].

En termes simples, en tentant d'intercepter une communication quantique pendant la transmission de celle-ci, l'expéditeur et le destinataire sont tous deux alertés qu'une personne tente d'écouter cette communication, et la transmission ne peut pas se faire. De ce fait, le seul moyen possible pour intercepter des communications quantiques consiste à installer des OEA sur les appareils qui seront utilisés par les utilisateurs pour envoyer et recevoir ces communications – comme les claviers avec lesquels les messages sont tapés ou les écrans sur lesquels le contenu de ces messages est affiché[46].

Dans un avenir proche, il est probable que les organismes de sécurité et de renseignement et les organismes d'application de la loi aient besoin de s'en remettre aux OEA pour obtenir l'accès à des communications numériques chiffrées.
Ainsi, les décideurs sont confrontés à la question de comment réglementer ces technologies avec tout leur potentiel d'abus. Examiner comment la fabrication et la vente de ces technologies devraient être réglementées dépasserait la portée du présent document. Toutefois, la dernière section propose quelques avenues pour réformer les lois canadiennes pertinentes.
La prochaine section décrit de façon sommaire l'état actuel de nos lois qui régissent l'utilisation de ces technologies par les organismes gouvernementaux.

3. LES LOIS INADÉQUATES DU CANADA

Cette section traite du cadre législatif qui régit actuellement au Canada l'autorisation d'utiliser des OEA. Elle est entièrement basée sur des documents de source publique, dont un examen des lois pertinentes et des décisions judiciaires qui interprètent ces lois.

[45] Elizabeth Fernandez, *« Practical Physics: How Quantum Uncertainty Will Make Our Communications Secure »*, Big Think (blogue), 18 octobre 2022, https://bigthink.com/the-future/quantum-communications-secure/.

[46] Communication personnelle avec Anne Broadbent, titulaire de la chaire d'excellence en recherche du Canada sur le traitement de l'information quantique, Université d'Ottawa, 14 novembre 2022.

Contrairement aux autres grandes démocraties, le Canada n'a pas réformé ses lois qui régissent l'interception des communications et les autres formes de perquisition numérique en réponse aux défis importants que présente l'utilisation des OEA par les organismes d'application de la loi, de sécurité et de renseignement. Le cadre actuel qui régit ces outils extrêmement puissants est fragmenté et n'a pas de mécanismes de contrôle, de transparence ni de responsabilisation appropriés.

La section débute par un aperçu des dispositions du *Code criminel* qui autorisent les organismes d'application de la loi nationaux à utiliser les OEA pour leurs enquêtes criminelles. Le rôle du CPSNR consiste à assurer la surveillance des organismes de sécurité et de renseignement du pays. Néanmoins, il est important d'examiner les autorisations législatives qui permettent aux organismes d'application de la loi nationaux d'utiliser des OEA dans leurs enquêtes, compte tenu de leur collaboration étroite avec les organismes de sécurité et de renseignement. La section traite ensuite des dispositions de la *Loi sur le SCRS* et de la *Loi sur le CST,* qui autorisent les organismes de renseignement du Canada à utiliser ces outils.

3.1. *Code criminel*

La partie VI du *Code criminel* décrit la procédure devant être suivie par les organismes d'application de la loi lorsqu'ils interceptent des communications. Également, elle définit une série d'infractions qui interdisent l'interception de communications par quiconque (peu importe qu'il s'agisse d'un agent d'application de la loi ou non) lorsque les procédures établies ne sont pas suivies[47]. Ces dispositions s'appliquent aux interceptions de communications prospectives (p. ex. écoute électronique) et non aux interceptions rétrospectives (p. ex. mandat visant l'obtention de courriels archivés par Google[48]).

En résumé, le *Code criminel* interdit l'interception de communications sans mandat, sauf dans certains cas exceptionnels. Ces exigences cadrent avec la garantie prévue à l'article 8 de la *Charte canadienne des droits et libertés* contre les fouilles, les perquisitions et les saisies abusives.

---

[47] Voir le *Code criminel*, art. 183.
[48] *R. c. Jones*, 2017, CSC 60, par. 69.

La procédure générale pour obtenir l'autorisation judiciaire d'intercepter des communications électroniques est présentée aux articles 185 et 186. Une demande doit être faite à un juge de la cour supérieure par les procureurs généraux provinciaux ou fédéraux (ou leurs délégués ou autres représentants désignés). Pour faire droit à

une telle demande, le juge de la cour supérieure doit être convaincu de ce qui suit :

1. il existe un motif raisonnable de croire que l'interception pourrait faciliter l'enquête sur une infraction;
2. l'octroi de cette autorisation servirait au mieux l'administration de la justice;
3. d'autres méthodes d'enquête ont été essayées et ont échoué, ou ont peu de chance de succès, ou l'urgence de l'affaire est telle qu'il ne serait pas pratique de mener l'enquête relative à l'infraction en n'utilisant que les autres méthodes d'enquête.

Le dernier critère, familièrement appelé *exhaustion requirement* en anglais, est levé pour certaines infractions, comme celles liées au terrorisme et au crime organisé[49].

---

[49] *Code criminel*, par. 185 (1.1)

Si le juge est convaincu que les agents de l'État se sont acquittés du fardeau de la preuve, il peut autoriser l'interception de communications pour une période de 60 jours. Cette autorisation peut être renouvelée ou prolongée pour une période totalisant jusqu'à trois (3) ans [voir les paragraphes 185(2), 185(3), 186(6) et 186(7)]. De plus, ces dispositions générales permettent à un juge de donner des mandats ou des ordonnances connexes en même temps, s'il est convaincu que ces mandats ou ordonnances sont liés à l'exécution de l'autorisation. Par exemple, un juge pourrait délivrer un mandat de perquisition en vertu de l'article 487 ou un mandat pour un dispositif de localisation en vertu de l'article 492.1 au moment où il accorde l'autorisation d'intercepter des communications en vertu de cette disposition.

En plus de ces procédures générales, le *Code criminel* présente plusieurs procédures spéciales et exceptionnelles portant sur l'interception de communications. Trois d'entre elles méritent d'être abordées ici.

Premièrement, l'article 184.2 permet l'interception de communications avec le consentement de l'une des parties. Cette disposition exige qu'un agent de l'État demande une autorisation à un juge et fournisse des motifs raisonnables de croire (1) qu'une infraction a été ou sera commise et (2) que des renseignements relatifs à l'infraction seront obtenus avec l'interception demandée.

Deuxièmement, dans le même ordre d'idées, l'article 184.1 permet aux agents de l'État d'intercepter des communications privées sans mandat afin de prévenir des lésions corporelles aussi longtemps que l'une des parties prenant part à la communication consent à l'interception et pourvu qu'il y ait des motifs raisonnables de croire que cette partie pourrait subir des lésions corporelles.

Troisièmement, le plus important, les articles 184.4, 188 et 196 présentent des dispositions qui permettent à la police d'intercepter des communications sans mandat dans certaines situations d'urgence. L'article 184.4 permet de telles interceptions s'il y a des motifs raisonnables de croire que :

1. l'urgence de la situation est telle qu'une autorisation ne pourrait pas être obtenue avec une diligence raisonnable;
2. une interception immédiate est nécessaire pour empêcher une infraction qui causerait des dommages sérieux;
3. l'une des parties prenant part à la communication est la personne susceptible de commettre l'infraction.

L'article 196.1 exige que les autorités remettent un avis à toute personne ayant fait l'« objet » d'une interception en vertu de l'article 184.4 dans un délai de 90 jours, sous réserve d'une procédure par laquelle la Couronne peut demander à un juge de reporter la remise de cet avis pour une période maximale de trois ans afin de protéger l'enquête criminelle en cours.
L'article 188, pour sa part, permet à un juge à qui l'on a fait une demande en vertu des articles 185 et 186 (dispositions générales relatives à l'interception de communications) d'autoriser par écrit de telles interceptions pour une période maximale de 36 heures, lors d'une situation d'urgence qui empêche d'obtenir une autorisation avec diligence raisonnable.

3.1.1. Analyse

Que devons-nous comprendre de ces dispositions? Comment savoir si elles sont adéquates face au pari difficile de réglementer les OEA aux capacités redoutables entre les mains des organismes d'application de la loi canadiens?

Comme il a été mentionné précédemment, la partie VI du *Code criminel* s'applique aux interceptions de communications prospectives plutôt qu'aux recherches rétrospectives de communications stockées. Elle est révélatrice de l'ancienne réalité technologique, où les méthodes étaient très différentes selon que l'on cherchât à intercepter des communications en temps réel (p. ex. écoute électronique) ou bien des communications passées (p. ex.

perquisition chez un suspect pour y trouver des lettres incriminantes). La partie VI soumet l'interception de communications en temps réel à des mesures de protection rigoureuses, comme si c'était la pire invasion de la vie privée imaginable de la part d'un État exerçant son pouvoir de faire respecter le droit criminel.

Les technologies modernes telles que les OEA viennent brouiller les hypothèses de ce genre. Tout d'abord, les OEA rendent floue la distinction entre l'interception prospective des communications et leur récupération rétrospective, car les outils utilisés pour l'une et l'autre sont les mêmes. De plus, certaines des suites logicielles d'OEA les plus couramment utilisées, comme le logiciel Pegasus de NSO, intègrent de nombreuses capacités dans un seul progiciel – capacités qui vont de l'interception de communications en temps réel à la conversion de l'appareil numérique d'un utilisateur en machine de surveillance en temps réel[50].

Également, les OEA permettent à leurs utilisateurs d'accéder à toutes les données stockées d'une personne, peu importe qu'il s'agisse de données stockées sur l'appareil lui-même ou de données accessibles par l'entremise d'un service infonuagique auquel l'appareil est connecté. En des termes simples, si un OEA comme Pegasus est installé sur mon téléphone, non seulement vous pouvez chercher du contenu dans mon téléphone, mais vous pouvez aussi faire des recherches dans mes comptes Gmail et Dropbox, car ceux-ci sont tous connectés à mon téléphone.

Aucune de ces réalités technologiques n'est prise en compte dans le *Code criminel* actuel. Nous savons maintenant, d'après les résultats du rapport du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (Comité ETHI) sur l'utilisation des OEA par la GRC, que ces outils ont été utilisés pour 32 enquêtes visant 49 appareils entre 2017 et 2022[51].

Nous savons également que le processus pour obtenir l'autorisation d'utiliser ces capacités est extrêmement complexe. Avec la structure actuelle du *Code criminel*, les organismes d'application de la loi doivent obtenir plusieurs autorisations qui invoquent diverses dispositions du Code.

On peut avancer que cette complexité joue un rôle de protection, en ce sens qu'il pourra être difficile pour les organismes d'application de la loi de monter une demande qui remplisse les critères. En même temps, le fait que l'on doit utiliser autant de dispositions éparpillées du *Code criminel* nuit à la transparence et à la responsabilisation. Les rapports sur l'utilisation de la partie VI du *Code criminel* destinés au public sont basés sur les dispositions du Code invoquées[52].

[50] Shankland, *« Pegasus Spyware and Citizen Surveillance »*.

[51] Chambre des communes, Outils d'enquête sur appareil utilisés par la Gendarmerie royale du Canada et enjeux liés : Rapport du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (novembre 2022) (Président : John Brassard), page 22 (rapport du Comité ETHI).

[52] Sécurité publique Canada, « Rapport annuel sur la surveillance électronique 2020 », 23 février 2022.

Ainsi, l'absence de dispositions pensées en fonction de ces outils hautement invasifs fait en sorte qu'il est difficile pour le législateur et pour le public de savoir comment et quand ces outils sont utilisés dans un contexte pénal.

De plus, les dispositions du *Code criminel* actuel ne sont pas adaptées au degré d'invasion de la vie privée que certaines capacités des OEA impliquent. Prenons l'exemple de la surveillance vidéo, qui est régie par l'article 487.01 du *Code criminel*. L'installation, par les autorités, d'une caméra vidéo dissimulée à un endroit précis aux fins d'enquête est une chose. L'utilisation, par les autorités policières, d'OEA pour allumer la caméra sur le téléphone d'un suspect à leur gré pendant qu'il parcourt son environnement en est une autre[53].

De ce fait, le *Code criminel* doit être mis à jour et modifié de manière à tenir compte de la nature des capacités des outils de surveillance et d'enquête modernes, et du degré d'interférence de ces outils avec le droit à la vie privée.

3.2. *Loi sur le SCRS*

Comme le *Code criminel*, la *Loi sur le SCRS* n'a pas de dispositions précises sur l'utilisation des OEA par le Service. Contrairement aux mandats autorisant l'utilisation d'OEA en vertu du *Code criminel*, lesquels requièrent d'invoquer plusieurs dispositions pour rendre compte de l'utilisation de ces outils, la *Loi sur le SCRS* fournit au Service des autorisations légales générales pour l'accomplissement de sa mission consistant à assurer la protection contre les menaces envers la sécurité du Canada. La portée et le caractère général de ces dispositions font en sorte qu'il est difficile de déterminer comment et quand le Service utilise des OEA, et de savoir si le droit à la vie privée des cibles canadiennes et étrangères des enquêtes du SCRS est adéquatement protégé lorsque ces outils sont utilisés.

L'article 12 de la *Loi sur le SCRS* confère au Service le pouvoir de recueillir, d'analyser et de conserver des informations et des renseignements « au moyen d'enquêtes ou autrement » si celui-ci a des motifs raisonnables de soupçonner qu'une activité représente une « menace envers la sécurité du Canada[54] ». Si le SCRS a des motifs raisonnables d'avoir des soupçons, il peut prendre des mesures, à l'intérieur ou à l'extérieur du Canada, afin de réduire la menace[55].

https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2022-nnl-rprt-lctrnc-srvllnc/index-fr.aspx#sec2.

[53] Rapport du Comité ETHI, p. 25.

[54] *Loi sur le SCRS*, article 12.

[55] *Loi sur le SCRS*, article 12.1.

Ces mesures doivent être raisonnables et proportionnelles dans les circonstances. Elles doivent également respecter la *Charte*[56]. Lorsque ses mesures empiètent sur les droits garanti par la *Charte*, le SCRS doit obtenir un mandat de la cour les autorisant[57].

Dans de tels cas, le SCRS peut présenter à un juge une demande de mandat conformément à l'approbation du ministre de la Sécurité publique et de la Protection civile[58]. Un juge peut délivrer un tel mandat s'il est convaincu qu'il y a des motifs raisonnables de croire qu'un mandat est en effet nécessaire, et qu'une des trois autres conditions suivantes s'applique :

1. d'autres méthodes d'enquête ont été essayées et ont échoué, ou ont peu de chance de succès;
2. l'urgence de l'affaire est telle qu'il ne serait pas pratique de mener l'enquête en n'utilisant que les autres méthodes d'enquête;
3. sans mandat, il est probable que des informations importantes concernant la menace envers la sécurité du Canada ne soient pas obtenues[59].

Si les conditions pertinentes sont remplies, un juge peut délivrer un mandat autorisant le SCRS à « intercepter des communications ou à acquérir des informations, des documents ou des objets. À cette fin, il peut autoriser aussi, de leur part :

1. l'accès à un lieu ou un objet ou l'ouverture d'un objet; 2. la recherche, l'enlèvement ou la remise en place de tout document ou objet, leur examen, le prélèvement des informations qui s'y trouvent, ainsi que leur enregistrement et l'établissement de copies ou d'extraits par tout procédé; ou

4. l'installation, l'entretien ou l'enlèvement d'objets[60] ».

Il semble que ces dispositions confèrent au SCRS le pouvoir d'utiliser des OEA pour intercepter des communications en temps réel et de recueillir les données d'appareils numériques avec une seule autorisation. Il est excellent que le paragraphe 21(1) de la *Loi sur le SCRS* exige d'épuiser d'abord tous les autres moyens. Toutefois, la *Loi* actuelle n'a pas de lignes directrices pour le Service, ses responsables ni le public concernant les circonstances où les différents types de capacités d'enquête numériques peuvent être utilisés légitimement. De plus, actuellement, il n'y a pas de renseignements accessibles au public sur l'utilisation des OEA par le SCRS, ce qui pose problème sur le plan à la fois de la transparence et de la responsabilisation.

---

[56] *Loi sur le SCRS*, par. 12.1(3.1).
[57] *Loi sur le SCRS,* par. 12.1(3.2).
[58] *Loi sur le SCRS,* par. 21(1).
[59] *Loi sur le SCRS,* par. 21(2).
[60] *Loi sur le SCRS,* par. 21(3).

3.3. *Loi sur le CST*

Adoptée en 2019, la *Loi sur le CST* régit l'organisme du renseignement électromagnétique du Canada. On sait peu de choses sur les activités et les capacités du CST. Toutefois, il est probable qu'un organisme d'une telle taille et d'un tel niveau de sophistication soit capable de contourner les protections de sécurité des appareils numériques modernes afin d'accéder au contenu de ces appareils[61].

Autrement dit, il se pourrait très bien que le CST possède des capacités semblables à celles offertes par la suite de logiciels espions Pegasus de NSO Group ou par les principaux concurrents de ce dernier, peu importe que ces logiciels aient été achetés en vente libre ou conçus à l'interne.

Bien que l'adoption de la *Loi sur le CST* s'accompagne de mesures de protection essentielles pour protéger la vie privée des Canadiens, il n'est pas certain que la *Loi* sous sa forme actuelle soit à la hauteur du défi que représente la protection de la vie privée des Canadiens et des étrangers face aux capacités redoutables des OEA modernes.

La *Loi sur le CST* interdit à ce dernier de cibler toute personne vivant au Canada et tout Canadien vivant à l'étranger dans le cours de ses opérations[62]. Cependant, les renseignements sur ces

personnes peuvent être obtenus « incidemment » par le CST au cours d'activités visant des cibles étrangères[63].

En effet, des renseignements sur les Canadiens ou les personnes vivant au Canada, ce qui comprend les communications privées interceptées, peuvent être communiqués par le CST si c'est essentiel aux affaires étrangères, à la défense, à la sécurité ou à la cybersécurité, ou nécessaire pour protéger l'infrastructure canadienne de l'information[64].

La *Loi sur le CST* exige que celui-ci prenne des mesures pour protéger la vie privée des Canadiens et de toute personne vivant au Canada[65], mais non pas qu'il se préoccupe de la vie privée des étrangers, même si le droit à la vie privée est un droit de la personne universellement reconnu.

[61] Dave Seglins, *« Canada's Electronic Spy Agency's Cyberwarfare Toolbox Revealed »*, CBC News, 23 mars 2015, https://www.cbc.ca/news/canada/communication-security-establishment-s- cyberwarfare-toolbox-revealed-1.3002978.

[62] *Loi sur le CST*, par 22(1).

[63] *Loi sur le CST*, par 23(4).

[64] *Loi sur le CST*, art. 43 et 44.

[65] *Loi sur le CST*, art. 24.

À la différence des organismes d'application de la loi nationaux et du SCRS, qui doivent obtenir une autorisation judiciaire pour entreprendre des activités susceptibles de porter atteinte aux droits de la *Charte* – comme des recherches avec un appareil numérique ou une interception de communications – le CST mène des activités autorisées par le ministre de la Défense nationale – où il agit seul, avec l'approbation du commissaire au renseignement, ou en réponse à une demande du ministre des Affaires étrangères.

Le CST, en tant qu'organisme du renseignement électromagnétique, est considéré comme une entité recueillant des communications en grand volume aux fins d'analyse. La *Loi sur le CST*, quant à elle, semble lui conférer le pouvoir d'utiliser des OEA, au besoin. Plus précisément, le paragraphe 26(2) permet au CST d'installer, de maintenir, de copier, de distribuer, de rechercher, de modifier, d'interrompre, de supprimer ou d'intercepter quoi que ce soit dans l'infrastructure mondiale de l'information ou par son entremise aux fins de renseignement étranger. L'alinéa 31b) permet au CST de mener les mêmes activités dans le cadre des cyberopérations actives et défensives, tandis que l'article 41 permet au ministre de la Défense nationale d'autoriser de telles activités lors des urgences. Toutefois,

on sait peu de choses sur la façon dont le CST utilise ces autorisations, et on n'est pas certain si celles-ci ont été invoquées par le Centre pour l'utilisation de capacités associées aux OEA modernes.

4. CONCLUSION

S'il est probable que les OEA demeurent l'option « la moins mauvaise » pour les organismes de sécurité et de renseignement et les organismes d'application de la loi pour faire face aux défis posés par le chiffrement dans un avenir rapproché, comment les lois du Canada devraient-elles être réformées pour composer avec cette réalité? Comme on l'a vu dans les sections précédentes, les capacités des OEA posent des risques beaucoup plus importants que les techniques d'enquête traditionnelles pour les droits de la personne et ceux garantis par la *Charte* aux Canadiens et aux étrangers. Par conséquent, nos lois doivent être réformées de manière à régir adéquatement l'utilisation de ces technologies et à limiter l'usage de celles-ci aux situations où elles sont vraiment nécessaires.

L'Allemagne offre au Canada un exemple convaincant de la façon dont notre *Code criminel,* la *Loi sur le SCRS* et la *Loi sur le CST* devraient être réformés pour que ces outils d'enquête puissants soient utilisés dans des circonstances appropriées uniquement[66].

[66] La discussion est fortement inspirée de la recherche et l'analyse juridique réalisées par mon adjoint à la recherche, Leonhard Knebel.

Le Code de procédure pénale allemand (StPO, pour utiliser son abréviation en allemand) a été modifié en 2017 par l'ajout de trois dispositions qui tiennent compte de la manière dont les autorités policières mènent les enquêtes à l'ère du numérique[67].

D'abord, l'article 100b du StPO régit les « intrusions » réalisées par les autorités policières dans les systèmes de TI pour recueillir les données qui y sont stockées. Les demandes faites par les autorités policières en vertu de cette disposition sont évaluées non pas par le tribunal et les juges locaux, qui autorisent la plupart des perquisitions sous le régime du StPO, mais par un cabinet de spécialistes composé de trois juges qui ne sont pas autorisés à présider à des procès criminels pendant qu'ils assument cette fonction. Les juges spécialistes sont généralement mal vus dans la tradition de *common law*[68], mais les connaissances que ces juges peuvent posséder au chapitre du fonctionnement et du caractère invasif des outils utilisés pour réaliser des « intrusions » peuvent leur permettre de mieux étudier la légitimité et la proportionnalité des demandes d'autorisation faites en vertu de cette disposition.

Ensuite, l'article 100a du StPO, qui régit la surveillance des

télécommunications, a récemment été modifié de manière à traiter non pas uniquement de l'interception de communications en temps réel, mais également de l'extraction des communications chiffrées stockées sur un appareil en ligne. Cette disposition du StPO s'applique uniquement aux enquêtes sur des crimes majeurs, et sous réserve d'une exigence d'épuisement des autres moyens semblable à celle figurant à la partie VI du *Code criminel*. En fait, cette disposition traite l'extraction des communications stockées et chiffrées d'un appareil numérique comme l'équivalent fonctionnel d'une écoute électronique en temps réel, et la soumet aux mêmes protections juridiques. Par contraste, en vertu de la loi canadienne actuelle, une recherche visant un appareil électronique est assujettie au même régime légal qu'une recherche visant n'importe quel autre lieu ou n'importe quelle autre chose. Autrement dit, elle n'est pas assujettie à une exigence d'épuisement des recours comme c'est le cas pour les interceptions de communications en temps réel.

Enfin, l'article 100c du StPO, qui régit la surveillance audio et visuelle, porte expressément sur l'utilisation des OEA pour l'activation à distance d'un microphone et d'une caméra d'un appareil électronique pour en faire un moyen de surveillance. De plus, l'article 100c entraîne les protections prévues par l'article 13 de la Loi fondamentale de l'Allemagne (essentiellement sa *Charte canadienne des droits et libertés*), lequel interdit la surveillance vidéo dans les résidences, la considérant comme une violation du droit à l'inviolabilité du domicile.

[67] GESLEY, Jenny, *« Germany: Expanded Telecommunications Surveillance and Online Search Powers »*, page Web, Library of Congress, 7 septembre 2017, https://www.loc.gov/item/global-legal-monitor/2017-09-07/germany-expanded- telecommunications-surveillance-and-online-search-powers/. Une traduction anglaise non officielle des dispositions pertinentes du StPO est disponible à l'adresse suivante : https://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html.

[68] OLDFATHER, Chad M., *« Judging, Expertise, and the Rule of Law »*, SSRN Scholarly Paper (Rochester, NY, 30 mars 2011), https://papers.ssrn.com/abstract=1799568.

Les réformes juridiques allemandes récentes sont une source d'inspiration pour la modification de la *Loi sur le SCRS* et de la *Loi sur le CST* quant à réglementer l'utilisation des puissants OEA par ces organismes.

La loi de l'Allemagne sur son service de renseignement extérieur (BND-G) a été modifiée en 2021 de manière à réglementer spécifiquement l'« intrusion dans les systèmes de TI » dans les opérations du Service. L'article 34 régit l'utilisation des OEA et des

capacités connexes dirigées vers les citoyens étrangers dans les opérations de la BND. L'utilisation de ces capacités doit être autorisée par le président de la BND en vertu d'une ordonnance relative au renseignement qui précise, entre autres, (1) l'objectif de la collecte de renseignements; (2) l'individu, le groupe ou le système de TI visé par l'opération; (3) l'étendue et la durée de l'intrusion, ainsi que la méthode utilisée; (4) le motif de l'opération.

En utilisant de tels outils dans ses opérations, la BND ne peut pas cibler les « aspects les plus sensibles de la vie privée ». La Loi fondamentale de l'Allemagne s'applique aux opérations menées par les autorités allemandes dans le monde entier;

5. Ainsi, l'article 34 de la BND-G reconnaît et respecte le droit à la vie privée en matière p. ex. familiale et sentimentale, même pour les cibles étrangères du renseignement. Également, l'article 34 interdit l'utilisation des OEA pour cibler des relations confidentielles telles que celles entre un prêtre et un pénitent, ou celles entre un journaliste et une source, sauf si les personnes en question sont soupçonnées d'avoir commis un crime grave ou d'avoir menacé la sécurité de l'Allemagne, de l'Union européenne ou de l'OTAN.

Alors que le Comité étudie comment réformer les lois canadiennes de manière à tenir compte de la réalité numérique dans laquelle nous vivons, il y a beaucoup à tirer de la façon dont l'Allemagne a récemment réformé ses lois afin de trouver un meilleur équilibre entre les droits de la personne de tous ses citoyens et les besoins légitimes des organismes d'enquête de son gouvernement.

[69] ROJSZCZAK, Marcin, *« Extraterritorial Bulk Surveillance after the German BND Act Judgment »*, European Constitutional Law Review 17, nº 1 (mars 2021) : 53 77, https://doi.org/10.1017/S1574019621000055. Par contraste, les tribunaux canadiens ont refusé d'étendre l'application de la Charte des droits et libertés en dehors du Canada dans des circonstances similaires. Voir Leah West, *« Within or Outside Canada: The Charter's Application to the Extraterritorial Activities of the Canadian Security Intelligence Service »*, Université de Toronto, Law Journal 73, nº 1 (1er novembre 2022) : 1 52, https://doi.org/10.3138/utlj-2021-0105.