UNIVERSITY OF TORONTO

munkschool
OF GLOBAL AFFAIRS & PUBLIC POLICY

Mémoire au Comité sénatorial permanent de la sécurité nationale, de la défense et des anciens combattants : Étude du projet de loi C-26 : Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois

Mémoire soumis par Kate Robertson
Citizen Lab, Munk School of Global Affairs & Public Policy
Université de Toronto

Partie 1. Introduction

1. En 2022, Citizen Lab a publié le document *Cybersecurity Will Not Thrive in Darkness: A Critical Analysis of Proposed Amendments in Bill C-26 to the Telecommunications Act* (« *Cybersecurity Will Not Thrive in Darkness*[1] *»*)). Le rapport a été rédigé par Christopher Parsons[2]. M. Parsons a examiné de façon approfondie le projet de loi proposé en vertu du projet de loi C-26, y compris les lacunes relevées. Ce faisant, M. Parsons a fourni le contexte historique et international nécessaire entourant la réforme proposée par le gouvernement fédéral dans le secteur des télécommunications. Le Canada n'est pas le premier de ses alliés à introduire de nouveaux pouvoirs gouvernementaux en raison d'une préoccupation et d'une sensibilisation accrues à l'égard des risques réels et alarmants pour les infrastructures essentielles. Toutefois, M. Parsons a affirmé que même si le projet de loi pouvait faire progresser des objectifs importants, sa version actuelle contenait des lacunes thématiques qui risquaient de miner son efficacité. Le rapport figure à l'**annexe B**.

2. Intégrant l'analyse contenue dans *Cybersecurity Will Not Thrive in Darkness* et prenant en considération les évolutions survenues depuis la parution du rapport, dont l'étude ainsi que l'amendement du projet de loi C-26 par le Comité permanent de la sécurité publique et nationale (SECU), ce mémoire est divisé en deux parties :

    a. **Partie 2 : Vulnérabilités des réseaux de communications mobiles :** La partie 2 du présent mémoire situe le projet de loi C-26 dans le contexte de lacunes historiques et persistantes en matière de surveillance réglementaire, de transparence et de responsabilisation qui ont entraîné de graves menaces pour les réseaux mobiles contemporains.

    b. **Partie 3 : Le projet de loi C-26 et la *Charte canadienne des droits et libertés* (la « *Charte* »)** : La partie 3 du présent mémoire traite du lien entre le projet de loi C-26 et la *Charte*. Elle met l'accent, en particulier, sur la façon dont le projet de loi C-26 peut avoir une incidence sur la liberté d'expression (alinéa 2*b*)) et la vie privée (article 8). Les répercussions du projet de loi sur la *Charte* devraient être un facteur central pour ce comité et tout au long du processus parlementaire à venir. La partie 3 propose également une analyse approfondie et des recommandations d'amendements pour remédier aux lacunes thématiques relevées dans le projet de loi C-26. Ces recommandations visent à combler les lacunes générales, y compris les questions de secret et de transparence, et reconnaissent la nécessité d'intégrer des balises pour les nouveaux pouvoirs gouvernementaux que le projet de loi crée.

    c. **Partie 4 : Les pouvoirs du projet de loi C-26 minant le chiffrement :** La partie 4 traite de l'importance pour les législateurs de créer des normes de sécurité solides et neutres vis-à-vis des fournisseurs, sans concessions, qui s'appliquent à l'ensemble des réseaux canadiens, plutôt que de se limiter à certains fournisseurs. Si le projet de loi C-26 est adopté sans amendement, tous les fournisseurs de télécommunications au Canada seront contraints, par des décrets secrets, d'affaiblir le chiffrement ou le matériel pour les réseaux. À cet égard, la partie 4 traite de la nécessité

[1] Christopher Parsons, « *Cybersecurity Will Not Thrive in Darkness: A Critical Analysis of Proposed Amendments in Bill C-26 to the Telecommunications Act* », rapport de recherche du Citizen Lab nº 158, Université de Toronto, octobre 2022.

[2] Ce rapport a également été publié à l'époque où M. Parsons était chercheur principal au Citizen Lab. Par conséquent, ses conclusions et ses recommandations ne reflètent pas nécessairement celles de son employeur actuel.

d'un amendement qui empêcherait le gouvernement fédéral d'avoir le pouvoir de contraindre les exploitants de réseaux à compromettre les normes de sécurité nécessaires.

Partie 2. Vulnérabilités historiques et actuelles dans les réseaux de communications mobiles à l'échelle mondiale

3. Les lois proposées dans le cadre du projet de loi C-26 doivent être considérées en fonction des vulnérabilités historiques et continues des réseaux de communications mobiles. En 2023, le Citizen Lab a publié le rapport *Finding You: The Network Effect of Telecommunications Vulnerabilities for Location Disclosure* (« *Finding You* ») [EN ANGLAIS SEULEMENT], rédigé par Gary Miller et Christopher Parsons[3]. Le rapport donne un aperçu général des menaces liées à la géolocalisation provenant des opérateurs de réseaux 3G, 4G et 5G. Les preuves de la prolifération de ces menaces démontrent comment les protocoles de signalisation qu'utilisent les fournisseurs de services de télécommunication pour faciliter l'itinérance permettent également aux réseaux de récupérer des données concernant la vie intime de l'utilisateur. Des acteurs du domaine de la surveillance ciblent et exploitent constamment les protocoles, « ce qui a pour effet d'exposer nos téléphones à de nombreuses méthodes de divulgation du lieu physique[4] ». Les risques et le secret entourant la surveillance de la géolocalisation mobile sont renforcés par des couches d'ententes commerciales et de sous-ententes entre les exploitants des réseaux, les intermédiaires des réseaux et les fournisseurs de services tiers. En fin de compte, les vulnérabilités des protocoles de signalisation ont « permis la mise au point de produits de surveillance commerciaux qui fournissent à leurs opérateurs l'anonymat, de multiples points d'accès et vecteurs d'attaque, un réseau omniprésent et accessible à l'échelle mondiale avec une liste illimitée de cibles, et pratiquement aucun risque financier ou juridique[5] ».

4. Ces vulnérabilités ne se limitent pas à la surveillance de l'emplacement à elle seule. Une fois en position d'accéder aux protocoles de signalisation, « les fournisseurs de surveillance privés ont carte blanche pour agir comme une entreprise de télécommunications afin d'échanger les mêmes messages de signalisation, mais exploitent cet accès pour suivre discrètement des personnes, perturber leurs services de téléphonie mobile, ou même intercepter leurs messages texte et leur messagerie vocale[6] ».

5. Il est grand temps que les responsables des organismes de réglementation prennent des mesures au niveau à la fois national et international pour sécuriser le service de réseau. Dans le rapport *Finding You,* on souligne l'importance d'élaborer une stratégie en matière de cybersécurité pour exiger l'adoption de normes en matière de sécurité à l'échelle du réseau, y compris l'obligation pour les exploitants de réseaux d'adopter la gamme complète des fonctions de sécurité offertes dans les normes et l'équipement 5G. Dans les conclusions du rapport, on souligne également l'importance de la transparence publique et de la responsabilisation dans la réglementation des opérateurs de télécommunications. Comme le notent les

[3] Gary Miller et Christopher Parsons. « *Finding You: The Network Effect of Telecommunications Vulnerabilities for Location Disclosure* », rapport de recherche du Citizen Lab nº 171, Université de Toronto, octobre 2023. M. Parsons était chercheur principal au Citizen Lab au moment de la production du rapport. Les conclusions du rapport font l'objet de commentaires et de recommandations dans le présent mémoire, mais ces commentaires ne reflètent pas nécessairement ceux de son employeur actuel.

[4] *Finding You*, p. 1 [TRADUCTION].

[5] *Finding You*, p. 2 [TRADUCTION].

[6] Ron Deibert et Gary Miller, « When You Roam, You're Not Alone », *Lawfare*, 28 décembre 2023 [TRADUCTION].

auteurs, « des décennies de manque de responsabilisation et de transparence ont contribué à l'environnement actuel où de vastes attaques de surveillance de la géolocalisation ne sont pas signalées[7] ». C'est pourquoi l'approche du gouvernement du Canada en matière de réglementation des télécommunications ainsi que de la cybersécurité doit être transparente, responsable et conforme aux normes applicables en matière de droits de la personne. Les recommandations formulées dans ce mémoire visent à corriger les déséquilibres présents dans l'avant-projet de loi.

Partie 3. Le projet de loi C-26 et la Charte : Vers une approche axée sur la sécurité humaine en matière de cybersécurité

6. En analysant les modifications proposées à la Loi sur les télécommunications du Canada dans le projet de loi C-26, M. Parsons a relevé les lacunes thématiques suivantes dans le projet de loi :

    - L'étendue de ce que le gouvernement pourrait ordonner à un fournisseur de services de télécommunication de faire n'est pas suffisamment limitée.
    - Des dispositions excessives sur le secret et la confidentialité dans le projet de loi menacent d'établir une catégorie de lois et de règlements secrets.
    - Il existe un risque important d'échange excessif de renseignements au sein du gouvernement fédéral ainsi qu'avec des partenaires internationaux.
    - Les coûts associés à l'observation des mesures amenées par les réformes pourraient menacer la viabilité des petits fournisseurs.
    - La formulation vague du projet de loi ne permet pas d'en évaluer pleinement les limites.
    - Il n'y a aucune reconnaissance du droit à la vie privée ou d'autres droits protégés par la *Charte* dans le projet de loi C-26 pour permettre de faire contrepoids aux exigences de sécurité proposées, et aucune exigence appropriée de transparence ou de reddition de comptes n'est imposée au gouvernement[8].

7. Ces lacunes thématiques ont trait à l'efficacité de la stratégie en matière de cybersécurité du gouvernement ainsi qu'aux risques potentiels pour les droits protégés par la Charte. À l'instar du Conseil de la radiodiffusion et des télécommunications canadiennes (« CRTC »), le gouvernement fédéral doit agir conformément à la *Charte* lorsqu'il réglemente les services de télécommunication et la cybersécurité.

8. À la suite de la publication du rapport de M. Parsons en octobre 2022 (y compris sa recommandation que le gouvernement fédéral dépose un énoncé concernant la Charte relativement au projet de loi C-26), le gouvernement fédéral a déposé son énoncé concernant la Charte à la Chambre des communes le 14 décembre 2022. L'énoncé non exhaustif indique les domaines dans lesquels le projet de loi C-26 met en cause certains droits protégés par la *Charte*. Toutefois, l'énoncé ne traite pas entièrement des questions pertinentes liées à la *Charte* liées au projet de loi C-26. Dans les paragraphes suivants (9 à 15 et 17 à 32), j'aborde des questions supplémentaires liées à la *Charte* pour, premièrement, soutenir les modifications proposées dans ce mémoire, et deuxièmement, souligner l'importance d'adopter une approche axée sur les

[7] *Finding You*, p. 32 [TRADUCTION].
[8] *Cybersecurity Will Not Thrive in Darkness*, précité, p. 4.

droits de la personne et la sécurité humaine en matière de cybersécurité et de réglementation des services de télécommunications.

Freedom of Expression and Section 2(b) of the *Charter*

9. L'ébauche actuelle des dispositions excessives sur le secret et la confidentialité du projet de loi C-26 compromet le droit à la liberté d'expression en vertu de l'alinéa 2b) de la Charte. L'énoncé concernant la Charte du gouvernement met l'accent sur le discours des entités commerciales qui seront directement réglementées en vertu du projet de loi C-26. Dans l'énoncé concernant la *Charte*, on soutient que, comme les restrictions sur le discours commercial n'ont pas tendance à mettre en cause les valeurs fondamentales de l'alinéa 2*b*), les restrictions peuvent être plus faciles à justifier[9]. Cependant, cette analyse ne prend pas en compte la manière dont les droits individuels garantis par la *Charte* pourraient être entravés par le projet de loi actuel, ne distinguant pas les acteurs commerciaux de leurs utilisateurs. Les dispositions excessives sur le secret et la confidentialité contenues dans le projet de loi restreignent également la liberté d'expression du public et des médias au Canada.

10. Les principes de la publicité des débats et du gouvernement ouvert sont des composantes dérivées de l'alinéa 2*b*) de la *Charte* (liberté d'expression). Le principe de la publicité des débats exige que les procédures judiciaires, y compris les contrôles judiciaires devant la Cour fédérale, soient présumées ouvertes et accessibles au public et aux médias. L'accès à l'information sur les mesures gouvernementales peut également être un droit dérivé de l'alinéa 2b), si un refus d'accès à l'information gouvernementale empêche effectivement une discussion publique significative sur une question d'intérêt public. Lorsque les restrictions à l'accès entravent considérablement les discussions et les critiques significatives sur des questions d'intérêt public, le gouvernement doit raisonnablement justifier sa violation de la liberté d'expression[10].

11. Les lois et politiques en matière de télécommunications et de cybersécurité sont sans aucun doute une question d'intérêt public. Il existe un lien étroit entre les droits de la personne et la politique publique concernant la réglementation des services de télécommunications. La politique canadienne en matière de télécommunications est intimement liée au « tissu social et économique » du Canada et de ses régions[11]. L'accès équitable aux services de télécommunications est parfois décrit comme un mécanisme d'« autodétermination numérique », ce qui témoigne de la nécessité de protéger le potentiel d'épanouissement humain à l'ère numérique[12].

12. Le récent rapport du Citizen Lab, Finding You, met en lumière plusieurs façons dont le secret excessif entourant la surveillance des télécommunications met en danger le public. Les auteurs notent des lacunes historiques dans la surveillance et la reddition de comptes pour la sécurité des réseaux, qui ont entraîné des menaces liées à la géolocalisation associées aux réseaux contemporains. Le secret excessif a contribué à la persistance de la « menace de géolocalisation facile » identifiée dans le rapport Finding You :

---

[9] Ministère de la Justice Canada, « Énoncé concernant la *Charte* : Projet de loi C-26 : Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois », 14 décembre 2022.

[10] Ontario (*Sûreté et Sécurité publique*) c. *Criminal Lawyers' Association*, 2010 CSC 23; *ARPA Canada and Patricia Maloney vR.*, 2017, ONSC 3285 [en anglais seulement]. Cette enquête comprend la mise en balance de toute considération compensatoire (comme un privilège) qui pourrait militer contre la divulgation.

[11] *Loi sur les télécommunications*, L.C. 1993, ch. 38, alinéa 7*a*).

[12] Voir le document de Nydia Remolina et Mark James Findlay, « *The Paths to Digital Self-Determination— A Foundational Theoretical Framework* », (22 avril 2021), document de recherche nº 03/2021 du SMU Centre for AI & Data Governance [en anglais seulement].

> Des décennies de manque de responsabilisation et de transparence ont contribué à l'environnement actuel où de vastes attaques de surveillance de la géolocalisation ne sont pas signalées. Ce statu quo a effectivement créé un marché florissant de la surveillance de géolocalisation tout en assurant que certains fournisseurs de services de télécommunication tirent profit du fait de fermer les yeux sur la disponibilité de leurs interconnexions réseau avec l'industrie de la surveillance[13].

13. Les menaces de surveillance de la géolocalisation abordées dans le rapport Finding You mettent en péril de façon disproportionnée les défenseurs des droits de la personne et d'autres personnes qui font face à des risques accrus de menaces ciblées à la sécurité (p. ex. cadres d'entreprise, personnel militaire, politiciens et leur personnel, hauts fonctionnaires, etc.). Par le passé, l'industrie a exigé d'importantes sommes d'argent pour recevoir de l'information sur les menaces bien connues de l'industrie, ce qui a pour effet d'empêcher des groupes non industriels comme les chercheurs dans le domaine de la sécurité et la société civile d'obtenir et de diffuser de l'information sur la nature des menaces auxquelles font face les personnes à risque, ou de défendre les recours qui profiteraient à la sécurité et à la vie privée de la société civile. Les auteurs notent que, dans bien des cas, les gens ne peuvent pas déterminer si leur propre fournisseur de services de télécommunication a « déployé et configuré des pare-feu de sécurité pour s'assurer que les messages de signalisation associés aux attaques de géolocalisation, aux attaques pour usurper l'identité ou à toute autre activité malveillante ne sont pas dirigés vers leur téléphone[14] ».

14. Les recherches du Citizen Lab soulignent l'intérêt public substantiel à permettre aux médias, aux chercheurs dans le domaine de la sécurité, à la société civile et au public (y compris les personnes confrontées à des risques accrus en matière de sécurité) d'accéder à l'information sur les politiques et les règlements en matière de télécommunications, et à la nature des risques pour la sécurité qui persistent en tout ou en partie. Comme l'ont souligné les chercheurs dans le domaine de la sécurité, « la voie la plus prometteuse vers une accessibilité complète [en matière de cybersécurité] réside dans la collaboration entre les fournisseurs, les groupes de défense d'intérêts et le gouvernement[15] ». Cette collaboration est facilitée grâce à « un discours auquel participent des professionnels de la cybersécurité, des universitaires dans le domaine de la sécurité axés sur la personne, des organismes caritatifs pour les personnes handicapées et d'autres intervenants[16] ». Les membres de la société civile et du milieu des affaires en général peuvent faire pression sur « les responsables des organismes de réglementation, les décideurs et les politiciens pour contraindre activement les fournisseurs de services de télécommunication à adopter des postures de sécurité appropriées afin d'atténuer les menaces pernicieuses et silencieuses associées à la surveillance de la géolocalisation[17] », ainsi que d'autres risques similaires en matière de sécurité.

15. Bien qu'une certaine confidentialité soit appropriée pour s'assurer que les vulnérabilités en matière de sécurité non résolues sont effectivement contrôlées, certains pouvoirs prévus dans le projet de loi C-26 vont plus loin que ce qui est requis pour atteindre les objectifs en matière de cybersécurité et de sécurité nationale. En outre, certains pouvoirs proposés ne sont pas accompagnés de mesures raisonnablement disponibles permettant de protéger l'intérêt de la population à accéder à l'information concernant ce domaine important d'intervention gouvernementale. Tel qu'il est rédigé, l'article 15.9 imposerait également des limites obligatoires

---

[13] *Finding You*, précité, p. 32.
[14] *Finding You*, précité, p. 32 [TRADUCTION].
[15] Karen Renaud et Lizzie Coles-Kemp, « *Accessible and Inclusive Cyber Security: A Nuanced and Complex Challenge* », SN Computer Science (2022) 3: 346, à la page 2 de 14 [en anglais seulement] [TRADUCTION].
[16] *Ibid.* [TRADUCTION]
[17] *Finding You*, précité, p. 33 [TRADUCTION].

aux principes de la publicité des débats, ce qui empêcherait les juges d'exercer leur pouvoir discrétionnaire pour concilier le besoin de secret ou de confidentialité et l'intérêt public lié à la communication. Comme il est mentionné au paragraphe 10 du présent document, la *Charte* protège les principes de la publicité des débats qui s'appliquent dans le contexte du contrôle judiciaire, y compris les mesures de protection de la liberté d'expression prévues par la *Charte*.

16. **À la lumière des lacunes relevées non résolues concernant le secret excessif ou l'absence de dispositions de responsabilisation, je recommande ce qui suit :**

    a. **Recommandation 1 : Les décrets de non-divulgation devraient être limités dans le temps.** Dans le projet de loi C-26, on propose des dispositions de bâillon en ce qui concerne les décrets ou les arrêtés ministériels, qui ne sont pas limités, que ce soit sur le plan temporel (c.-à-d., pendant combien de temps le secret est-il nécessaire?) ou de manière significative (c.-à-d., dans quelles circonstances le secret sera-t-il justifié?). Comme il est mentionné au paragraphe 10, les décrets de non-divulgation touchent non seulement le destinataire de l'ordonnance de bâillon, mais aussi le droit de la population à de l'information qui éclaire un débat démocratique significatif. La loi devrait être modifiée pour inclure des contraintes de temps entourant les ordonnances de non-divulgation. Si le ministre a besoin de plus de temps au-delà de la limite fixée, je suis d'accord avec la *Présentation conjointe de la société civile au Sénat concernant le projet de loi C-26*, selon laquelle le gouvernement devrait être tenu d'obtenir une ordonnance d'un tribunal fédéral pour autoriser toute prolongation supplémentaire des ordonnances de non-divulgation[18].

    b. **Recommandation 2 : Les circonstances dans lesquelles la confidentialité est censée être justifiée dans une ordonnance de non-divulgation devraient être définies dans la législation.** Compte tenu des conséquences graves et négatives sur la liberté d'expression de l'exclusion de la population de l'accès aux ordonnances, les raisons qui justifient le secret autour de l'émission d'une ordonnance de non-divulgation devaient être définies dans la loi. Par exemple, dans les procédures de contrôle judiciaire en vertu du projet de loi C-26, la divulgation est limitée dans les cas où elle « porterait atteinte aux relations internationales, à la défense nationale, à la sécurité nationale ou à la sécurité d'autrui ». À l'inverse, il n'existe aucune restriction sur les circonstances dans lesquelles des décrets de non-divulgation pourraient être émis, ce qui permet aux fonctionnaires gouvernementaux de préférer éviter le contrôle public et la responsabilisation démocratique.

    c. **Recommandation 3 : Section 15.9 L'article 15.9 devrait être modifié pour que le juge conserve le pouvoir d'établir un équilibre entre l'intérêt public à l'égard de la divulgation et l'intérêt à l'égard de la confidentialité :** En général, les limites obligatoires imposées à la publicité des débats (qui empêchent le juge d'équilibrer les intérêts publics en jeu) sont généralement considérées comme des atteintes excessives aux droits garantis par l'alinéa 2*b*)[19]. Par exemple, même dans des dispositions analogues de la Loi sur la preuve au Canada (permettant le secret dans des procédures judiciaires pour des questions portant atteinte aux relations internationales, à la défense ou à la sécurité nationale ou qui mettent en danger la sécurité d'une personne), le juge conserve le pouvoir de déterminer que « l'intérêt public à la divulgation l'emporte sur l'importance de l'intérêt public à la

[18] *Présentation conjointe de la société civile au Sénat concernant le projet de loi C-26*, p. 8.

[19] Voir Kent Roach et David Schneiderman, « Freedom of Expression in Canada », (2013) 61 S.C.L.R. (2d), p. 488 (« Même si les tribunaux sont généralement enclins à radier les interdictions obligatoires d'accès aux tribunaux, ils se montrent également plus respectueux des interdictions qui laissent aux juges la discrétion de limiter l'accès aux tribunaux et la liberté d'expression. »)

non-divulgation ». La même mesure de sécurité devrait être intégrée à l'article 15.9 du projet de loi C-26 afin de s'assurer que toute limite à l'ouverture porte minimalement atteinte à la liberté d'expression.

d. **Recommandation 4 : Lorsque des résumés des éléments de preuve et des renseignements reçus par le tribunal sont fournis, conformément à l'alinéa 15.9(1)*c*), ils devraient être mis à la disposition du « demandeur <u>et [du] public</u> ».** Comme il est mentionné au paragraphe 10, le principe de la publicité des débats protège l'intérêt du public et des médias à l'égard de la transparence des procédures judiciaires. En pratique, le droit d'accès de la population aux résumés judiciaires de cette nature est habituellement servi à l'aide de la désignation de ces résumés comme des pièces à l'instance. Le droit d'accès du public aux pièces est un corollaire du principe de la publicité des débats.

e. **Recommandation 5 : Le seuil déclencheur justifiant les limites relatives à la transparence des procédures ne devrait pas être supérieur à celui qui est déjà contenu dans les dispositions analogues de la *Loi sur la preuve au Canada*[20].** À cet égard, nous recommandons de reproduire le libellé de la Loi sur la preuve au Canada au moyen de la modification suivante :

> Alinéa 15.9(1)a) : « […] si, de l'avis du juge, la divulgation de ces éléments de preuve ou renseignements ~~pourrait~~ porter atteinte aux relations internationales, à la défense nationale, à la sécurité nationale ou à la sécurité d'autrui ».

<u>Incidences sur la vie privée et article 8 de la *Charte*</u>

17. Le projet de loi C-26 propose plusieurs nouveaux pouvoirs en matière de collecte et d'échange de renseignements, ce qui peut comprendre la collecte ou l'échange de renseignements personnels en possession des fournisseurs de télécommunications et d'infrastructures essentielles. Bon nombre de ces pouvoirs ne sont pas suffisamment délimités ou définis. L'absence de mécanismes importants de responsabilisation et de surveillance accroît les risques d'atteinte à la vie privée que posent les pouvoirs. L'étendue des pouvoirs de collecte et d'échange de renseignements augmente le risque considérable que la loi, si elle est adoptée telle que rédigée, interfère de manière déraisonnable avec l'article 8 de la *Charte*. Le principal déficit constitutionnel du projet de loi C-26 réside dans la proposition d'accorder au ministre de l'Industrie un nouveau pouvoir de collecte sans précédent lui permettant de réclamer des renseignements personnels de nature très délicate aux fournisseurs de télécommunications et aux infrastructures critiques au Canada <u>*sans*</u> un examen et une approbation judiciaires préalables.

18. Un aspect fondamental de la protection de l'article 8 est de préserver la vie privée en exigeant des mécanismes adéquats de responsabilisation et de contrôle pour accompagner les pouvoirs de collecte de renseignements. Les pouvoirs de collecte doivent également être raisonnables et justifiés. Sans des mesures de protection clairement établies et raisonnables, une loi qui permet des intrusions sur des attentes raisonnables en matière de vie privée n'est pas conforme à l'article 8 de la *Charte*.

19. À titre de contexte, après que le projet de loi C-26 a été déposé, le ministère de la Justice a publié son énoncé concernant la *Charte*, affirmant que le projet de loi C-26 n'interfère pas avec l'article 8, en partie en raison du fait que « les renseignements recueillis, puis échangés dans ce contexte concernent les opérations

[20] Voir *Loi sur la preuve au Canada*, L.R.C. 1985, ch. C-5, article 38 à 38.15.

techniques des FST, qui sont des entités commerciales », plutôt qu'à des « renseignements biographiques ou personnels qui suscitent des attentes élevées en matière de respect de la vie privée[21] ».

20. Toutefois, le projet de loi C-26 ne restreint pas les pouvoirs de collecte du ministre à des renseignements techniques uniquement. L'article 15.4 conférerait plutôt au ministre le pouvoir d'exiger de « toute personne » qu'elle fournisse tout renseignement « selon les modalités qu'il précise » s'il a des motifs raisonnables de croire qu'ils sont pertinents pour ses pouvoirs en matière de décrets, un seuil extrêmement bas[22].

21. Les opérateurs de télécommunications concernés par le projet de loi C-26 sont des transmetteurs des renseignements les plus privés connus dans le système judiciaire. Comme l'a fait remarquer le Commissaire à la protection de la vie privée du Canada durant son témoignage concernant le projet de loi C-26[23], la loi pourrait entraîner l'échange inapproprié de renseignements sur les comptes d'abonnés, de données de communication, de visites de sites Web, de métadonnées, de données de localisation et de données financières. Il n'existe aucun doute raisonnable sur le fait que de telles sources d'information comportent des intérêts importants en matière de protection de la vie privée. Cette réalité a été maintes fois confirmée par la Cour suprême, et le gouvernement est extrêmement bien informé de l'importance de la protection de la vie privée des particuliers concernant ces données[24].

22. Autrement dit, les incidences potentielles sur la vie privée du projet de loi C-26 sont nettement plus importantes que celles qui ont été analysées par le ministère de la Justice dans son énoncé concernant la *Charte*, lorsqu'il a affirmé n'avoir identifié aucune lacune constitutionnelle dans le projet de loi C-26 en rapport avec l'article 8 de la *Charte*. En vertu de la loi, le pouvoir proposé est également présumément déraisonnable, et donc présumément contraire à cet article 8, car il autoriserait la collecte de renseignements qui sont soumis à une attente raisonnable de vie privée, sans autorisation préalable par un organe judiciaire indépendant[25].

23. À la suite de son étude par le Comité permanent de la sécurité publique et nationale, la Partie I du projet de loi C-26 prévoit maintenant *une certaine* protection légale pour les renseignements personnels et dépersonnalisés en tant que « renseignements confidentiels ». Néanmoins, cette modification ne permet pas d'aborder de manière adéquate les problèmes constitutionnels significatifs que comporte le projet de loi. L'article 15.4 du projet de loi C-26 donnerait au ministre de l'Industrie un pouvoir sans précédent, sans mandat, pour recueillir des données sur les télécommunications et pour échanger ces renseignements à grande échelle dans l'ensemble du gouvernement fédéral, y compris avec le Service canadien du renseignement de sécurité (SCRS) et le Centre de la sécurité des télécommunications (CST). Dans la loi, il est énoncé que les pouvoirs ne permettent pas l'interception des communications privées (paragraphe 15.2[2.2]), mais les fournisseurs de télécommunications hébergent des volumes de renseignements personnels de nature délicate qui pourraient être recueillis dans des circonstances qui ne répondent pas à la définition technique de l'interception de telles communications. Les renseignements ne

---

[21] Ministère de la Justice Canada, « Énoncé concernant la *Charte* : Projet de loi C-26 : Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois », 14 décembre 2022.
[22] À la suite des modifications apportées lors de l'étude du projet de loi par les membres du Comité permanent de la sécurité publique et nationale, on reconnaît maintenant explicitement dans celui-ci la capacité de saisir « des renseignements personnels et dépersonnalisés », qui sont désormais inclus dans la définition de renseignements confidentiels selon la Partie I (alinéa 15.5[1] *d*)).
[23] Procès-verbaux du Comité permanent de la sécurité publique et nationale concernant le projet de loi C-26, Témoignage de Philippe Dufresne, commissaire à la protection de la vie privée du Canada, 15 février 2024.
[24] Voir, p. ex., *R. c. Jones*, 2017 CSC 60; *R. c. Spencer*, 2014 CSC 43; *R. c. Bykovets*, 2024 CSC 6.
[25] *Hunter et coll. v Southam Inc.,* [1984] 2 RCS 145.

doivent aucunement répondre à la définition de communications privées pour que l'article 8 soit protégé en vertu de la *Charte* et, par conséquent, le projet de loi est manifestement incomplet.

24. La collecte ainsi que l'utilisation par les organismes de sécurité et de renseignement d'information au sujet de Canadiens ou de personnes se trouvant au Canada sont une question fondamentale d'intérêt à la fois public et constitutionnel. Il y a quelques années seulement, les lois canadiennes sur la sécurité nationale ont été considérablement remaniées dans le cadre de la *Loi de 2017 sur la sécurité nationale*[26]. Dans ce train de réformes législatives complètes, le Parlement a tenté d'établir un équilibre entre la nécessité de mesures de protection et les contraintes soigneusement calibrées entourant la collecte d'information au Canada. Les protections ainsi que les limitations varient considérablement entre les organes de sécurité et de renseignements de sécurité. Les « mandats des différents organismes de renseignement et de sécurité du Canada… sont extrêmement importants pour déterminer la légalité d'une activité d'enquête donnée[27] ». Le CST, par exemple, ne peut diriger ses activités vers les Canadiens ou les personnes au Canada et il existe une série de mécanismes qui cherchent à équilibrer les intérêts constitutionnellement protégés visés par le mandat et les pouvoirs du CST. Par contre, le SCRS a pour mandat de recueillir des renseignements sur les menaces au Canada. Toutefois, les responsables du SCRS sont tenus d'obtenir l'approbation des tribunaux fédéraux pour recueillir des données qui sont susceptibles de protéger la vie privée auprès des fournisseurs de télécommunications du Canada[28].

25. Dans de nombreux domaines importants, la constitutionnalité des lois canadiennes sur la sécurité nationale après 2017 n'a pas encore été examinée ou déterminée par les tribunaux canadiens. Cela est particulièrement remarquable étant donné que bon nombre des réformes qui sont maintenant mises en œuvre en vertu de la *Loi de 2017 sur la sécurité nationale* sont controversées et ont fait l'objet d'un débat public intense. Depuis l'adoption de la *Loi*, en 2019, le débat public et l'examen continuent d'être justifiés. Parmi les nombreux exemples de ce genre, une décision rendue publique par la Cour fédérale au début de 2024 a soulevé de graves préoccupations concernant des révélations d'échange inapproprié de renseignements personnels de Canadiens dans des circonstances impliquant à la fois le CST et le SCRS[29]. La Cour a critiqué à plusieurs reprises le manque de franchise du SCRS envers elle, affirmant que « l'échec touche au cœur même de la relation entre le SCRS et la Cour[30] ». Les juges de la Cour fédérale ont fait remarquer que ce n'était pas le premier type de décision de ce genre de ces dernières années[31].

26. Depuis sa création, l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR) a signalé des problèmes chroniques dans le contrôle de la légalité des activités du CST, les

---

[26] *Loi de 2017 sur la sécurité nationale*, L.C. 2019, ch 13.

[27] Craig Forcese et Leah West, *National Security Law* (Canada : Irwin Law, 2020, p. 387 [TRADUCTION].

[28] *Loi sur le Service canadien du renseignement de sécurité*, L.R.C. 1985, ch. C-23, art. 21 (et les modifications connexes à la suite de l'adoption récente du projet de loi C-70, Loi visant à lutter contre l'ingérence étrangère).

[29] *Loi sur le Service canadien du renseignement de sécurité (CA) (Re)*, 2023 cf. 1341.

[30] *Ibid*., par. 7 [TRADUCTION].

[31] Citant *Loi sur le Service canadien du renseignement de sécurité (Ca) (Re)*, 2020 cf. 616 aux paragraphes 83 à 85, 91 à 100 et 167 (autre décision dans laquelle le SCRS a omis de divulguer une question concernant des renseignements qui avaient été recueillis potentiellement illégalement). La Cour a conclu que « les éléments de preuve indiquent que la question de l'illégalité potentielle était largement connue dans le cercle des organisations et institutions qui jouent un rôle dans la surveillance ou la gestion des opérations du SCRS... Malgré cette connaissance répandue et la pertinence potentielle de la question de l'illégalité dans le contexte des demandes de mandat, la question n'a jamais été portée à l'attention de la Cour. Cette situation est inexcusable, surtout lorsqu'il y a eu une sensibilisation accrue à l'importance du devoir de franchise et d'engagement continu entre la Cour, le Service et le ministère de la Justice dans le calcul de la décision *Données associées* et du rapport Segal. Il semble que seule la Cour était dans l'ignorance » (par. 168).

difficultés à obtenir l'accord du CST pour fournir à l'OSSNR les renseignements nécessaires pour examiner la légalité des activités du CST[32]. Dans le dernier rapport annuel, on continue de signaler « d'importantes difficultés d'accès à l'information du CST dans le cadre de cet examen », ce qui ne permet pas de donner confiance aux responsables de l'OSSNR dans « l'exhaustivité de l'information fournie par le CST[33] ».

27. Dans un rapport publié le 27 mars 2024[34], l'OSSNR a également soulevé de graves préoccupations au sujet du traitement par le SCRS des ensembles de données concernant les Canadiens et les personnes se trouvant au Canada. Entre autres constatations, l'OSSNR a conclu que « le régime des ensembles de données établi par le SCRS n'était pas conforme au cadre législatif en vigueur », que « le SCRS n'a pas été en mesure d'opérationnaliser adéquatement le régime des ensembles de données », et lorsque la Cour fédérale s'est trouvée confrontée à des préoccupations concernant l'étendue des ensembles de données du SCRS, ce dernier « n'a pas cherché à résoudre les éléments juridiques ambigus des modalités d'application du régime à l'appréciation de la Cour ».

28. Il est particulièrement inquiétant que les responsables de l'OSSNR aient soulevé des préoccupations selon lesquelles « l'approche que le SCRS applique actuellement sur le plan de la collecte des ensembles de données au titre de l'article 12 pose le risque de créer un mécanisme de collecte parallèle qui pourrait affaiblir les critères minimaux tout en se privant d'un régime de surveillance externe apte à protéger les renseignements personnels dans le contexte du régime des ensembles de données[35] ».

29. Dans ce contexte, les législateurs devraient être prudents lorsqu'ils examinent la pertinence ou la nécessité de conférer de nouveaux pouvoirs supplémentaires en vertu du projet de loi C-26, surtout compte tenu de l'incapacité de ce projet de loi d'assurer que la Cour fédérale conserve un rôle crucial dans la vérification et l'autorisation des demandes du gouvernement à l'égard de données de télécommunications soumises à l'attente d'un certain respect de la vie privée. Les institutions indépendantes de contrôle judiciaire, quasi judiciaire ou expert permettent au Parlement de jouer un rôle essentiel dans l'assurance que les lois du Canada sont adéquates pour obliger les organismes gouvernementaux à rendre des comptes et protéger les droits constitutionnels de tous les Canadiens. L'OSSNR a été créé comme organisme de contrôle indépendant et externe qui fait rapport au Parlement. En corollaire, il est important que le Parlement soit attentif et réactif aux conclusions dont ses responsables font part.

30. Malgré la précarité de l'équilibre actuel dans la loi canadienne sur la sécurité nationale, le projet de loi C-26 ne ferait que déstabiliser davantage les circonstances existantes en créant un nouveau portail de collecte et d'échange de renseignements entre les fournisseurs de télécommunications, le ministre de l'Industrie et les organismes de sécurité nationale du Canada. Le canal d'échange de renseignements mis en place par le projet de loi C-26 semble accomplir indirectement ce que le SCRS ainsi que le CST ne peuvent légalement

---

[32] Christopher Parsons, « Do not give more powers to CSE until it submits to effective review », *Policy Options*, 29 novembre 2022, citant les rapports annuels 2020 et 2021 qui attirent l'attention sur la résistance continue du CST à fournir à l'OSSNR les renseignements qu'il juge nécessaires pour que l'OSSNR examine la légalité des activités du CST.

[33] Office de surveillance des activités en matière de sécurité nationale et de renseignement, Rapport annuel 2022, déposé au Parlement le 30 octobre 2023.

[34] Office de surveillance des activités en matière de sécurité nationale et de renseignement, Examen de l'OSSNR portant sur le régime applicable aux ensembles de données, publié le 27 mars 2024

[35] Ces risques sont maintenant accrus par les nouvelles modifications législatives apportées à la loi habilitante du SCRS qui ont été adoptées par le Parlement en vertu du projet de loi C-70.

faire directement[36], et on n'y définit pas clairement le rôle de la Cour fédérale dans l'examen et l'autorisation de toute collecte de renseignements auprès des fournisseurs de télécommunications qui est assujettie à l'attente d'un certain respect de la vie privée. La crainte que, au sein d'organismes gouvernementaux comme le CST, on utilise et réutilise les renseignements que l'on reçoit dans le cadre du projet de loi C-26 pour d'autres activités de renseignement n'a rien d'hypothétique. Comme il est mentionné dans la *Présentation conjointe de la société civile au Sénat concernant le projet de loi C-26*[37], le témoignage du directeur général de la politique stratégique au CST a confirmé l'intérêt au sein de l'organisme à utiliser les renseignements recueillis grâce aux nouveaux pouvoirs conférés par le projet de loi C-26 à des fins autres que pour son mandat de cybersécurité et de sûreté des renseignements[38].

31. Dans son énoncé concernant la *Charte* sur le projet de loi C-26, le ministre de la Justice affirme que les intérêts en matière de protection des renseignements personnels diminuent dans « les contextes réglementaires et administratifs ». Toutefois, comme il est mentionné ci-dessus, il avait supposé que le projet de loi C-26 était axé sur la collecte d'informations « techniques », plutôt que sur les « renseignements personnels qui suscitent un intérêt accru en matière de protection de la vie privée[39] ». Les attentes des acteurs commerciaux dans les « domaines d'activité fortement réglementés » peuvent avoir été « diminuées », mais les intérêts des personnes qui dépendent des services de télécommunication et d'infrastructure critique en matière de vie privée ne diminuent en rien.

32. De plus, les pouvoirs de collecte et d'échange de renseignements proposés dans le projet de loi C-26 sont loin d'être un exemple typique des régimes « réglementaires » qui ont été examinés dans les cours canadiennes. Dans sa *substance*, le projet de loi C-26 vise à réforme des lois ainsi que des pouvoirs en matière de sécurité nationale du Canada et aura des répercussions potentielles sur les intérêts en matière de protection de la vie privée de millions de personnes au Canada, des personnes qui ne sont pas des entreprises « réglementées ». Il faut qu'une approbation judiciaire préalable de la Cour fédérale soit requise pour l'obtention de renseignements qui font l'objet d'une attente raisonnable en matière de protection de la vie privée, avec des dispositions pour les circonstances exceptionnelles dans des circonstances d'urgence. C'est une raison essentielle pour laquelle les pouvoirs de collecte sans mandat du projet de loi C-26 sont présumés déraisonnables en vertu de la *Charte*. Même s'il s'agissait d'un régime réglementaire ordinaire, les juges de la Cour suprême affirment que, « même si un contrôle moins rigoureux peut se révéler suffisant dans un contexte réglementaire, la possibilité de recourir au contrôle et l'efficacité de celui-ci sont néanmoins pertinentes pour permettre de juger du caractère raisonnable pour l'application de l'article 8[40] ».

---

[36] Comme il a été mentionné, le SCRS est tenu d'obtenir de la Cour fédérale l'autorisation d'obtenir des renseignements qui sont assujettis à une attente raisonnable de confidentialité auprès des fournisseurs de télécommunications : *Loi sur le Service canadien du renseignement de sécurité*, L.R.C. 1985, ch. C-23, art. 21 (et les modifications connexes à la suite de l'adoption récente du projet de loi C-70, *Loi visant à lutter contre l'ingérence étrangère).* Pour sa part, lorsqu'ils agissent conformément à leur mandat en matière de cybersécurité et de sûreté des renseignements, les agents du CST ne sont pas autorisés à rechercher intentionnellement des données concernant des Canadiens ou des personnes au Canada ni à diriger leurs activités d'acquisition d'information vers des Canadiens ou des personnes au Canada : *Loi sur le Centre de la sécurité des télécommunications,* L.C. 2019, c. 13, art. 76, art. 23 (voir aussi *ibid.* aux par. 22[1] et [2]).

[37] *Présentation conjointe de la société civile au Sénat concernant le projet de loi C-26*, p. 17-18.

[38] Procès-verbaux du Comité permanent de la sécurité publique et nationale concernant le projet de loi C-26, Témoignage de M. Stephen Bolton (directeur général, Politique stratégique, Centre de la sécurité des télécommunications), 8 avril 2024.

[39] Ministère de la Justice Canada, « Énoncé concernant la *Charte* : Projet de loi C-26 : Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois », 14 décembre 2022.

[40] *Goodwin c. Colombie-Britannique (Superintendent of Motor Vehicles)*, 2015 CSC 46, par. 71. Voir *R. c. Tse*, 2012 CSC 16, par. 83

33. Pour imposer des balises plus appropriées aux pouvoirs proposés d'échanger des renseignements au sein des organismes canadiens et ailleurs, je recommande les modifications suivantes, qui s'appuient sur les recommandations de M. Parsons dans *La cybersécurité ne prospérera pas dans l'obscurité*[41] :

    a. **Recommandation 6 : Une autorisation judiciaire préalable doit être requise pour que le gouvernement obtienne des renseignements personnels ou dépersonnalisés d'un fournisseur de services de télécommunications.** La loi devrait être modifiée de telle sorte que, avant que le gouvernement puisse obliger un fournisseur de télécommunications à divulguer des renseignements personnels ou dépersonnalisés[42], il doit d'abord obtenir l'autorisation judiciaire de la Cour fédérale. Cette modification est essentielle pour combler les lacunes constitutionnelles de l'ébauche actuelle du projet de loi C-26. Comme il a été mentionné précédemment, les fournisseurs de services de télécommunication hébergent des renseignements qui comptent parmi les plus hauts niveaux de protection de la vie privée de notre système juridique. La surveillance judiciaire est essentielle à la protection de ces renseignements reconnue à l'article 8 de la *Charte*.

    b. **Recommandation 7 : Les renseignements obtenus des fournisseurs de services de télécommunication ne doivent être utilisés que par les organismes gouvernementaux pour les activités de cybersécurité et de sûreté des renseignements.** Les renseignements ne doivent pas être utilisés à des fins de renseignement de signalisation et de renseignement étranger, d'aide interministérielle non liée à la cybersécurité ou de cyberopérations actives ou défensives. Ces restrictions devraient s'appliquer à tous les organismes.

    c. **Recommandation 8 : La collecte et l'échange de renseignements personnels devraient être soumis à des exigences de nécessité et de proportionnalité.** Plusieurs témoins ont évoqué devant le Comité permanent de la sécurité publique et nationale l'importance d'inclure la nécessité et la proportionnalité comme mesure de sécurité dans le projet de loi C-26. En réponse, un fonctionnaire du ministère de l'Industrie a fait état des secteurs où la proportionnalité pourrait déjà être intégrée dans la loi en vigueur sur la prise de décisions administratives ou dans le droit constitutionnel[43]. Toutefois, il s'agit de questions juridiques distinctes, qui ne suppriment ni ne rendent caduque la nécessité d'exiger la proportionnalité comme limite à un pouvoir statutaire important. Par exemple, en vertu de la *Loi sur le Centre de la sécurité des télécommunications*, le ministre ne peut délivrer une autorisation de cybersécurité à moins que le ministre « conclue qu'il y

---

à 85; *Wakeling c. États-Unis d'Amérique*, 2014 CSC 72, par. 70; *T.L. c. British Columbia (Attorney General)*, 2023 BCCA 167, par. 171 à 173 et 237 [TRADUCTION].

[41] À titre de comparaison, les recommandations 6, 7, 9, 11 et 12 de cette section se trouvent dans les recommandations 29, 16, 13, 14, 17, 18 et 20 de *La cybersécurité ne prospérera pas dans l'obscurité*.

[42] Comme mentionné dans une étude antérieure du Citizen Lab, « lorsque des renseignements personnels ont été dépersonnalisés ou agrégés, il peut être possible de réidentifier les personnes en tirant des inférences ou en établissant des corrélations à partir des données ou en les superposant sur des renseignements personnels connus » : Amanda Cutinha et Christopher Parsons. « *Minding Your Business: A Critical Analysis of the Collection of De-identified Mobility Data and Its Use Under the Socially Beneficial and Legitimate Interest Exemptions in Canadian Privacy Law* », rapport de recherche du Citizen Lab nº 161, Université de Toronto, 22 novembre 2022.

[43] Procès-verbaux du Comité permanent de la sécurité publique et nationale concernant le projet de loi C-26, Témoignage d'Andre Arbour, directeur général, Secteur des stratégies et politiques d'innovation, ministère de l'Industrie, 18 mars 2024.

a des motifs raisonnables de croire que l'activité en cause est raisonnable et proportionnelle compte tenu de la nature de l'objectif à atteindre et des activités[44] ».

De plus, le Comité permanent de la sécurité publique et nationale n'a pas déposé ou voté une modification qui appliquerait spécifiquement les normes de nécessité et de proportionnalité pour la collecte et l'échange de renseignements personnels[45]. Dans son témoignage devant le Comité, le commissaire à la protection de la vie privée du Canada a souligné l'importance d'exiger à la fois la nécessité et la proportionnalité pour que les pouvoirs soient aussi peu intrusifs que possible pour les intérêts en matière de protection de la vie privée[46]. Exiger la nécessité et la proportionnalité dans le contexte de l'échange de renseignements protégerait les personnes qui dépendent des services de télécommunication au Canada, et qui seraient indirectement touchées par le cadre réglementaire du projet de loi C-26. À cette fin, je recommande les modifications suivantes :

- Article 15.4 : Le pouvoir de recueillir des renseignements prévus à l'art. 15.4 devrait comprendre les exigences de nécessité et de proportionnalité.
- Paragraphe 15.6(1) : « Malgré l'article 15.5, dans la mesure nécessaire **et proportionnelle** à toute fin… »
- Alinéa 15.5(3)*c*) : La même modification « nécessaire **et proportionnelle** » devrait être ajoutée à l'alinéa 15.5(3)*c*).

d. **Recommandation 9 : Des périodes de conservation des données devraient être imposées aux données des fournisseurs de télécommunication et aux divulgations de renseignements à l'étranger.** Il faudrait modifier la loi afin qu'il y soit précisé que les renseignements confidentiels ne peuvent être conservés que le temps nécessaire pour qu'un décret soit rendu, modifié ou révoqué en vertu de l'article 15.1 ou 15.2, ou un règlement, en vertu de l'alinéa 15.8(1)*a*), pour que la conformité soit vérifiée, ou pour que le non-respect d'un tel décret, arrêté ou règlement soit empêché… De même, une modification devrait également exiger que le gouvernement joigne des clauses sur la conservation et la suppression des données dans les ententes ou les protocoles d'entente conclus avec des organismes étrangers. Les périodes de conservation doivent être communiquées aux fournisseurs de services de télécommunication concernés.

e. **Recommandation 10 : Le consentement ne devrait être obtenu que de la personne à qui les renseignements se rapportent.** L'alinéa 15.5(3)*b*) permet la divulgation de renseignements confidentiels avec le consentement de la personne qui a désigné ces renseignements comme étant confidentiels. Toutefois, maintenant que les membres du Comité permanent de la sécurité publique et nationale y ont apporté un amendement lors de l'étude du projet de loi C-26 afin d'ajouter les renseignements personnels et dépersonnalisés à la portée des « renseignements confidentiels », il faudrait modifier l'alinéa 15.5(3)*b*) pour tenir compte des circonstances particulières de ces

[44] *Loi sur le Centre de la sécurité des télécommunications*, L.C. 2019, ch. 13, art 34 (1).
[45] Les membres du Comité permanent de la sécurité publique et nationale ont examiné une modification connexe qui aurait permis d'inclure un libellé dans les nouveaux paragraphes 15.1(1.1) et 15.2(2.1) pour s'assurer que les décrets ainsi que les arrêtés sont proportionnels à la gravité de la menace d'interférence, de manipulation, de perturbation ou de dégradation : Procès-verbaux du Comité permanent de la sécurité publique et nationale concernant le projet de loi C-26, 18 mars 2024.
[46] Procès-verbaux du Comité permanent de la sécurité publique et nationale concernant le projet de loi C-26, Témoignage de Philippe Dufresne, commissaire à la protection de la vie privée du Canada, 15 février 2024.

renseignements personnels et dépersonnalisés. Il s'agit d'un changement positif, et il faudrait en outre préciser la disposition relative au consentement qui accompagne les renseignements confidentiels. Compte tenu des mécanismes de divulgation alternatifs prévus aux alinéas 15.5*a*) et *c*), il serait préoccupant que la loi permette aux opérateurs de télécommunication de « consentir » au nom des utilisateurs à la communication de renseignements de nature hautement délicate à d'autres organismes gouvernementaux, y compris ceux relevant du ministre de la Sécurité publique et de la Protection civile (p. ex., la GRC et le Service canadien du renseignement de sécurité) ainsi que du ministre de la Défense nationale (p. ex., les Forces armées canadiennes et le Centre de la sécurité des renseignements). Comme l'a rappelé la Cour suprême, le consentement à renoncer au droit constitutionnel à la vie privée ne peut être donné par un tiers[47], y compris par des fournisseurs de télécommunications, en ce qui concerne les données privées de leurs utilisateurs[48].

L'exclusion des renseignements personnels ou dépersonnalisés de l'alinéa 15.5(3)*b*) ou la modification de la disposition comme suit :

> « la personne qui a désigné les renseignements comme confidentiels consent à leur communication, **ou dans le cas de renseignements personnels ou dépersonnalisés, la personne à laquelle les renseignements se rapportent consent à leur communication** » pourrait avoir une incidence sur cette modification.

f. **Recommandation 11 : Des indemnisations devraient être prévues si le gouvernement ne gère pas correctement les renseignements confidentiels.** Il faudrait modifier la loi pour permettre aux particuliers et aux fournisseurs de services de télécommunication de demander réparation si le gouvernement ou une partie à laquelle il a divulgué des renseignements confidentiels, personnels ou dépersonnalisés perd le contrôle de ces renseignements, lorsque cette perte de contrôle entraîne des conséquences importantes pour le particulier ou pour les activités commerciales ou techniques d'un fournisseur de services de télécommunication.

g. **Recommandation 12 : La loi devrait mieux préciser les conditions dans lesquelles les renseignements d'une organisation privée peuvent être divulgués.** Tel qu'il est rédigé, le paragraphe 15.7(1) semble entraîner l'établissement d'un seuil excessivement bas pour la divulgation de renseignements aux gouvernements étrangers afin que soient contrées des menaces non précisées qui ne sont pas énoncées dans la loi. Le seuil ne comprend aucun critère de caractère raisonnable, de nécessité ou de proportionnalité. Comme l'a souligné M. Parsons, « l'utilisation conjointe des termes « croit » et « pourraient » suggère que les conditions qui doivent être remplies avant la divulgation des renseignements ne sont pas particulièrement strictes[49] ». De plus, l'utilisation du terme « y compris » dans le projet de loi actuel ne définit pas clairement ce que l'on entend par « assurer la sécurité » d'un système de télécommunications canadien ou étranger[50]. Les modifications textuelles proposées se trouvent à la page 30 du rapport Cybersecurity Cannot Thrive in the Darkness (annexe A du présent mémoire).

---

[47] *R. c. Cole*, [2012] 3 R.C.S. 34.
[48] *R. c. Spencer*, 2014 CSC 43.
[49] Christopher Parsons, « *Cybersecurity Will Not Thrive in Darkness: A Critical Analysis of Proposed Amendments in Bill C-26 to the Telecommunications Act* » [en anglais seulement] », rapport de recherche du Citizen Lab nº 158, Université de Toronto, octobre 2022, p. 40 [TRADUCTION].
[50] *Ibid*.

Partie 4. Le projet de loi C-26 contient des pouvoirs de chiffrement qui compromettent la sécurité des réseaux du Canada

34. La partie 4 recommande d'ajouter une clause interprétative à l'article 15.2 pour confirmer que ses pouvoirs ne peuvent être utilisés pour « **compromettre la confidentialité, la disponibilité ou l'intégrité d'une installation de télécommunication, d'un service de télécommunication ou d'une installation de transmission** ». Comme le précise la partie 4, cet amendement vise à éliminer un danger essentiel de cybersécurité, soit que les pouvoirs étendus prévus à l'article 15.2 du projet de loi C-26 puissent être utilisés pour émettre des arrêtés qui affaiblissent les normes de chiffrement dans les réseaux de télécommunication[51]. Compte tenu du fait que le gouvernement fédéral a déclaré que l'intention du projet de loi C-26 est de mieux protéger la sécurité des réseaux canadiens, cet amendement est essentiel pour faire en sorte que les pouvoirs généraux prévus à l'article 15.2 ne soient pas mis en œuvre d'une façon qui *affaiblisse* la sécurité des réseaux. Cet amendement figure également dans la *Présentation conjointe de la société civile au Sénat concernant le projet de loi C-26* (recommandation 1).

35. En 2022, le gouvernement fédéral a annoncé une mesure visant à bloquer l'équipement de télécommunications de Huawei et ZTE, en invoquant les « répercussions économiques et sécuritaires en cascade[52] » qu'une violation de la chaîne d'approvisionnement mettrait en danger. Le gouvernement a mentionné des préoccupations selon lesquelles Huawei ou ZTE pourraient être « obligés de se conformer à des directives extrajudiciaires de gouvernements étrangers[53] ». Pourtant, le projet de loi C-26 conférerait aux fonctionnaires canadiens les mêmes pouvoirs que ceux que le gouvernement a publiquement condamnés. Si le projet de loi C-26 est adopté sans amendement, tous les fournisseurs de télécommunications au Canada seraient contraints, par des décrets secrets, d'intégrer des mesures de protection dans les réseaux canadiens en diminuant la sécurité du chiffrement ou de l'équipement réseau. Plus précisément, le libellé général des alinéas 15.2(2)*c*), l) et *m*) pourrait être servir à ordonner aux responsables des entreprises de télécommunications canadiennes d'instaurer des mesures relatives à l'accès légal dans les composantes chiffrées des réseaux de télécommunication du Canada.

36. Par exemple, à l'alinéa 15.2(2)*l*), on énonce que le ministre peut rendre un décret exigeant « qu'un fournisseur de services de télécommunication mette en œuvre des normes qu'il précise relativement à ses services de télécommunication ». Cela pourrait inclure l'obligation pour les fournisseurs de télécommunications de modifier les normes de chiffrement 5G qui protègent les communications mobiles[54] afin de permettre au gouvernement d'avoir une plus grande visibilité sur les données de communication. Le secteur des télécommunications au Canada est d'accord. Dans son témoignage devant le Comité permanent de la sécurité publique et nationale, Eric Smith, vice-président principal de l'Association canadienne des

---

[51] L'analyse de la présente partie 4 est élaborée à partir de : Kate Robertson et Ron Deibert, « Ottawa wants the power to create secret backdoors in our networks to allow for surveillance », *The Globe and Mail*, 29 mai 2024.

[52] Innovation, Sciences et Développement économique Canada, « Énoncé de politique – Sécuriser le système de télécommunications au Canada https://www.canada.ca/fr/innovation-sciences-developpement-economique/nouvelles/2022/05/enonce-de-politique--securiser-le-systeme-de-telecommunications-au-canada.html », 19 mai 2022.

[53] *Ibid*. [TRADUCTION]

[54] 3GPP, « SA WG3 — Security and Privacy », en ligne : <https://www.3gpp.org/3gpp-groups/service-system-aspects-sa/sa-wg3>, (consulté le 15 octobre 2024).

télécommunications, a également averti que les pouvoirs « très larges » du projet de loi C- 26 pourraient servir à affaiblir le chiffrement[55].

37. Les normes de chiffrement dans la 5G protègent un réseau de points de connexion entourant nos communications mobiles, protégeant ainsi les utilisateurs contre les attaques de type homme du milieu qui exposent les utilisateurs au suivi de leur localisation et à l'interception de messages texte et d'appels vocaux. Compromettre ces normes augmenterait la surface d'attaque des menaces malveillantes contre la vie privée et la sécurité de tous les utilisateurs du réseau, y compris les plus hauts fonctionnaires canadiens[56]. De nouvelles vulnérabilités compromettraient également les appareils intelligents connectés au nuage, comme les voitures, la vidéosurveillance à domicile ou les stimulateurs cardiaques[57] et les services par satellite comme Starlink[58].

38. Malgré l'avertissement de plusieurs témoins que le projet de loi C-26 pourrait en fait faciliter les nouveaux pouvoirs du gouvernement pour obliger le déchiffrement dans les normes de télécommunications, le gouvernement a présenté le projet de loi sans débat ni amendement pour régler le problème. La volonté du gouvernement de le faire soulève des questions, surtout qu'il a déclaré publiquement que l'intention du projet de loi n'est pas de créer un nouveau « mandat de surveillance[59] ».

39. La mise en place de pouvoirs pour affaiblir les normes de chiffrement des télécommunications ne ferait qu'ancrer ou intensifier les menaces de cybersécurité dans les réseaux du Canada. De nos jours, de nombreuses failles de sécurité des réseaux subsistent, atteignant même les couches d'infrastructure des technologies de communication. Le système de signalisation nº 7 (SS7), conçu en 1975 pour diriger les appels téléphoniques, est devenu une source importante d'insécurité pour les téléphones mobiles[60]. En 2017, un rapport de CBC a révélé que des pirates n'auraient eu besoin que du numéro de téléphone cellulaire d'un député canadien pour intercepter ses mouvements, ses messages vocaux, ses messages textes et ses appels téléphoniques[61]. Peu de choses ont changé depuis. Tel qu'il a été mentionné auparavant dans ce mémoire, dans un rapport datant de 2023, le Citizen Lab documente les vulnérabilités omniprésentes au cœur des réseaux mobiles mondiaux[62].

40. Pour faire face aux vulnérabilités critiques, le gouvernement fédéral devrait exercer un leadership en imposant aux opérateurs de réseau d'adopter toutes les fonctionnalités de sécurité disponibles dans les normes et équipements 5G, y compris toutes les capacités de chiffrement qui accompagnent la technologie 5G et,

---

[55] Procès-verbaux du Comité permanent de la sécurité publique et nationale concernant le projet de loi C-26, Témoignage d'Eric Smith, vice-président principal, Association canadienne des télécommunications, 18 mars 2024

[56] Catherine Cullen et Brigitte Bureau, « Someone is spying on cellphones in the nation's capital », *CBC News*, 3 avril 2017.

[57] Centre canadien pour la cybersécurité, « Considérations liées à la cybersécurité pour les réseaux 5G (ITSAP.80.116) », septembre 2022.

[58] Centre canadien pour la cybersécurité, « Télécommunications par satellite - ITSAP.80.029 », mars 2023.

[59] Procès-verbaux du Comité permanent de la sécurité publique et nationale concernant le projet de loi C-26, Témoignage de la députée Jennifer O'Connell, 8 avril 2024.

[60] Bill Marczak, John Scott-Railton, Siddharth Prakash Rao, Siena Anstis et Ron Deibert, « Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles », rapport de recherche du Citizen Lab nº 133, Université de Toronto, décembre 2020.

[61] Brigitte Bureau, Catherine Cullen, et Kristen Everson, « Hackers only needed a phone number to track this MP's cellphone », *CBC News*, 24 novembre 2017.

[62] Gary Miller et Christopher Parsons. « *Finding You: The Network Effect of Telecommunications Vulnerabilities for Location Disclosure* », rapport de recherche du Citizen Lab nº 171, Université de Toronto, octobre 2023.

éventuellement, 6G — sans compromis[63]. Cependant, au lieu de corriger les failles, le projet de loi C-26 donnerait au gouvernement la capacité d'infecter les outils de cybersécurité de nouvelle génération avec d'anciennes menaces. Ce faisant, le gouvernement s'octroie le pouvoir d'être le seul arbitre des moments et des conditions selon lesquels les Canadiens méritent la sécurité de leurs communications les plus confidentielles, qu'elles soient personnelles, professionnelles, religieuses ou autres.

41. Compromettre le chiffrement des réseaux serait un avantage pour les cybercriminels. Selon un rapport technique de 2020 produit par l'Union internationale des télécommunications (UIT), agissant par l'intermédiaire de l'Initiative mondiale en faveur de l'inclusion financière (un partenariat entre l'UIT, la Banque mondiale et le Committee on Payments and Market Instructure), des acteurs malveillants exploitent régulièrement les vulnérabilités des télécommunications pour commettre des fraudes financières en ligne :

> Les vulnérabilités des télécommunications permettent aux criminels d'effectuer divers types d'attaques entraînant des fraudes pour voler de l'argent numérique; un grand nombre de ces attaques impliquent que l'attaquant se fasse passer pour le fournisseur de [services financiers numériques (SFN)]], afin de frauder l'utilisateur final, ou pour l'utilisateur final, afin de frauder le fournisseur de SFN. Dans toutes ces situations, l'attaquant exploite les vulnérabilités des télécommunications pour passer l'authentification et réaliser des opérations sur des comptes compromis[64].

42. Les fraudeurs peuvent recourir à différentes attaques pour contourner l'authentification à deux facteurs, accéder sans autorisation aux comptes bancaires en ligne, ou récolter des données sensibles qui sont ensuite utilisées pour créer des attaques d'hameçonnage plus élaborées[65]. L'UIT note que « l'exploitation de ces vulnérabilités permet aux attaquants de commettre des fraudes et de voler les fonds de victimes sans méfiance, qui dans la plupart des cas ne sont pas au courant que leur compte est compromis ou piraté[66] ». Le rapport indique qu'il est « erroné » de dire que ces attaques sont difficiles à perpétrer : « aujourd'hui, tout pirate informatique ayant environ 500 $ à dépenser peut exploiter les vulnérabilités des réseaux cellulaires[67] ».

43. Selon des estimations récentes, seulement un quart des opérateurs de réseaux mobiles dans le monde ont déployé un pare-feu de signalisation conçu pour nuire à la surveillance de la géolocalisation[68]. Selon une enquête réalisée par l'Agence européenne pour la cybersécurité des réseaux et de l'information, environ 75 % des opérateurs européens ont affirmé dans une enquête que « le coût est le facteur limitant dans la mise en œuvre, ainsi que l'absence de réglementation l'exigeant[69] ». Pour cette raison, dans le rapport *Finding You*,

---

[63] *Ibid,* partie 5, p. 33.

[64] Financial Inclusion Global Initiative, Security, Infrastructure and Trust Working Group, *Technical report on SS7 vulnerabilities and mitigation measures for digital financial services transactions* (Union internationale des télécommunications, 2020), p. 9.

[65] *Ibid.*, p. 11 et 14.

[66] *Ibid.*, p. 9 [TRADUCTION].

[67] *Ibid.*, p. 13 [TRADUCTION].

[68] *Finding You*, p. 2, citant Mobileum, Mobilesquared, *The State of the Signaling Firewall Landscape*, novembre 2021, <https://www.mobilesquared.co.uk/wp-content/uploads/2023/04/Mobileum_Security-Research_Nov21-FINAL-VERSION.pdf > Une enquête menée auprès des opérateurs de réseaux dans l'Union européenne par l'Agence européenne pour la cybersécurité des réseaux et de l'information a également révélé que seulement 28 % des opérateurs ont mis en place des pare-feu de signalisation : *Signalling Security in Telecom: SS7/Diameter/5G EU level assessment of the current situation*, mars 2018, <https://www.enisa.europa.eu/publications/signalling-security-in-telecom-ss7-diameter-5g>.

[69] Financial Inclusion Global Initiative, Security, Infrastructure and Trust Working Group, *Technical report on SS7 vulnerabilities and*

on recommande aux législateurs et aux responsables des organismes de réglementation de se demander si les participants du secteur mobile dans leur territoire « sont engagés dans des pratiques commerciales douteuses qui mettent en danger la sécurité, la vie privée et les droits des consommateurs » ou s'ils « donnent la priorité aux revenus plutôt qu'à la protection de leurs abonnés[70] ».

44. Lors des délibérations à la Chambre des communes, le gouvernement a souligné qu'un objectif fondamental du projet de loi C-26 est de donner au gouvernement l'autorité « d'interdire aux fournisseurs canadiens de services de télécommunications d'utiliser des produits et des services de fournisseurs à risque élevé, comme Huawei et ZTE, au besoin et après consultation[71] ». Toutefois, le cadre de cybersécurité du Canada ne devrait pas être axé sur des fournisseurs ou des opérateurs individuels, mais plutôt sur des normes de sécurité solides et neutres qui s'appliquent à tous les réseaux canadiens. À cette fin, le gouvernement ne devrait pas être habilité à obliger les exploitants de réseaux à compromettre l'intégrité de ces normes de sécurité.

45. Malheureusement, l'histoire est riche en exemples de portes dérobées par le gouvernement qui exposent les individus à des niveaux profonds d'insécurité informatique[72]. Bien que les portes dérobées puissent être destinées à la surveillance gouvernementale, les points d'accès installés dans des éléments de réseau chiffrés peuvent être exploités par les organismes d'application de la loi, les criminels et les rivaux étrangers. Il a été démontré que les équipements d'interception utilisés par les gouvernements présentent des lacunes importantes en matière de sécurité[73].

46. Comme exemple récent et dévastateur, le 5 octobre 2024, le *Wall Street Journal* a rapporté une « brèche de sécurité catastrophique » causée par un groupe de piratage lié à la République populaire de Chine, qui « a pénétré dans les réseaux d'une bande de fournisseurs américains de services à large bande, ayant potentiellement accès aux renseignements provenant des systèmes utilisés par le gouvernement fédéral pour les demandes d'écoute électronique autorisées par les tribunaux[74] ». Les « pirates semblent avoir pris part à une vaste collecte de trafic Internet provenant de fournisseurs d'accès Internet qui comptent des entreprises grandes et petites, et des millions d'Américains, comme clients[75] ».

47. Le 11 octobre 2024, le sénateur américain Ron Wyden a envoyé une lettre de réponse à la Commission fédérale des communications et au procureur général des États-Unis, dans laquelle il écrit que « la récente attaque par piratage des systèmes d'écoute électronique des entreprises de télécommunications américaines devrait constituer un signal d'alarme important pour le gouvernement[76] ». Le sénateur Wyden a souligné la

---

mitigation measures for digital financial services transactions (Union internationale des télécommunications, 2020), p. 2017, citant l'Agence européenne pour la cybersécurité, *Signalling Security in Telecom: SS7/Diameter/5G EU level assessment of the current situation*, mars 2018, <https://www.enisa.europa.eu/publications/signalling-security-in-telecom-ss-7-diameter-5g>; Catherine Cullen et Brigitte Bureau, « Les compagnies de téléphone cellulaire pourraient devoir renforcer la protection des renseignements personnels, a déclaré le ministre », *CBC News*, 23 novembre 2017 [TRADUCTION].

[70] Gary Miller et Christopher Parsons. « *Finding You: The Network Effect of Telecommunications Vulnerabilities for Location Disclosure* », rapport de recherche du Citizen Lab n° 171, Université de Toronto, octobre 2023, p. 32 [TRADUCTION].

[71] Débats de la Chambre des communes, Témoignage du ministre de la Sécurité publique, Marco Mendocino, 1er décembre 2022.

[72] James Ball, Julian Borger et Glenn Greenwaldm « Revealed: how US and UK spy agencies defeat internet privacy and security », *The Guardian*, 6 septembre 2013.

[73] James Bambord, « A Death in Athens: Did a Rogue NSA Operation Cause the Death ofa Greek Telecom Employee? », *The Intercept*, 28 septembre 2015; Dan Goodin, « Root backdoor found in surveillance gear used by law enforcement », 28 mai 2014.

[74] Sarah Krouse, Dustin Volz, Aruna Viswanatha et Robert McMillan, « U.S. Wiretap Systems Targeted in China-Linked Hack », *The Wall Street Journal*, 5 octobre 2024 [TRADUCTION].

[75] *Ibid*. [TRADUCTION]

[76] Lettre, sénateur des États-Unis Ron Wyden, 11 octobre 2024, <https://www.wyden.senate.gov/imo/media/doc/wyden_letter_to_fcc__doj_on_wiretapping_systems_hackpdf.pdf> [TRADUCTION].

nécessité d'une action réglementaire pour sécuriser les réseaux américains, et a souligné que le ministère de la Justice des États-Unis « doit cesser de faire pression pour des politiques qui nuisent à la vie privée et à la sécurité des Américains en défendant les portes dérobées de surveillance dans d'autres technologies de communication », étant donné que ces portes dérobées « créent une cible irrésistible pour les pirates informatiques et les espions[77] ». Le sénateur Wyden a souligné la responsabilité partagée des deux entreprises de télécommunications et des lois fédérales qui ont imposé les systèmes de surveillance, pour l'insécurité dans les systèmes de télécommunication. Le sénateur Wyden a écrit :

> Lors des audiences du Congrès pour la Commission on Accreditation for Law Enforcement Agencies, les experts en cybersécurité ont averti que les portes dérobées seraient des cibles privilégiées pour les pirates informatiques et les agents des services de renseignement étrangers. Ces préoccupations ont toutefois été écartées par le directeur du FBI de l'époque, Louis J. Freeh, qui a déclaré au Congrès que les craintes des experts quant à une vulnérabilité accrue étaient « infondées et déplacées ». Le Congrès, s'appuyant sur les assurances du directeur du FBI selon lesquelles les risques de sécurité signalés par les experts pouvaient être résolus, a adopté la loi imposant des portes dérobées.
>
> … Bien que le gouvernement n'ait pas publié d'information publique sur le piratage le plus récent, si les rapports de presse sont exacts, il est possible qu'il ait causé un préjudice énorme à la sécurité nationale des États-Unis[78].

48. Ces événements récents aux États-Unis devraient également servir de signal d'alarme pour corriger la loi canadienne sur la cybersécurité, comme le propose le projet de loi C-26. Analysant le projet de loi C-26 en juin 2024 (avant la récente atteinte à la sécurité), la Electronic Frontier Foundation a déclaré que « l'expérience américaine offre un récit alarmant de ce qui peut arriver lorsqu'un gouvernement s'accorde de larges pouvoirs pour surveiller et diriger les réseaux de télécommunications, en l'absence de protections correspondantes des droits de la personne[79] ».

49. Si le projet de loi C-26 donne au gouvernement le pouvoir d'obliger les opérateurs de télécommunications à affaiblir les dispositifs ou équipements de sécurité de nouvelle génération pour permettre la surveillance par les autorités canadiennes, il ouvrira sans aucun doute la voie aux adversaires ou aux sociétés de cyberespionnage pour trouver plus de moyens d'accéder aux communications des citoyens[80]. Les gouvernements autoritaires à l'étranger pourraient aussi invoquer la loi canadienne pour justifier leur propre loi répressive en matière de sécurité. Comme Ron Deibert et moi-même l'avons conclu en écrivant pour le *Globe and Mail* en mai 2024 :

> Dans ce contexte de menaces, le projet de loi C-26 est crucial. Le Canada a besoin de lois sur la cybersécurité qui permettent de reconnaître explicitement que le chiffrement sans compromis est

[77] *Ibid*. [TRADUCTION]
[78] *Ibid*.
[79] Corynne McSherry, Matthew Guariglia, Brendan Gilligan, et Andrew Crocker, « Security, Surveillance, and Government Overreach – the United States Set the Path but Canada Shouldn't Follow It », Electronic Frontier Foundation, juin 2024 [TRADUCTION].
[80] *Ibid*.

l'épine dorsale de la cybersécurité et doit être mandaté ainsi que protégé par tous les moyens possibles[81].

50. Par conséquent, la partie 4 recommande :

a. **Recommandation 13 : Les pouvoirs de rendre des décrets devraient être modifiés pour s'assurer que les nouveaux pouvoirs ministériels ne sont pas utilisés pour compromettre la sécurité des réseaux du Canada.** Une clause interprétative devrait être ajoutée à l'article 15.2, afin de confirmer que, pour plus de certitude, le ministre n'est pas autorisé à prendre un décret qui compromettrait la confidentialité, la disponibilité ou l'intégrité d'une installation de télécommunication, d'un service de télécommunication ou d'une installation de transmission. L'objectif de cette recommandation est « d'empêcher le gouvernement d'ordonner ou d'exiger que les fournisseurs de services de télécommunication déploient ou autorisent des capacités ou des pouvoirs légaux liés à l'accès au service de « sécurisation de l'infrastructure par l'adoption d'une norme[82] ».

b. **Recommandation 14 : Le gouverneur en conseil et le ministre de l'Industrie devraient être tenus d'examiner les effets des décrets sur la protection des renseignements personnels et la sécurité des communications.** Selon les nouvelles modifications apportées lors des audiences du Comité permanent de la sécurité publique et nationale, le gouverneur en conseil ainsi que le ministre de l'Industrie sont maintenant tenus d'examiner une liste de facteurs avant de prendre des décrets en vertu de l'article 15.1 ou 15.2 (facteurs énumérés aux paragraphes 15.1[2.1] et 15.2[3.1]). Je recommande d'ajouter une clause à ces facteurs pour exiger que l'effet du décret sur la protection des renseignements personnels et la sécurité des communications soit pris en considération :

> **(a)** son incidence opérationnelle sur les fournisseurs de services de télécommunications touchés;
> **(b)** son incidence financière sur les fournisseurs de services de télécommunications touchés;
> **(c)** son effet sur la prestation de services de télécommunication au Canada;
> **(d)** **son effet sur la confidentialité et la sécurité des communications**;
>
> **(e)** tout autre facteur que le [gouverneur en conseil/ministre] juge pertinent.

Partie 5. Conclusion

51. J'exhorte le Comité à prendre au sérieux les recommandations formulées dans le rapport *Cybersecurity Will Not Thrive in Darkness,* en particulier les recommandations prioritaires qui sont développées dans ce mémoire. En détaillant ces recommandations aux fins de l'étude du Comité, j'exhorte également le Comité à tenir compte des intérêts supplémentaires découlant de la *Charte* qui sont visés par le projet de loi C-26, y compris la liberté d'expression et la protection de la vie privée, comme il est décrit à la partie 3 du présent mémoire. Je me fais l'écho de l'opinion de M. Parsons, selon lequel « les efforts déployés en matière de cybersécurité par le projet de loi C-26 devraient viser à établir la confiance entre le gouvernement et les entités

[81] Kate Robertson et Ron Deibert, « Ottawa wants the power to create secret backdoors in our networks to allow for surveillance », *The Globe and Mail*, 29 mai 2024.

[82] Christopher Parsons, « *Cybersecurity Will Not Thrive in Darkness: A Critical Analysis of Proposed Amendments in Bill C-26 to the Telecommunications Act* », rapport de recherche du Citizen Lab nº 158, Université de Toronto, octobre 2022, p. 17 [TRADUCTION].

non gouvernementales, y compris le grand public », et des organismes indépendants (dont le Comité des parlementaires sur la sécurité nationale et le renseignement et l'OSSNR) devraient être davantage intégrés aux pouvoirs de collecte et d'échange de renseignements énoncés dans le projet de loi C-26.

52. Le récent rapport du Citizen Lab, Finding You (ci-joint à l'annexe C), documente les vulnérabilités persistantes au coeur des réseaux de communications mobiles du monde. Les conclusions du rapport soulignent que la cybersécurité n'a pas prospéré dans l'obscurité. Les lacunes historiques et persistantes en matière de surveillance, de transparence et de responsabilisation pour la sécurité des réseaux ont entraîné de graves menaces liées à la géolocalisation associées aux réseaux contemporains. Le rapport souligne que « l'échec d'une réglementation, d'une responsabilisation et d'une transparence efficaces a été une bénédiction pour la surveillance de la géolocalisation par les réseaux[83] ».

53. Bien que le Canada doive aller de l'avant dans la lutte contre les menaces qui pèsent sur ses télécommunications et son infrastructure essentielle, il ne devrait pas légiférer par peur et au détriment des normes et des garanties démocratiques, de la transparence publique et de la responsabilité, le respect de la *Charte* et des droits de la personne. Une approche axée sur la sécurité et les droits de la personne en matière de cybersécurité exige plutôt la reconnaissance de l'importance de la cybersécurité accessible et inclusive, de la responsabilité publique et de la transparence publique dans la réglementation des télécommunications et de la cybersécurité.

Partie 6. Renseignements organisationnels

54. Je suis avocat et associé de recherche principal au Citizen Lab de la Munk School of Global Affairs & Public Policy, à l'Université de Toronto. Dans le cadre de mes recherches, j'explore l'intersection du droit, de la politique et de la technologie, et je me concentre sur les mécanismes de transparence ainsi que de responsabilisation pertinents aux relations entre les sociétés et les organismes publics en ce qui concerne les données personnelles et les autres activités de surveillance. Je m'appuie sur mon expérience antérieure en tant qu'assistante judiciaire de la Cour suprême du Canada et, par la suite, en tant qu'avocate dans le système de justice canadien.

55. Les points de vue présentés dans ce mémoire sont les miens et se basent sur des recherches que moi-même et mes collègues avons menées à notre lieu de travail, le Citizen Lab. Le Citizen Lab est un laboratoire interdisciplinaire établi à la Munk School of Global Affairs and Public Policy de l'Université de Toronto. Il met l'accent sur la recherche, le développement et les politiques stratégiques de haut niveau ainsi que l'engagement juridique au croisement des technologies de l'information et des communications, des droits de la personne et de la sécurité mondiale.

56. Nous utilisons une approche « mixte » pour la recherche combinant les pratiques des sciences politiques, du droit, de l'informatique et des études régionales. Nos recherches comprennent les enquêtes sur l'espionnage numérique contre la société civile; la documentation du filtrage d'Internet et d'autres technologies et pratiques qui ont une incidence sur la liberté d'expression en ligne; l'analyse des contrôles de protection de la vie privée, de la sécurité et de l'information des applications populaires; ainsi que l'examen des mécanismes de transparence et de responsabilisation pertinents pour la relation entre les entreprises et les organismes d'État concernant les données personnelles et d'autres activités de surveillance.

[83] *Finding You*, précité, p. 19 [TRADUCTION].

Annexe A – Tableau des recommandations

Recommendation 1: Les décrets de non-divulgation doivent être limités dans le temps	5
Recommendation 2: Les circonstances censées justifier la confidentialité dans un décret de non-divulgation devraient être définies dans la loi	6
Recommendation 3: L'article 15.9 devrait être modifié pour que le juge conserve le pouvoir d'établir un équilibre entre l'intérêt public à l'égard de la divulgation et l'intérêt à l'égard de la confidentialité	6
Recommendation 4: Lorsque des résumés des éléments de preuve et des renseignements reçus par le tribunal sont fournis, conformément à l'alinéa 15.9(1)C), ces résumés doivent également être accessibles au « demandeur et au public ».	6
Recommendation 5: Le seuil déclencheur justifiant les limites relatives à la transparence des procédures ne devrait pas être supérieur à celui qui est déjà contenu dans les dispositions analogues de la *Loi sur la preuve au Canada*	6
Recommendation 6: Une autorisation judiciaire préalable devrait être requise pour que le gouvernement obtienne des renseignements personnels ou anonymisés d'un fournisseur de services de télécommunication.	10
Recommendation 7 Les renseignements obtenus des fournisseurs de services de télécommunication ne doivent être utilisés que par les organismes gouvernementaux pour les activités de cybersécurité et d'assurance de l'information.	11
Recommendation 8: Des exigences de nécessité et de proportionnalité doivent servir à limiter la collecte ainsi que le partage d'information à caractère personnel.	11
Recommendations 9: Les périodes de conservation des données doivent être jointes aux données des fournisseurs de services de télécommunication et aux divulgations de renseignements à l'étranger.	12
Recommendation 10: Il faut obtenir le consentement de la personne à laquelle les renseignements se rapportent..	12
Recommendation 11: Des mesures de redressement devraient être offertes si le gouvernement traite mal des renseignements confidentiels	12
Recommendation 12: La loi devrait préciser les conditions dans lesquelles les renseignements d'une organisation privée peuvent être divulgués	12
Recommendation 13: Les pouvoirs de rendre des ordonnances devraient être modifiés pour que les nouveaux pouvoirs ministériels ne servent pas compromettre la sécurité des réseaux canadiens.	17
Recommendation 14: Il faudrait exiger que le gouverneur en conseil et le ministre de l'Industrie tiennent compte de l'effet des ordonnances sur la vie privée ainsi que sur la sécurité des communications.	17

Annexe B – Rapport en annexe

Christopher Parsons. « Cybersecurity Will Not Thrive in Darkness: A Critical Analysis of Proposed Amendments in Bill C-26 to the Telecommunications Act » [en anglais seulement], rapport de recherche du Citizen Lab no 158, Université de Toronto, 18 octobre 2022.

La cybersécurité ne prospérera pas dans l'obscurité

Une analyse critique des modifications proposées à la *Loi sur les télécommunications* dans le projet de loi C-26

Par Christopher Parsons

18 OCTOBRE 2022
RAPPORT DE RECHERCHE Nº 158

munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY

UNIVERSITY OF TORONTO

THECITIZENLAB

Droit d'auteur

Version électronique publiée pour la première fois par Citizen Lab en 2022. Ce rapport peut être consulté à l'adresse https://citizenlab.ca/2022/10/a-critical-analysis-of- pro-posed-amendments-in-bill-c-26-to-the-telecommunications-act.

Version du document : 1.0

À propos du Citizen Lab, Munk School of Global Affairs and Public Policy, Université de Toronto

Le Citizen Lab est un laboratoire interdisciplinaire établi à la Munk School of Global Affairs and Public Policy de l'Université de Toronto. Il met l'accent sur la recherche, le développement et les politiques stratégiques de haut niveau ainsi que l'engagement juridique au croisement des technologies de l'information et des communications, des droits de la personne et de la sécurité mondiale.

Nous utilisons une approche « mixte » pour la recherche, combinant les méthodes des sciences politiques, du droit, de l'informatique et des études régionales. Nos recherches comprennent les enquêtes sur l'espionnage numérique contre la société civile; la documentation du filtrage d'Internet et d'autres technologies et pratiques qui ont une incidence sur la liberté d'expression en ligne; l'analyse des contrôles de protection de la vie privée, de la sécurité et de l'information des applications populaires; ainsi que l'examen des mécanismes de transparence et de responsabilisation pertinents pour la relation entre les entreprises et les organismes d'État concernant les données personnelles et d'autres activités de surveillance.

À propos de l'auteur

Christopher Parsons est associé de recherche principal au Citizen Lab du Munk School of Global Affairs and Public Policy de l'Université de Toronto. Il a obtenu son baccalauréat et sa maîtrise à l'Université de Guelph et son doctorat à l'Université de Victoria.

Remerciements

Je tiens à exprimer ma gratitude aux personnes qui m'ont fait part de leurs réflexions, de leur expertise et de leur temps tout au long du processus de rédaction de ce rapport. Les experts internes et externes au gouvernement qui ont exprimé leurs réflexions sur la manière dont le projet de loi C-26 fonctionnerait dans la pratique ainsi que sur sa portée ont été d'une aide inestimable pour mieux comprendre la loi.

Je tiens à remercier tout particulièrement les personnes qui ont révisé les versions préliminaires de ce rapport, mais qui ne peuvent être nommées pour des raisons professionnelles. J'assume la responsabilité des erreurs qui pourraient rester dans le texte.

Je tiens également à remercier Mari Zhou pour son aide dans la conception et la mise en page du rapport. Les révisions ont été effectuées par Joyce Parsons de Stone Pillars Editing and Consulting.

Ce rapport a été réalisé sous la supervision du professeur Ronald Deibert.

Corrections et questions

Veuillez envoyer toutes vos questions et corrections à : chris@citizenlab.ca

---

Citation suggérée

PARSONS, Christopher. *La cybersécurité ne prospérera pas dans l'obscurité : Une analyse critique des modifications proposées à la* Loi sur les télécommunications *dans le projet de loi C-26,* rapport de recherche de Citizen Lab nº 158, Université de Toronto, 18 octobre 2022.

Table des matières

Résumé 1

Introduction 3

1. Contexte 6

2. Réformes proposées à la *Loi sur les télécommunications* 10

2.1. Contraindre ou ordonner des modifications des activités techniques ou commerciales des organisations 10

Recommandation 1 : Les décrets et les arrêtés ministériels doivent être pertinents, proportionnés et raisonnables 13

Recommandation 2 : Les décrets et arrêtés doivent contenir une référence aux délais 15

Recommandation 3 : Le gouvernement devrait procéder à des évaluations des impacts avant l'émission de décrets et d'arrêtés 16

Recommandation 4 : Les dispositions d'abstention ou de réduction des coûts devraient être incluses 16

Recommandation 5 : Les normes imposables doivent être définies 18

2.2. Le secret et l'absence de dispositions en matière de transparence ou de responsabilité 18

Recommandation 6 : Les décrets et arrêtés devraient paraître dans la *Gazette du Canada* 20

Recommandation 7 : Le ministre devrait être contraint de présenter des rapports relatifs aux décrets, arrêtés et règlements 20

Recommandation 8 : Les consignes du silence devraient être limitées dans le temps 21

Recommandation 9 : Le CRTC devrait indiquer quand les décrets et arrêtés annulent des parties de ses décisions 22

Recommandation 10 : Le rapport annuel devrait indiquer le nombre de fois où les décrets, arrêtés ou règlements gouvernementaux ont prévalu sur les décisions du CRTC 22

Recommandation 11 : Tous les règlements en vertu de la *Loi sur les télécommunications* doivent être accessibles au Comité mixte permanent d'examen de la réglementation 23

2.3. Une procédure de contrôle judiciaire déficiente 23

Recommandation 12 : Le contrôle judiciaire devrait explicitement permettre la désignation d'un intervenant désintéressé 27

2.4. Échange intensif de renseignements au sein des agences canadiennes et au-delà 27

Recommandation 13 : Des indemnisations devraient être prévues si le gouvernement ne gère pas correctement les renseignements confidentiels 30

Recommandation 14 : Des indemnisations devraient être prévues si le gouvernement ne gère pas correctement les renseignements personnels ou dépersonnalisés 30

Recommandation 15 : Le gouvernement devrait expliquer comment il

utilisera les renseignements et révéler les agences nationales auxquelles les renseignements sont divulgués 31

Recommandation 16 : Les renseignements obtenus auprès des fournisseurs de services de télécommunication ne doivent être utilisés que pour des activités de cybersécurité et d'assurance des renseignements 31

Recommandation 17 : Des périodes de conservation des données devraient être imposées aux données des fournisseurs de services de télécommunication 32

Recommandation 18 : Des périodes de conservation des données devraient être imposées aux divulgations de renseignements à l'étranger 32

Recommandation 19 : Les fournisseurs de services de télécommunication devraient être informés des parties étrangères qui reçoivent leurs renseignements 33

Recommandation 20 : La loi devrait délimiter les conditions dans lesquelles les renseignements d'un organisme privé peuvent être divulgués 34

2.5. Coûts liés à la conformité en matière de sécurité 34

Recommandation 21 : Une indemnisation devrait être incluse pour les petites organisations 35

Recommandation 22 : Les évaluations de la proportionnalité et de l'équité devraient être incluses dans les décrets, arrêtés et règlements 36

Recommandation 23 : Le gouvernement devrait encourager la formation à la cybersécurité 37

2.6. Formulation vague du projet de loi 37

Recommandation 24 : Tout le contenu de la loi doit être clair 39

Recommandation 25 : Des définitions claires devraient être présentes dans la loi ou rendues publiques 39

Recommandation 26 : La flexibilité ministérielle doit être limitée 40

Recommandation 27 : Situations d'urgence 40

Recommandation 28 : Les renseignements personnels sont des renseignements confidentiels 41

Recommandation 29 : Autorisation judiciaire préalable pour l'obtention de renseignements personnels ou dépersonnalisés 42

Recommandation 30 : Interdire la divulgation de renseignements personnels ou dépersonnalisés à des organismes étrangers 42

3. Contrepoids à la sécurité 43

4. Conclusion 46

Tableau des acronymes

3GPP	3rd Generation Partnership Project
CALEA	Communications Assistance for Law Enforcement Act (Loi sur l'aide des services de communications à l'application de la loi)
CCC	Centre canadien pour la cybersécurité
ACEI	Autorité canadienne pour les enregistrements Internet
CRTC	Conseil de la radiodiffusion et des télécommunications canadiennes
CST	Centre de la sécurité des télécommunications
CCCST	Comité consultatif canadien pour la sécurité des télécommunications
ETSI	European Telecommunications Standards Institute
PeES	Programme évolué d'examen de la sécurité
GSMA	Système mondial de communication avec les mobiles
HBS	Capteurs au niveau de l'hôte
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
TI	Technologies de l'information
NCSC	National Cyber Security Centre
CPSNR	Comité des parlementaires sur la sécurité nationale et le renseignement
NASG	Normes d'application du Solliciteur général
FST	Fournisseur de services de télécommunication

Tableau des recommandations

Recommandation 1 : Les décrets et les arrêtés ministériels doivent être pertinents, proportionnés et raisonnables	p. 13
Recommandation 2 : Les décrets et arrêtés doivent contenir une référence aux délais	p. 15
Recommandation 3 : Le gouvernement devrait procéder à des évaluations des impacts avant l'émission de décrets et d'arrêtés	p. 16
Recommandation 4 : Les dispositions d'abstention ou de réduction des coûts devraient être incluses	p. 16
Recommandation 5 : Les normes imposables doivent être définies	p. 18
Recommandation 6 : Les décrets et arrêtés devraient paraître dans la *Gazette du Canada*	p. 20
Recommandation 7 : Le ministre devrait être contraint de présenter des rapports relatifs aux décrets, arrêtés et règlements	p. 20
Recommandation 8 : Les consignes du silence devraient être limitées dans le temps	p. 21
Recommandation 9 : Le CRTC devrait indiquer quand les décrets et arrêtés annulent des parties de ses décisions	p. 22
Recommandation 10 : Le rapport annuel devrait indiquer le nombre de fois où les décrets, arrêtés ou règlements gouvernementaux ont prévalu sur les décisions du CRTC	p. 22
Recommandation 11 : Tous les règlements en vertu de la *Loi sur les télécommunications* doivent être accessibles au Comité mixte permanent d'examen de la réglementation	p. 23
Recommandation 12 : Le contrôle judiciaire devrait explicitement permettre la désignation d'un intervenant désintéressé	p. 27
Recommandation 13 : Des indemnisations devraient être prévues si le gouvernement ne gère pas correctement les renseignements confidentiels	p. 30
Recommandation 14 : Des indemnisations devraient être prévues si le gouvernement ne gère pas correctement les renseignements personnels ou dépersonnalisés	p. 30
Recommandation 15 : Le gouvernement devrait expliquer comment il utilisera les renseignements et révéler les agences nationales auxquelles les renseignements sont divulgués	p. 31
Recommandation 16 : Les renseignements obtenus auprès des fournisseurs de services de télécommunication ne doivent être utilisés que pour des activités de cybersécurité et d'assurance des renseignements	p. 31
Recommandation 17 : Des périodes de conservation des données devraient être imposées aux données des fournisseurs de services de télécommunication	p. 32
Recommandation 18 : Des périodes de conservation des données devraient être imposées aux divulgations de renseignements à l'étranger	p. 32
Recommandation 19 : Les fournisseurs de services de télécommunication devraient être informés des parties étrangères qui reçoivent leurs renseignements	p. 33
Recommandation 20 : La loi devrait délimiter les conditions dans lesquelles les renseignements d'un organisme privé peuvent être divulgués	p. 34
Recommandation 21 : Une indemnisation devrait être incluse pour les petites organisations	p. 35

Recommandation 22 : Les évaluations de la proportionnalité et de l'équité devraient être incluses dans les décrets, arrêtés ou règlements	p. 36
Recommandation 23 : Le gouvernement devrait encourager la formation à la cybersécurité	p. 37
Recommandation 24 : Tout le contenu de la loi doit être clair	p. 39
Recommandation 25 : Des définitions claires devraient être présentes dans la loi ou rendues publiques	p. 39
Recommandation 26 : La flexibilité ministérielle doit être limitée	p. 40
Recommandation 27 : Situations d'urgence	p. 40
Recommandation 28 : Les renseignements personnels sont des renseignements confidentiels	p.41
Recommandation 29 : Autorisation judiciaire préalable pour l'obtention de renseignements personnels ou dépersonnalisés	p. 42
Recommandation 30 : Interdire la divulgation de renseignements personnels ou dépersonnalisés à des organismes étrangers	p. 42

Sommaire

Le 14 juin 2022, le gouvernement du Canada a présenté le « projet de loi C-26 : Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois ». S'il est adopté, le projet de loi réformera en profondeur la *Loi sur les télécommunications* et imposera de nouvelles exigences aux fournisseurs d'infrastructures essentielles réglementés par le gouvernement fédéral. Ce rapport, *La cybersécurité ne prospérera pas dans l'obscurité : Une analyse critique des modifications proposées à la* Loi sur les télécommunications *dans le projet de loi C-26*, propose 30 recommandations au projet de loi afin de corriger ses lacunes en matière de secret et de responsabilité, tout en suggérant des modifications qui imposeraient certaines restrictions à l'éventail des pouvoirs que le gouvernement serait en mesure d'exercer. Ces modifications doivent être sérieusement prises en compte en raison du caractère radical de la loi.

Dans sa version actuelle, le projet de loi C-26 permettrait au ministre de l'Innovation, des Sciences et de l'Industrie d'obliger les fournisseurs de services de télécommunication à faire ou à s'abstenir de faire quoi que ce soit pour protéger les réseaux de télécommunication canadiens contre les menaces d'ingérence, de manipulation ou de perturbation. La loi autoriserait le ministre à obliger les fournisseurs à divulguer des renseignements confidentiels, y compris des renseignements personnels identifiables ou dépersonnalisés, puis habiliterait le ministre à diffuser ces renseignements à grande échelle au sein du gouvernement fédéral. De plus, le ministre pourrait transmettre à l'étranger des renseignements non confidentiels même lorsque cela risque d'entraîner des processus d'application de la réglementation ou des droits d'action privés contre un particulier ou un organisme. Si le ministre ou une autre partie à qui celui-ci a communiqué des renseignements perd involontairement le contrôle sur les renseignements, le gouvernement serait dégagé de toute responsabilité pour l'incident.

Lorsque des décrets, arrêtés ou règlements sont émis, ils n'auraient pas à être publiés dans la *Gazette du Canada*, et des consignes du silence pourraient être imposées aux destinataires de ces décrets et arrêtés. Il peut même arriver que le gouvernement émette un décret, arrêté ou règlement, avec l'interdiction de publication et la consigne du silence susmentionnées, qui aille à l'encontre d'une décision du Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) et qui annule certains aspects de cette décision. Dans tous les cas où un fournisseur de services de télécommunication demande un contrôle judiciaire, il se peut qu'il ne voie jamais les preuves utilisées pour justifier un décret, arrêté ou règlement. Toutefois, s'il s'avère qu'un fournisseur de services de télécommunication a délibérément ignoré ou n'a pas

respecté un décret ou arrêté, les personnes qui ont dirigé l'action ou le fournisseur de services de télécommunication peuvent se voir infliger des sanctions administratives pécuniaires.

En résumé, ce rapport nomme et analyse une série de lacunes dans le projet de loi C- 26 tel qu'il est actuellement rédigé :

- L'étendue de ce que le gouvernement pourrait ordonner à un fournisseur de services de télécommunication n'est pas suffisamment délimitée.
- Les dispositions relatives au secret et à la confidentialité excessives que l'on imposerait aux fournisseurs de services de télécommunication menacent de créer une catégorie de lois et de règlements secrets.
- Il existe un risque important d'échange de renseignements excessif au sein du gouvernement fédéral, ainsi qu'avec des partenaires internationaux.
- Les coûts associés à l'observation des mesures amenées par les réformes pourraient menacer la viabilité des petits fournisseurs.
- La formulation vague du projet de loi ne permet pas d'en évaluer pleinement les limites.
- Il n'y a aucune reconnaissance du droit à la vie privée ou d'autres droits protégés par la Charte pour faire contrepoids aux exigences de sécurité proposées, et aucune exigence appropriée de transparence ou de responsabilité n'est imposée au gouvernement.

Même si l'on suppose que le gouvernement a besoin de pouvoir encourager ou obliger les fournisseurs de services de télécommunication à modifier leurs opérations techniques ou commerciales pour améliorer la sécurité de leurs services et installations, il est évident qu'il faut exiger plus de transparence et de responsabilité de la part du gouvernement. Toutes les recommandations de ce rapport visent à résoudre certains des problèmes existants dans la loi.

Si ces recommandations ou celles qui en découlent ne sont pas prises en compte, le gouvernement créera une loi de la pire espèce dans la mesure où elle exigera du public et des fournisseurs de services de télécommunication qu'ils se contentent de croire que le gouvernement sait ce qu'il fait, qu'il prend les bonnes décisions et qu'il n'est pas nécessaire d'organiser un débat public plus large sur les types de protections à mettre en place pour protéger la cybersécurité des réseaux de télécommunication du Canada. La cybersécurité ne peut pas se développer sur la base de décrets gouvernementaux secrets et obscurs. Le gouvernement doit modifier sa loi pour s'assurer que ses activités sont conformes aux valeurs démocratiques du Canada et aux normes de transparence et de responsabilité.

Introduction

Ces deux dernières années ont montré que les fournisseurs d'infrastructures essentielles sont constamment menacés et que les acteurs de la menace sont disposés à cibler les infrastructures en Amérique du Nord et s'y intéressent[1]. Dans le même temps, les gouvernements occidentaux se sont largement inquiétés du fait que les fournisseurs établis en Chine pourraient être contraints par le gouvernement chinois de modifier leurs produits, ce qui aurait pour effet de compromettre l'intégrité des infrastructures essentielles dans les pays occidentaux[2]. En bref, les menaces pesant sur les infrastructures essentielles sont réelles et pressantes, et les gouvernements occidentaux ont généralement cherché à déterminer comment ils pouvaient renforcer les infrastructures contre les faiblesses perçues et réelles.

Le 19 mai 2022, le ministre de la Sécurité publique et le ministre de l'Innovation, des Sciences et du Développement économique ont tenu une conférence de presse au cours de laquelle ils ont annoncé que les fournisseurs de services de télécommunication canadiens seraient tenus de retirer les équipements Huawei et ZTE de leurs infrastructures[3]. Le gouvernement a également présenté un énoncé de politique qui précisait ce qu'il prévoyait précisément d'exiger des fournisseurs de services de télécommunication[4]. La loi susceptible de donner effet à l'énoncé de politique a été déposée le 14 juin 2022. La loi, le projet de loi C-26 : Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois, réformerait en profondeur la *Loi sur les télécommunications* et imposerait de nouvelles exigences à d'autres fournisseurs d'infrastructures essentielles[5].

---

[1] Voir : Centre canadien pour la cybersécurité. (2020). « Évaluation des cybermenaces nationales 2020 », gouvernement du Canada. Accessible à : https://www.cyber.gc.ca/fr/orientation/evaluation-des-cybermenaces-nationales-2020; Centre canadien pour la cybersécurité. (2022). « Bulletin sur les cybermenaces : Les activités de cybermenace liées à l'invasion de l'Ukraine par la Russie ». Accessible à : https://www.cyber.gc.ca/fr/orientation/bulletin-cybermenaces-activites-cybermenace-liees-invasion-Ukraine-Russie; Agence de cybersécurité et de sécurité des infrastructures. « Shields Up », gouvernement des États-Unis. Accessible à : https://www.cisa.gov/shields-up; Maison-Blanche. (2021). « Executive Order 14028: Improving the Nation's Cybersecurity », Maison-Blanche. Accessible à : https://www.whitehouse.gov/briefing- room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[2] Voir : « Security Stances Adopted by Canada's Allies » dans « The Policy and Political Implications of "Securing Canada's Telecommunications Systems" », accessible à : https://christopher-parsons. com/2022/06/08/les-implications-politiques-et-politiques-de-la-sécurisation-des- systèmes-de-télécommunications-des-canadastélécommunications/.

[3] CPAC. (2022). « Ottawa announces move to ban Huawei and ZTE equipment from Canada's 5G networks », *YouTube*. Accessible à : https://www.youtube.com/watch?v=6odAKonqzIc.

[4] Ministère de l'Innovation, Sciences et Développement économique Canada (ISDE). (2022). « Énoncé de politique - Sécuriser le système de télécommunications au Canada », gouvernement du Canada. Accessible à : https://www.canada.ca/fr/innovation-sciences-developpement- economique/nouvelles/2022/05/enonce-de-politique--securiser-le-systeme-de-telecommunications-au-canada.html.

[5] Parlement du Canada. (2022). « Projet de loi C-26 : Loi concernant la cybersécurité, modifiant la *Loi sur les télécommunications* et apportant des modifications corrélatives à d'autres lois », Parlement du Canada. Accessible à : https://www.parl.ca/DocumentViewer/fr/44-

De manière générale, les réformes proposées donneraient au gouvernement de nouveaux pouvoirs pour obliger les fournisseurs de services de télécommunication et les fournisseurs d'infrastructures essentielles à modifier leurs pratiques techniques et organisationnelles afin de renforcer la sécurité des opérations de ces organisations conformément aux exigences du gouvernement. La loi suit les traces des alliés du Canada qui ont reconnu les menaces pesant sur les fournisseurs d'infrastructures essentielles et ont cherché à atténuer les dangers en permettant aux agences gouvernementales d'imposer des changements aux pratiques des fournisseurs par l'intermédiaire de lois et de décrets-lois[6].

Ce rapport évalue de manière critique les réformes proposées pour la *Loi sur les télécommunications* du Canada. Ce faisant, il nomme une série de lacunes dans la loi, telle qu'elle est actuellement rédigée :

- L'étendue de ce que le gouvernement pourrait ordonner à un fournisseur de services de télécommunication n'est pas suffisamment délimitée.
- Les dispositions relatives au secret et à la confidentialité excessives que l'on imposerait aux fournisseurs de services de télécommunication menacent de créer une catégorie de lois et de règlements secrets.
- Il existe un risque important d'échange de renseignements excessif au sein du gouvernement fédéral, ainsi qu'avec des partenaires internationaux.
- Les coûts associés à l'observation des mesures amenées par les réformes pourraient menacer la viabilité des petits fournisseurs.
- La formulation vague du projet de loi ne permet pas d'en évaluer pleinement les limites.
- Il n'y a aucune reconnaissance du droit à la vie privée ou d'autres droits protégés par la Charte pour faire contrepoids aux exigences de sécurité proposées, et aucune exigence appropriée de transparence ou de responsabilité n'est imposée au gouvernement.

Dans de nombreux cas, ces lacunes peuvent être comblées par des modifications législatives, et le présent rapport propose des suggestions à cet effet dans son analyse du projet de loi. Cependant, ni l'énoncé de politique « Sécuriser le système de télécommunications au Canada » ni les commentaires qui accompagnent le projet de

1/projet-loi/C-26/premiere-lecture.

[6] Voir, par exemple : Maison-Blanche. (2021). « Executive Order 14028: Improving the Nation's Cybersecurity », Maison-Blanche. Accessible à : https://www.whitehouse.gov/briefing-room/presidential- actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/; ou Department of Home Affairs. (2022). « Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 », gouvernement de l'Australie. Accessible à : https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/slacip-bill-2022.

loi C-26 ne font état de la nécessité empirique de sécuriser les systèmes de télécommunication du Canada à l'aide des mécanismes législatifs proposés. Contrairement à ses homologues et à ses alliés, le gouvernement canadien n'a pas publiquement rassemblé de preuves indiquant que les réseaux de télécommunication essentiels du Canada ne sont pas sécurisés, et il n'a pas non plus publié de document stratégique général indiquant comment le projet de loi C-26 s'inscrit dans le cadre d'un effort plus large visant à sécuriser les infrastructures essentielles du Canada. Comme le constate le rapport, en plus de modifications législatives précises, le gouvernement du Canada devrait expliquer clairement et publiquement les risques qui le préoccupent et la mesure dans laquelle la loi proposée est tournée vers le passé pour résoudre des problèmes existants ou historiques, par rapport à la mesure dans laquelle elle est tournée vers l'avenir et destinée à relever des défis futurs ou à permettre des activités avec des nations étroitement alliées.

1. Contexte

Depuis des décennies, les agences gouvernementales canadiennes s'inquiètent des propriétés de sécurité des réseaux de télécommunication du Canada. Les documents qui ont été publiés à la suite de demandes d'accès à l'information montrent que même en 2012, par exemple, le Centre de la sécurité des télécommunications (CST) préparait des présentations sur les menaces pesant sur la chaîne d'approvisionnement des réseaux de télécommunication canadiens. Le CST l'a reconnu :

> Il n'y a aucun moyen d'empêcher l'introduction de technologies étrangères au Canada. Nous devons trouver un juste équilibre entre les exigences en matière de sécurité informatique, l'environnement des menaces et des risques et la nécessité de traiter efficacement les informations et de fournir des services aux Canadiens tout en permettant à l'industrie de rester compétitive[7].

Pour tenter de trouver un juste équilibre, le gouvernement canadien a interdit à Huawei de soumissionner pour le réseau de télécommunication et de messagerie du gouvernement en 2012[8]. En outre, les équipements étrangers, tels que ceux vendus par Huawei, ont été évalués par EWA-Canada dans le cadre du programme Critères communs. Le gouvernement a également évalué les équipements Huawei dans le cadre du Programme d'examen de la sécurité du Centre de la sécurité des télécommunications[9] et a présenté les grandes lignes d'un programme évolué en juin 2022[10].

Le gouvernement n'a pas considéré que les menaces pesant sur l'infrastructure de télécommunication du Canada provenaient uniquement des équipements de

[7] Centre de la sécurité des télécommunications du Canada. (2012). « Supply Chain Threats to Canada », accessible à : https://christopherparsonscom.files.wordpress.com/2022/07/a-2012-00397.pdf, p. 6.
[8] Steven Chase. (2012). « Ottawa set to ban Chinese firm from telecommunications bid », *The Globe & Mail*. Accessible à : https://www.theglobeandmail.com/news/politics/ottawa-set-to-ban-chinese-firm-de-telecommunications-bid/article4600199/.
[9] Centre canadien pour la cybersécurité. (2019). « Programme d'examen de la sécurité du CST visant les technologies 3G, 4G et LTE », gouvernement du Canada. Accessible à : https://www.cyber.gc.ca/fr/nouvelles-evenements/programme-dexamen-de-la-securite-du-cst-visant- les-technologies-3g-4g-et-lte.
[10] Le gouvernement du Canada a annoncé un Programme « évolué » d'examen de la sécurité (PeES) en juin 2022, dont les détails sont accessibles à : Centre canadien pour la cybersécurité. (2022). « Programme évolué d'examen de la sécurité du CST », gouvernement du Canada. Accessible à : https://www.cyber.gc.ca/fr/nouvelles-evenements/programme-evolue-dexamen-de-la-securite-du-cst.
Le programme évolué « fera appel à tous les fournisseurs clés sur le marché canadien pour établir de nouveaux partenariats afin de bâtir la confiance dans les produits et services déployés dans les infrastructures de télécommunications du Canada » et poursuivra des « examens annuels de l'architecture pour cerner les lacunes en matière de sécurité et collaborer avec les fournisseurs de services de télécommunications afin d'améliorer la sécurité globale du secteur des télécommunications ». Le PeES « élargira les évaluations pour tenir compte du déploiement de produits de fournisseurs clés, en mettant l'accent sur les composants les plus importants et sensibles de l'infrastructure de télécommunications. L'évaluation du déploiement permet de cerner les risques et de recommander des mesures d'atténuation pour assurer la résilience du réseau ou du service »; il se concentre également sur la cyber-résilience, émet des recommandations en matière de sécurité des télécommunications et s'engage à « continu[er] de travailler avec des partenaires à l'échelle mondiale afin de promouvoir l'adoption de normes internationales qui permettront de renforcer la base de référence commune en matière de cybersécurité et d'accroître la confiance dans les systèmes de télécommunications partout dans le monde ».

télécommunication Huawei ou ZTE configurés de manière potentiellement malveillante. Dans son évaluation de la menace pour 2020, le Centre canadien pour la cybersécurité a reconnu que les fournisseurs d'infrastructures essentielles intéressaient les acteurs de la menace et que, par conséquent, le Centre comptait communiquer avec ces fournisseurs[11]. Dans son rapport annuel de 2021-2022, le CST a indiqué que le Centre canadien pour la cybersécurité avait reçu des informations de la part de fournisseurs d'infrastructures essentielles, comme les secteurs de l'énergie et du gaz, afin de mieux comprendre le paysage des menaces[12].

De manière générale, le CST, en collaboration avec Services partagés Canada et le Secrétariat du Conseil du Trésor, est responsable des principaux aspects de la défense des systèmes du gouvernement fédéral. En vertu de la loi qui l'autorise, le CST peut également fournir des avis, des conseils ou des services pour aider à protéger l'information électronique et les infrastructures de l'information désignées comme étant « d'importance » par le gouvernement du Canada[13]. Comme l'indique un rapport publié en 2022 par le Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR), une organisation non spécialisée dans les télécommunications a été la première à recevoir l'aide du CST en vertu de la *Loi sur le Centre de la sécurité des télécommunications* pour mettre fin à une opération cybernétique qui la visait. Comme l'ont noté les responsables du CST dans le rapport du CPSNR :

> Ce type de déploiement n'était pas prévu au moment où la loi a été rédigée; le pouvoir avait plutôt pour objet de donner lieu à une collaboration proactive à long terme avec les organisations non fédérales, particulièrement les entreprises de télécommunications[14].

Le même rapport décrit comment les systèmes de capteurs défensifs du CST, comprenant des capteurs au niveau de l'hôte, du réseau et du nuage, peuvent être utilisés pour atténuer les menaces pesant sur les organisations qui les ont adoptés[15]. Des documents historiques inclus dans les révélations d'Edward Snowden suggèrent

---

[11] Centre canadien pour la cybersécurité. (2020). « Évaluation des cybermenaces nationales 2020 », gouvernement du Canada. Accessible à : https://www.cyber.gc.ca/fr/orientation/evaluation-des-cybermenaces-nationales-2020.
[12] Centre de la sécurité des télécommunications. (2022). « Rapport annuel du Centre de la sécurité des télécommunications 2021-2022 », gouvernement du Canada. Accessible à : https://www.cse-cst.gc.ca/fr/reddition-de-comptes/transparence/rapports/rapport-annuel-du-cst- 2021-2022.
[13] *Loi sur le CST*, alinéa 17(a)ii).
[14] Comité des parlementaires sur la sécurité nationale et le renseignement. (2022). « Rapport spécial sur le cadre et les activités du gouvernement pour défendre ses systèmes et ses réseaux contre les cyberattaques », gouvernement du Canada. Accessible à : https://www.nsicop- cpsnr.ca/reports/rp-2022-02-14/2022-cyber-attack-framework-report-fr.pdf, p. 81, sans mise en gras dans l'original.
[15] Pour une analyse de ces capteurs, voir soit « Rapport spécial sur le cadre et les activités du gouvernement pour défendre ses systèmes et ses réseaux contre les cyberattaques » de 2022 du CPSNR, gouvernement du Canada. Accessible à : https://www.nsicop-cpsnr.ca/reports/rp-2022- 02-14/2022-cyber-attack-framework-report-fr.pdf, soit l'analyse de ce même rapport, intitulée « Unpacking NSICOP's Special Report on the Government of Canada's Framework and Activities to Defend its Systems and Networks from Cyber Attack », accessible à : https://christopher- parsons.com/2022/03/30/unpacking-nsicops-special-report-on-the-government-of-canadas-framework-and-activities-to-defend-its-systems- and-networks-from-cyber-attack/.

que le CST avait l'intention de placer ses capteurs sur au moins certains réseaux de télécommunication nationaux[16].

D'autres organismes gouvernementaux, outre le CST, ont également reconnu les risques et les menaces qui pèsent sur l'infrastructure canadienne des télécommunications, ou qui passent par celle-ci. Le CRTC, par exemple, a publié la *Décision de Conformité et Enquêtes et de Télécom CRTC 2022-170*. Cette décision détaille les risques que posent les réseaux zombies en ligne[17]. Le Conseil a estimé que « des mesures réglementaires sont nécessaires afin de faire en sorte que les entreprises canadiennes qui bloquent les réseaux zombies le fassent d'une manière qui assure un niveau de protection de base aux Canadiens ». Une action est nécessaire, car selon le CRTC, « le trafic des réseaux zombies constitue un problème important en matière de cybersécurité, tant en termes de volume que de gravité des préjudices ». Dans les prochains mois, le CRTC devrait publier un rapport nommant la ou les parties, y compris éventuellement le Centre canadien pour la cybersécurité (CCCS) ou l'Autorité canadienne pour les enregistrements Internet (ACEI), qui pourrait servir d'autorité centrale d'un cadre de blocage. Les menaces posées par les zombies ont également été évoquées dans le rapport de 2022 du Comité permanent de la sécurité publique et nationale, intitulé *La montée de l'extrémisme violent à caractère idéologique au Canada*. Plus précisément, ce rapport invite le gouvernement à « investi[r] dans le développement d'une cyberinfrastructure pour le pays, notamment pour détecter et supprimer les robots automatisés utilisés pour amplifier les contenus extrémistes en ligne auxquels les Canadiens peuvent accéder » (recommandation 33)[18]. Dans l'ensemble, le CST pourrait se voir confier un rôle d'assistance ou d'orientation des fournisseurs de services de télécommunication afin d'atténuer les menaces posées par les robots automatisés.

---

[16] PARSONS, Christopher. « CASCADE: Joint Cyber Sensor Architecture », *Technology, Thoughts, and Trinkets*. Accessible à : https://christopher- parsons.com/resources/cse-summaries/#cse-cascade-joint.

Il convient de noter que certains alliés du Canada, dont le National Cyber Security Centre (NCSC) du Royaume-Uni, utilisent certains des capteurs du CST. Voir : HEAD, Richard E. (2020). « Introducing Host Based Capability (HBC) », gouvernement du Royaume-Uni. Accessible à : https://www.ncsc.gov.uk/blog-post/introducing-host-based-capability-hbc. Comme le dit Head : « Heureusement, nos amis du Centre canadien pour la cybersécurité nous ont permis d'utiliser la technologie de pointe des capteurs au niveau de l'hôte (HBS) qu'ils ont mise au point pour défendre le gouvernement du Canada. Cela nous a permis d'être opérationnels beaucoup plus rapidement.

> Le NCSC collabore désormais activement avec son homologue canadien dans toute une série de domaines, y compris le codéveloppement de la technologie de capacité au niveau de l'hôte sous-jacente en soi, mais aussi l'analyse et la meilleure utilisation des données pour défendre nos gouvernements respectifs contre les cyberattaques.
>
> [...]
>
> Nous aimerions profiter de cette occasion pour remercier le Centre canadien pour la cybersécurité pour toute l'aide et le soutien qu'il nous a apportés et qui nous ont permis d'en arriver là. Le NCSC n'aurait pas été en mesure de relever ce défi seul. »

[17] Conseil de la radiodiffusion et des télécommunications canadiennes. (2022). « Décision de Conformité et Enquêtes et de Télécom CRTC 2022- 170 », gouvernement du Canada. Accessible à : https:// crtc.gc.ca/fra/archive/2022/2022-170.htm.
[18] Comité permanent de la sécurité publique et nationale. (2022). « La montée de l'extrémisme violent à caractère idéologique au Canada », Parlement du Canada. Accessible à : https://www.noscommunes.ca/documentviewer/fr/44-1/SECU/rapport-6.

Enfin, les autorités chargées de l'application de la loi peuvent s'appuyer sur les autorisations d'interception électronique pour lutter contre les criminels qui ciblent ou utilisent les télécommunications canadiennes. Cette activité peut comprendre la délivrance d'un mandat aux fournisseurs de services de télécommunication afin d'identifier les personnes impliquées dans des infractions criminelles, et de voir ces personnes inculpées par les organismes d'application de la loi par la suite. Ces infractions peuvent être associées à la compromission de services et de systèmes de télécommunication essentiels ou à l'utilisation de services ou de systèmes de télécommunication pour mener d'autres activités criminelles cybernétiques. La Gendarmerie royale du Canada (GRC), par exemple, recueille des données sur les télécommunications électroniques pour cibler, implanter et maintenir des logiciels malveillants (appelés « outils d'enquête sur appareil ») sur les appareils des suspects19. Toutefois, alors que les Normes d'application du Solliciteur général (NASG) exigent que les fournisseurs de services de télécommunication offrant des services mobiles sans fil possèdent une capacité d'interception légale, qui est utilisée en association avec les logiciels malveillants de la GRC, il n'en va pas de même pour les fournisseurs de services de télécommunication filaires20. Il en résulte qu'au moins certains fournisseurs peuvent ne pas posséder les capacités d'interception filaire dont les services d'application de la loi et de sécurité ont besoin pour mener à bien leurs enquêtes criminelles ou leurs enquêtes de sécurité nationale, y compris celles relatives aux menaces pesant sur les infrastructures essentielles.

[19] Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique. (2022). « Outils d'enquête sur appareil utilisés par la Gendarmerie royale du Canada (GRC) », Parlement du Canada. Accessible à : https://

www.noscommunes.ca/Committees/fr/ETHI/StudyActivity?studyActivityId=11794265. Pour les documents détaillant le fonctionnement technique des outils d'enquête sur appareil, ou les mandats ou politiques associés, voir « RCMP On-Device Investigative Tools » à l'adresse : https://christopher-parsons.com/resources/miscellaneous/.

[20] Voir : « Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications », accessible à : https://christopherparsonscom.files.wordpress.com/2022/07/a-2020-00246-sges.pdf, ainsi que Christopher Parsons et Tamir Israel. (2015).
« Canada's Quiet History Of Weakening Communications Encryption », *Citizen Lab*. Accessible à : https://citizenlab.ca/2015/08/canadas-quiet- history-of-weakening-communications-encryption/.

2. Réformes proposées à la *Loi sur les télécommunications*

Cette section du rapport examine les différentes parties du projet de loi. Elle détermine ce qui est possible ou nécessaire en vertu de la loi et, ensuite, évalue les conséquences possibles de la formulation actuelle. Dans la mesure du possible, le rapport formule des recommandations précises visant à améliorer le projet actuel.

2.1. Contraindre ou ordonner des modifications des activités techniques ou commerciales des organisations

En vertu de l'article 15.1, le gouvernement peut, par l'intermédiaire d'un décret, obliger un fournisseur de services de télécommunication à interdire l'utilisation de certains services ou produits [alinéa 15.1(1)a)] ou à ordonner la suppression de certains produits ou services [alinéa 15.1(1)b)] afin de protéger les systèmes de télécommunication contre les ingérences, les manipulations, les perturbations ou d'autres menaces (non définies) [paragraphe 15.1(1)]. En vertu du paragraphe 15.2(1), le ministre de l'Industrie, des Sciences et de la Technologie peut présenter un arrêté interdisant [alinéa 15.2(1)a)] à un fournisseur de services de télécommunication de fournir un service ou lui ordonnant [alinéa 15.2(1)b)] de suspendre la fourniture de ce service à une personne déterminée, y compris à un fournisseur de services de télécommunication. Notamment, le ministre peut « par arrêté, ordonner aux fournisseurs de services de télécommunication de faire ou de s'abstenir de faire toute chose […] qu'il estime nécessaire pour sécuriser le système canadien de télécommunication, notamment face aux menaces d'ingérence, de manipulation ou de perturbation » [paragraphe 15.2(2), sans mise en gras dans l'original].

Les arrêtés auraient une grande portée et incluraient les éléments suivants, « entre autres » [paragraphe 15.2(2)] :

Formulation législative du paragraphe 15.2(2)	Langage clair
a) interdire aux fournisseurs de services de télécommunication d'utiliser dans tout ou partiede leurs réseaux ou installations de télécommunication, ou en lien avec ceux-ci, les produits ou les services qu'il précise;	Un fournisseur de services de télécommunication ne peut pas utiliser X.
(b) leur ordonner de retirer de tout ou partie de leurs réseaux ou installations de télécommunication les produits qu'il précise;	Un fournisseur de services de télécommunication doit retirer X.
(c) leur imposer des conditions quant à leur utilisation de produits ou de services, notamment ceux fournis par toute personne qu'il précise, notamment un fournisseur de services de télécommunication;	Si un fournisseur de services de télécommunication utilise X, il doit respecter les conditions Y.
(d) leur imposer des conditions relativement à la fourniture de leurs services à toute personne qu'il précise, notamment un fournisseur de services de télécommunication;	Si un fournisseur de services de télécommunication fournit un type de service X, il doit respecter les conditions Y.
(e) leur interdire de conclure des ententes de service visant un produit ou un service qu'ils utilisent dans tout ou partie de leurs réseaux ou installations de télécommunication, ou en lien avec ceux-ci;	Un fournisseur de services de télécommunication ne peut pas conclure une entente avec une entreprise X pour un produit ou un service Y.
(f) exiger qu'ils mettent fin aux ententes de service visées à l'alinéa e);	Un fournisseur de services de télécommunication doit mettre fin à l'entente de service Y visée à l'alinéa 15.2(2)e).
(g) leur interdire de mettre à niveau les produits et les services qu'il précise;	Un fournisseur de services de télécommunication ne peut pas mettre à niveau un produit ou service X.
(h) exiger que leurs réseaux ou installations de télécommunication, ainsi que les projets d'approvisionnement qui s'y rapportent, fassent l'objet des processus d'examen qu'il précise;	Les réseaux, les installations et les projets d'approvisionnement d'un fournisseur de services de télécommunication font tous l'objet d'une procédure d'examen.
(i) exiger qu'ils élaborent des plans de sécurité liés à leurs réseaux ou installations de télécommunication ou à leurs services de télécommunication;	Un fournisseur de services de télécommunication doit élaborer un plan de sécurité.

Formulation législative du paragraphe 15.2(2)	Langage clair
(j) exiger que soient menées des évaluations pour repérer toute vulnérabilité de leurs réseaux ou installations de télécommunication, de leurs services de télécommunication ou des plans de sécurité visés à l'alinéa i);	Un fournisseur de services de télécommunication doit repérer les vulnérabilités, y compris celles qui découlent des plans de sécurité [visés à l'alinéa 15.2(2)i)], en ce qui concerne ses réseaux, ses installations et ses services.
(k) exiger qu'ils prennent des mesures visant à atténuer toute vulnérabilité de leurs réseaux ou installations de télécommunication, de leurs services de télécommunication ou des plans de sécurité visés à l'alinéa i);	Un fournisseur de services de télécommunication doit prendre des mesures pour atténuer les vulnérabilités repérées dans son plan de sécurité [visé à l'alinéa 15.2(2)i)] ou qui concernent ses réseaux, ses installations ou ses services.
(l) exiger qu'ils mettent en œuvre des normes qu'il précise relativement à leurs réseaux ou installations de télécommunication ou à leurs services de télécommunication.	Un fournisseur de services de télécommunication est tenu de mettre en œuvre des normes concernant ses réseaux, ses installations et ses services.

Toute personne peut être contrainte de fournir au ministre ou aux personnes désignées par celui-ci des renseignements dont le ministre « a des motifs raisonnables de croire qu'ils sont pertinents dans le cadre de la prise, de la modification ou de la révocation d'un décret visé à l'article 15.1, d'un arrêté visé à l'article 15.2 ou d'un règlement visé à l'alinéa 15.8(1)a) ou de la vérification du respect ou de la prévention du non-respect de l'un ou l'autre de ces textes » (article 15.4). Le gouverneur en conseil, en vertu de l'article 15.8, peut prendre des règlements concernant « les mêmes dispositions qu'un arrêté pris en vertu de l'article 15.2 » [article 15.8(1)a)] et prévoir « les personnes et entités pour l'application de l'alinéa 15.6j) » [article 15.8(1)b)]. L'alinéa 15.6j) décrit l'éventail des parties qui peuvent recueillir ou divulguer des informations les unes des autres, ce qui est abordé plus en détail dans la partie 2.4.

Analyse

Telle qu'elle est rédigée, la loi prévoit un sous-ensemble de menaces pour la cybersécurité qui sont susceptibles d'entraîner l'émission d'un décret ou d'un arrêté ministériel. Ce fait est mis en évidence par l'utilisation du terme « notamment » dans les paragraphes 15.1(1)[21] et 15.2(1)[22], ainsi que dans le paragraphe 15.2(2). En vertu du paragraphe 15.2(2), un arrêté ministériel peut être pris pour « ordonner aux fournisseurs de services de télécommunication de faire ou de s'abstenir de faire toute chose qu'il précise » afin de « sécuriser le système canadien de télécommunication, notamment

[21] « S'il est d'avis que cela est nécessaire pour sécuriser le système canadien de télécommunication, notamment face aux menaces d'ingérence, de manipulation ou de perturbation, le gouverneur en conseil peut, par décret […] ». [Souligné par l'auteur].
[22] « S'il est d'avis que cela est nécessaire pour sécuriser le système canadien de télécommunication, notamment face aux menaces d'ingérence, de manipulation ou de perturbation, le ministre peut, par arrêté, après consultation du ministre de la Sécurité publique et de la Protection civile […] ». [Souligné par l'auteur].

face aux menaces d'ingérence, de manipulation ou de perturbation »[23]. Il en résulte que la loi peut être invoquée, à l'avenir, pour traiter d'autres types d'activités en plus de l'ingérence, de la manipulation ou de la perturbation afin de sécuriser le système de télécommunication canadien.

Dès le départ, la loi limite le gouvernement à l'émission d'un décret ou d'un arrêté ministériel uniquement lorsque cela est nécessaire pour sécuriser le système de télécommunication canadien. Cependant, la nécessité en elle-même ne constitue pas une limite suffisante au pouvoir du gouvernement. La première recommandation est donc de modifier la loi afin d'indiquer de façon explicite que ces décrets et arrêtés doivent être nécessaires, proportionnées et raisonnables.

Recommandation 1 : Les décrets et les arrêtés ministériels doivent être pertinents, proportionnés et raisonnables

La loi devrait être modifiée pour imposer des conditions supplémentaires concernant les circonstances particulières dans lesquelles le gouvernement

Texte	Modification proposée
15.1(1) S'il est d'avis que cela est nécessaire pour sécuriser le système canadien de télécommunication, notamment face aux menaces d'ingérence, de manipulation ou de perturbation, le gouverneur en conseil peut, par décret :	15.1(1) S'il est d'avis que cela est nécessaire, proportionnel et raisonnable pour sécuriser le système canadien de télécommunication ~~notamment~~ face aux menaces d'ingérence, de manipulation ou de perturbation, le gouverneur en conseil peut, par décret :
15.2(2) Le ministre peut, par arrêté, ordonner aux fournisseurs de services de télécommunication de faire ou de s'abstenir de faire toute chose qu'il précise – à l'exception d'une chose prévue aux paragraphes (1) ou 15.1(1) – et qu'il estime nécessaire pour sécuriser le système canadien de télécommunication, notamment face aux menaces d'ingérence, de manipulation ou de perturbation. Il peut, entre autres, par le même arrêté :	15.2(2) Le ministre peut, par arrêté, ordonner aux fournisseurs ~~de services de télécommunication~~ d'entreprendre les actions nécessaires, proportionnées et ~~de faire ou de s'abstenir de faire toute chose qu'il précise~~ – à l'exception d'une chose prévue aux paragraphes (1) ou 15.1(1) – pour exécuter des directives qu'il estime être nécessaires pour sécuriser le système canadien de télécommunication ~~notamment~~ face aux menaces d'ingérence, de manipulation ou de perturbation. Il peut, ~~entre autres,~~ par le même arrêté :

[23] [Souligné par l'auteur].

Deuxièmement, la loi ne contient pas de disposition prévoyant que les organismes privés disposeront d'un délai raisonnable pour modifier leurs pratiques [voir : alinéas 15.1(1)a)-b) et alinéas 15.2(1)a)-b); voir également : alinéas 15.2(2)a)-l)][24]. Alors qu'un décret ou arrêté ne peut être pris que lorsque cela est nécessaire, il n'y a pas d'exigence selon laquelle il doit être réellement possible pour un fournisseur de mettre en œuvre le décret ou arrêté dans le délai imparti. En d'autres termes, même si le gouvernement détermine correctement une menace qui nécessite une modification du mode de fonctionnement d'un fournisseur de services de télécommunication, la vitesse à laquelle le gouvernement s'attend à ce qu'une modification soit mise en œuvre peut être déraisonnable compte tenu de la complexité du réseau ou des services d'un fournisseur.

Il en résulte que le gouvernement peut émettre des décrets ou arrêtés qui reflètent potentiellement une méconnaissance ou un manque d'intérêt pour les défis que pose la mise en œuvre d'interdictions ou de directives, ou qui montrent peu d'intérêt pour les charges financières que de telles activités pourraient imposer à des organismes privés et, par extension, à leurs utilisateurs, abonnés ou clients. Alors que les fournisseurs de services de télécommunication peuvent demander réparation en faisant appel à la Cour fédérale pour un contrôle judiciaire des décrets ou des arrêtés ministériels, les organisations pourraient ne pas avoir besoin de faire appel à cette procédure de plainte si le gouvernement était tenu, lors de la préparation d'un décret ou d'un arrêté, de préciser que les changements dans les réseaux ou les services des fournisseurs de services télécommunication peuvent être apportés dans une période de temps raisonnable. Bien qu'il soit possible que ces délais soient normalement fixés par des organismes comme le Comité consultatif canadien pour la sécurité des télécommunications (CCCST), la loi devrait être plus explicite[25]. Le caractère raisonnable des délais de mise en œuvre devrait être précisé dans la loi plutôt que d'être établi par des organismes de coordination, comme le CCCST, et en particulier lorsque ces organismes n'incluent pas tous les fournisseurs de services de télécommunication susceptibles de recevoir des décrets et arrêtés.

[24] L'article 9 de la *Loi sur la protection des cybersystèmes essentiels* fixe des délais pour la mise en place d'un programme de cybersécurité. Elle comprend également la possibilité de prolonger les délais fixés par la Loi à la discrétion de l'autorité de régulation compétente [article 11 et article 14(3)].

[25] Pour en savoir plus, consultez : Gouvernement du Canada. (2020). « Comité consultatif canadien pour la sécurité des télécommunications (CCCST) », gouvernement du Canada. Accessible à : https://ised-isde.canada.ca/site/gestion-spectre-telecommunications/fr/savoir- plus/comites-intervenants/conseils-comites/comite-consultatif-canadien-pour-securite-telecommunications-cccst.

Recommandation 2 : Les décrets et arrêtés doivent contenir une référence aux délais

Le projet de loi devrait être modifié pour inclure une exigence selon laquelle les fournisseurs de services de télécommunication doivent mettre en œuvre les demandes, les décrets ou les arrêtés en matière de cybersécurité dans un délai raisonnable dans les situations où le respect d'une demande, d'un décret ou d'un arrêté nécessiterait des changements importants dans les activités commerciales ou les opérations techniques des destinataires.

Troisièmement, certaines des activités particulières que les organismes privés pourraient être chargés d'exécuter en vertu des alinéas 15(2)a)-l), peuvent poser des problèmes de sécurité en aval. En vertu de l'alinéa 15.2(2)g), par exemple, il pourrait être interdit aux fournisseurs de services de télécommunication de mettre à niveau un produit ou un service particulier. Une telle interdiction peut être prononcée parce que le gouvernement estime que la mise à niveau fait probablement partie d'une attaque de la chaîne d'approvisionnement et que la nouvelle version d'un produit ou d'un service contient un code malveillant, ou parce qu'une agence gouvernementale, comme le Centre de la sécurité des télécommunications, a besoin d'un délai supplémentaire pour analyser la mise à niveau afin de déterminer si elle comporte des vulnérabilités graves qui ont été ajoutées au code de manière accidentelle ou délibérée. Toutefois, l'interdiction d'une mise à niveau peut également avoir pour effet de bloquer des correctifs de sécurité, des mises à niveau matérielles ou des offres de services qui sont reconnus comme étant bénéfiques, mais qui font partie du même paquet de mise à niveau. En outre, cette interdiction peut avoir des conséquences de plus en plus graves en matière de cybersécurité, lorsqu'un organisme privé se voit interdire de mettre à jour un produit ou un service d'un fournisseur particulier ou de le faire en temps voulu; ce type de circonstances pourrait créer des difficultés pour les opérations commerciales s'il n'existe pas d'autres fournisseurs proposant des produits ou services de remplacement équivalents. Plus concrètement, s'il était interdit de faire appel à un fournisseur qui vend des équipements spécialisés à des fournisseurs de services de télécommunication dans des régions rurales ou moins peuplées du Canada où, sans ces équipements, les services de télécommunication ne pourraient pas être offerts de manière efficace, le respect du décret ou de l'arrêté pourrait conduire à une réduction de la qualité des services de télécommunication dont les clients canadiens bénéficient.

Recommandation 3 : Le gouvernement devrait procéder à des évaluations des impacts avant l'émission de décrets et d'arrêtés

La loi devrait préciser que le gouvernement doit procéder à des évaluations de ses décrets et arrêtés afin de déterminer s'ils peuvent avoir des effets secondaires ou tertiaires qui aggraveraient les pratiques ou la position d'une organisation en matière de cybersécurité. Ces évaluations doivent être présentées aux fournisseurs de services de télécommunication, de même que toute demande ou tout décret, arrêté ou règlement fondé sur ces évaluations. Ces évaluations devraient être incluses dans toutes les analyses de proportionnalité des demandes, des décrets et des arrêtés du gouvernement.

Il est possible que le gouvernement émette un décret, un arrêté ou un règlement ayant pour effet de modifier ou d'entraver gravement la manière dont un fournisseur de services télécommunications peut offrir un service à ses clients existants. Si, même à la suite d'un contrôle judiciaire, un décret ou arrêté est jugé nécessaire, proportionné et raisonnable, un fournisseur devrait être en mesure de demander une aide financière lorsque la mise en œuvre de changements dans ses opérations techniques ou commerciales aurait une incidence importante sur la viabilité économique de son organisation.

Recommandation 4 : Les dispositions d'abstention ou de réduction des coûts devraient être incluses

La loi devrait être modifiée de manière à ce que les fournisseurs de services de télécommunication puissent demander l'abstention de certains décrets ou arrêtés lorsque leur mise en œuvre aurait une incidence importante sur leur viabilité économique. Par ailleurs, si un décret, arrêté ou règlement a un effet néfaste sur la viabilité économique d'un fournisseur de services de télécommunication et que le gouvernement exige qu'il soit exécuté malgré tout, le fournisseur devrait être indemnisé en fonction du coût ou pour la réduction des coûts[26].

L'alinéa 15.2(2)l) de la loi permettrait au ministre d'« exiger qu'ils mettent en œuvre des normes qu'il précise relativement à leurs réseaux ou installations de télécommunication ou à leurs services de télécommunication ». Ce pouvoir pourrait permettre au ministre d'obliger les fournisseurs de services de télécommunication à mettre en place, par exemple, des normes de sécurité optionnelles dans les normes de

[26] Le terme « réduction des coûts » fait référence à un système d'indemnisation dans lequel seule une partie du coût total est indemnisée. Dans ce cas, il s'agirait pour le gouvernement de fournir une partie, mais pas la totalité, de l'indemnisation en fonction du coût destinée aux fournisseurs de services de télécommunication qui modifient leurs offres de services aux abonnés dans le cadre de leurs efforts pour se conformer à un décret, un arrêté ministériel ou un règlement.

télécommunication, de mettre en place une authentification multifactorielle efficace dans les interfaces internes et destinées aux clients, ou de faire quoi que ce soit d'autre qui ait été normalisé quelque part. Il est même possible que des normes soient fixées pour la sécurité physique des installations de télécommunication, notamment en exigeant certains modes de confirmation d'identité biométrique, des habilitations de sécurité pour les employés, ou tout autre élément considéré comme normalisé.

Un précédent rapport du Citizen Lab sur la sécurité des télécommunications affirmait que le gouvernement devrait pouvoir imposer des normes de sécurité en fonction des besoins. Plus précisément, ce rapport indiquait que :

> Le gouvernement pourrait obliger les entreprises de télécommunication canadiennes à activer les éléments de sécurité 5G ou imposer des sanctions commerciales aux entreprises qui refusent d'activer ces éléments (p. ex. en les tenant responsables des dommages ou des fuites de données lorsque des réseaux n'ont pas pleinement activé les éléments de sécurité 5G). Si ces approches demeuraient insuffisantes, le gouvernement pourrait imposer des normes de sécurité de base indépendantes des fournisseurs, que tous les opérateurs canadiens (et leurs fournisseurs) seraient tenus de respecter pour pouvoir fournir des services 5G au Canada[27].

En l'absence d'une définition claire de ce qui est considéré comme une norme dans le projet de loi, il est difficile de déterminer si le gouvernement envisage des normes ou des recommandations internationales (p. ex. 3GPP, recommandations GSMA, IEEE, IETF, CALEA ou ETSI, etc.) ou des normes élaborées et promulguées par le gouvernement canadien ou des organisations canadiennes, ou s'il exige que les fournisseurs de services de télécommunication adoptent des normes qui « sécurisent » les renseignements en permettant au gouvernement d'accéder au trafic de données des fournisseurs, de l'évaluer ou de l'enregistrer à des fins d'application de la loi ou de sécurité nationale. Pour illustrer ce dernier point, un arrêté ministériel pourrait obliger les fournisseurs de services de télécommunication à adopter des normes de chiffrement potentiellement problématiques, au motif que la visibilité d'une partie du trafic pourrait sécuriser le système de télécommunication canadien en permettant aux organismes chargés de l'application de la loi ou de la sécurité de mieux déceler les menaces et d'agir contre elles[28]. Par ailleurs, les normes pourraient obliger les fournisseurs de services de télécommunication filaires à adopter des équipements d'interception légaux conformes aux normes internationales, comme la *Communications Assistance*

---

[27] PARSONS, Christopher. (2020). « Huawei & 5G: Clarifying the Canadian Equities and Charting a Strategic Path Forward », *Citizen Lab*. Accessible à : https://citizenlab.ca/2020/12/huawei-5g-clarifying-the-canadian-equities-and-charting-a-strategic-path-forward/, p. 26.

[28] Voir : Matthew Braga. (2016). « Rogers and Alcatel-Lucent Proposed an Encryption Backdoor for Police », *Motherboard*. Accessible à : https://www.vice.com/en/article/pgkpvz/rogers-and-alcatel-lucent-proposed-an-encryption-backdoor-for-police; Steven J. Murdoch. (2016).
« Insecure by design: protocols for encrypted phone calls », Bentham's Gaze. Accessible à : https://www.benthamsgaze.org/2016/01/19/insecure- by-design-protocols-for-encrypted-phone-calls/.

for Law Enforcement Act (CALEA) des États-Unis ou celles promulguées par l'European Telecommunications Standards Institute (ETSI).

Pour être clair, permettre au gouvernement d'obliger les fournisseurs de services de télécommunication à adopter certaines normes pour mieux sécuriser les réseaux et les services est une bonne chose. Toutefois, telle que rédigée actuellement, la loi ne précise guère les motifs pour lesquels des normes pourraient être exigées[29] et ne prévoit pas non plus d'exigences en matière d'évaluation de l'adoption de normes (p. ex. évaluer si une norme donnée pourrait menacer la vie privée des personnes ou la sécurité des communications). Cela a pour conséquence qu'un aspect potentiellement positif de la loi pourrait, en fait, être utilisé à des fins plus nébuleuses qui pourraient compromettre la capacité des fournisseurs de services de télécommunication à sécuriser leurs réseaux ou les communications de leurs abonnés.

Recommandation 5 : Les normes imposables doivent être définies

La loi devrait être modifiée pour préciser clairement quels types de normes entrent ou non dans son champ d'application. Le projet de loi devrait préciser qu'un décret, un arrêté ou un règlement imposant l'adoption de normes particulières ne peut être utilisé pour compromettre délibérément ou accidentellement la confidentialité, l'intégrité ou la disponibilité d'une installation de télécommunication, d'un service de télécommunication ou d'une installation de transmission. L'objectif de cette recommandation est d'empêcher le gouvernement d'ordonner ou d'exiger que les fournisseurs de services de télécommunication déploient ou activent des capacités ou des pouvoirs liés à l'accès légal afin de « sécuriser » l'infrastructure par l'adoption d'une norme.

2.2. Le secret et l'absence de dispositions en matière de transparence ou de responsabilité

Dans sa version actuelle, le projet de loi C-26 contient de nombreuses exigences en matière de secret et de confidentialité. À un niveau élevé, ces exigences visent à garantir que les renseignements relatifs aux vulnérabilités en matière de sécurité, aux acteurs de la menace et à la sécurité nationale ne soient pas rendus publics. En cas de menaces connues ou d'opérations de menace actives, il n'est pas forcément dans l'intérêt du gouvernement de divulguer ce qu'il sait et d'informer potentiellement les acteurs de la menace de vulnérabilités existantes ou potentielles. Cette philosophie est omniprésente dans le projet de loi.

[29] Le paragraphe 15.2(2) stipule que si le ministre est d'avis qu'une norme est nécessaire pour « sécuriser le système canadien de télécommunication », il existe des motifs suffisants pour imposer l'adoption de la norme.

Les décrets [paragraphe 15.1(2)] et les arrêtés ministériels pris par le ministre de l'Industrie, des Sciences et de la Technologie [paragraphe 15.2(3)] peuvent contenir des dispositions interdisant « à toute personne » de divulguer tout ou une partie du contenu du décret ou de l'arrêté. En outre, le décret ou l'arrêté en question « est » publié dans la *Gazette du Canada*, à moins que le gouverneur en conseil [paragraphe 15.1(4)] ou le ministre [paragraphe 15.2(5)] n'en décide autrement. Dans les cas où un décret ou arrêté est promulgué aux fournisseurs de services de télécommunication, mais est incompatible avec « toute décision prise par le [Conseil de la radiodiffusion et des télécommunications canadiennes] en vertu de la présente loi, de tout autre arrêté pris en vertu de la présente loi ou de la *Loi sur la radiocommunication* ou de toute autorisation délivrée par le ministre en vertu de la présente loi ou de la *Loi sur la radiocommunication* » [paragraphe 15.2(6)], les dispositions du décret l'emportent sur les dispositions incompatibles. Si le gouverneur en conseil prend des règlements, alors dans ces cas également, s'il y a incompatibilité entre ces règlements et « toute décision prise par le Conseil » ou « tout arrêté pris en vertu de la présente loi ou de la *Loi sur la radiocommunication* ou [ ] toute autorisation délivrée par le ministre en vertu de la

présente loi ou de la *Loi sur la radiocommunication* » [paragraphe 15.8(2)], les dispositions de ces règlements l'emportent sur les dispositions incompatibles.

Analyse

Le projet de loi comporte des exigences étendues et excessivement onéreuses en matière de secret et de confidentialité. On peut soutenir qu'un certain degré de secret et de confidentialité est nécessaire dans la loi, étant donné qu'il est insensé que le gouvernement rende publics des systèmes ou des produits dont la vulnérabilité est connue; les fournisseurs de services de télécommunication auront besoin d'un certain temps pour éliminer les vulnérabilités existantes ou potentielles. Toutefois, les exigences du projet de loi en matière de confidentialité sont trop étendues et peuvent permettre au gouvernement d'agir sans avoir imposé de restrictions appropriées à ses pouvoirs ou sans avoir associé des mécanismes de responsabilité à ses pouvoirs de décret ou d'arrêté.

Tout d'abord, c'est généralement dans la *Gazette du Canada* que le gouvernement du Canada publie « les nouvelles lois, les nouveaux règlements et les règlements proposés, les décisions des tribunaux administratifs ainsi que les avis publics[30] ». Bien que les paragraphes 15.1(4) et 15.2(5) affirment que le décret ou l'arrêté « doit » être publié de la même manière, le ministre peut en ordonner autrement dans le décret ou l'arrêté. Il en résulte que le gouvernement peut prendre des décrets ou arrêtés qui ne sont jamais

[30] Gouvernement du Canada. (2022). « Gazette du Canada », gouvernement du Canada. Accessible à : https://www. gazette.gc.ca/accueil-home-fra.html.

publiés dans la *Gazette du Canada*, et qu'il n'est pas nécessaire qu'ils soient publiés dans un format complet et non expurgé. Cela signifie en fin de compte que le gouvernement pourrait contraindre des organismes privés à modifier leurs pratiques techniques ou commerciales, même si ces modifications sont disproportionnées par rapport à une menace ou vont à l'encontre de la protection des infrastructures essentielles canadiennes contre les menaces, et le gouvernement ne risquerait jamais d'être critiqué par le public qui lit et analyse les décrets ou arrêtés en question. En outre, il n'existe aucun critère à remplir pour interdire la publication d'un décret ou arrêté dans la *Gazette*, ce qui aurait pour effet de laisser la décision au bon vouloir du gouverneur en conseil ou du ministre au lieu de nécessiter la démonstration d'un besoin pressant.

Recommandation 6 : Les décrets et arrêtés devraient paraître dans la *Gazette du Canada*

La loi devrait être modifiée pour exiger la publication des décrets et arrêtés dans la *Gazette du Canada* dans les 180 jours suivant leur émission ou dans les 90 jours suivant leur mise en œuvre, selon la condition qui est satisfaite en premier.

Recommandation 7 : Le ministre devrait être contraint de présenter des rapports relatifs aux décrets, arrêtés et règlements

La loi devrait être modifiée de manière que le ministre de l'Industrie, des Sciences et de la Technologie soit tenu de présenter chaque année une liste des éléments suivants :

- le nombre de décrets, d'arrêtés et de règlements émis;
- les types de décrets, d'arrêtés et de règlements émis;
- le nombre de fournisseurs de services de télécommunication qui ont reçu les décrets et arrêtés;
- le nombre de fournisseurs de services de télécommunication qui se sont partiellement conformés aux décrets et arrêtés;
- le nombre de fournisseurs de services de télécommunication qui se sont entièrement conformés aux décrets et arrêtés;
- une analyse de la nécessité, de la proportionnalité, du caractère raisonnable et de l'utilité des pouvoirs prévus par les décrets et arrêtés.

Si le ministre ne présente pas ces rapports, il devrait être tenu de se présenter devant un comité parlementaire pour expliquer ce manquement et fournir un délai dans lequel ces rapports seront déposés.

Les décrets et les arrêtés ministériels peuvent contenir des dispositions de consigne du silence. Celles-ci peuvent empêcher les dénonciateurs d'informer le public de directives ou d'interdictions disproportionnées ou déficientes de la part du gouvernement. Ces consignes du silence ne sont pas soumises à un test de raisonnabilité, de nécessité ou de proportionnalité qui permettrait de déterminer quand elles peuvent être incluses dans un décret ou arrêté. La loi ne contient pas non plus de dispositions qui lèveraient la consigne du silence après un certain temps, dans un délai particulier (p. ex. 90, 180 ou 365 jours) ou après l'achèvement d'une action (p. ex. la mise en œuvre de pratiques conformes au décret ou à l'arrêté en question), ou une combinaison des deux (p. ex. 90 jours après la mise en œuvre de pratiques conformes au décret, à l'arrêté ou au règlement en question). Par conséquent, il est possible que tous les décrets et arrêtés comportent des consignes du silence qui ne sont jamais levées, de sorte que les citoyens canadiens ou même les organismes privés ne se rendent jamais compte de la mesure dans laquelle le gouvernement émet des décrets, des arrêtés ou des règlements.

Recommandation 8 : Les consignes du silence devraient être limitées dans le temps

La loi devrait être modifiée afin d'inclure une période précise après la réception d'un décret, d'un arrêté ou d'un règlement, ou après la mise en conformité à celui-ci, pendant laquelle un fournisseur de services de télécommunication peut communiquer qu'il a reçu un décret, un arrêté ou un règlement, ou s'est mis en conformité à celui-ci.

La possibilité pour un décret, un arrêté ministériel ou un règlement d'annuler une décision du Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC), accompagnée des dispositions relatives au secret susmentionnées, risque de créer un nouveau type de droit quasi occulte. Le CRTC organise des procédures publiques relativement ouvertes au cours desquelles les intervenants peuvent présenter et contester les preuves et les positions du CRTC dans le cadre du processus d'élaboration d'un ensemble de règles publiques sur la manière dont les fournisseurs de services de télécommunication peuvent ou doivent mener leurs activités.

Cependant, les décisions du CRTC ne sont pas toujours correctes sur le plan des faits[31], ce qui pourrait, dans certaines situations, contraindre les fournisseurs de services de télécommunication à prendre des mesures qui vont à l'encontre de ce que le gouvernement du Canada estime être la meilleure façon de sécuriser l'infrastructure des télécommunications du Canada.

[31] Voir à titre d'exemple : Clarification de l'ACEI dans laquelle elle explique pourquoi une récente décision du CRTC concernant les zombies avait une mauvaise compréhension de certains des services que l'ACEI offre à Mozilla. Accessible à : Autorité canadienne pour les enregistrements Internet (ACEI). « Un cadre de blocage des réseaux de zombies pour le Canada », ACEI. Accessible à : https://www.cira.ca/fr/ressources/nouvelles/etat-de-linternet/un-cadre-de-blocage-des-reseaux-de-zombies-pour-le-canada/.

S'il est compréhensible que le gouvernement veuille pouvoir empêcher les fournisseurs de services de télécommunication d'entreprendre des activités qu'il considère comme préjudiciables aux intérêts canadiens, les décrets, les arrêtés ministériels ou les règlements que les fournisseurs de services de télécommunication recevront ne seront pas nécessairement rendus publics. Cela risque de créer une sorte de droit public – connu par les décisions du CRTC – et de droit occulte – compris uniquement par les parties qui ont reçu des décrets, des arrêtés ou des règlements contraires du gouvernement – ayant pour effet d'empêcher les particuliers de comprendre réellement les règles qui régissent les fournisseurs de services de télécommunication qui mènent des activités au Canada.

Recommandation 9 : Le CRTC devrait indiquer quand les décrets et arrêtés annulent des parties de ses décisions

La loi devrait être modifiée pour, au minimum, exiger que le CRTC publie un avis public joint à toutes ses décisions lorsqu'il y a une contradiction entre sa décision et un décret, un arrêté ministériel ou un règlement qui a prévalu sur une partie d'une décision du CRTC.

La possibilité pour le gouvernement d'émettre des décrets, des arrêtés ou des règlements qui annulent les décisions de droit public prises dans le cadre des procédures du CRTC peut mettre en péril le processus par lequel les décisions sont prises par les intervenants dans les audiences du CRTC. Si le processus de délibération actuel du CRTC fait l'objet de critiques externes, il reste néanmoins relativement transparent pour les fournisseurs et le public. En ajoutant la possibilité d'obliger discrètement les fournisseurs de services de télécommunication à faire quelque chose, potentiellement en violation des décisions du CRTC et sans avis public, la valeur et l'importance même de la participation aux décisions du CRTC liées à la cybersécurité sont remises en question : pourquoi participer alors que le gouvernement peut secrètement émettre des décrets et arrêtés qui sont contraires à la procédure et aux décisions publiquement débattues ?

Recommandation 10 : Le rapport annuel devrait indiquer le nombre de fois où les décrets, arrêtés ou règlements gouvernementaux ont prévalu sur les décisions du CRTC

La loi devrait être modifiée pour obliger le gouvernement à divulguer chaque année le nombre de fois où il a émis des décrets, des arrêtés ou des règlements qui ont prévalu en cas d'incohérence entre un décret, un arrêté ou un règlement donné et une décision du CRTC, ainsi qu'à indiquer quelle décision du CRTC a été visée.

L'un des rôles du Parlement est d'examiner les réglementations. En imposant des restrictions sur les règlements, en les excluant potentiellement de la *Gazette du Canada* et en ayant modifié la *Loi sur les textes réglementaires* en 2015[32], il est possible que le Comité mixte permanent d'examen de la réglementation ne soit pas en mesure de tenir le gouvernement responsable des règlements qui sont adoptés dans le cadre des projets de réforme de la *Loi sur les télécommunications*. Il en résulte que des règlements peuvent être créés et promulgués sans que le Comité puisse évaluer « la légalité et les aspects procéduraux de la réglementation, et non sur le bien-fondé des règlements eux-mêmes ou des politiques qu'ils mettent en œuvre[33] ».

Recommandation 11 : Tous les règlements en vertu de la *Loi sur les télécommunications* doivent être accessibles au Comité mixte permanent d'examen de la réglementation

La loi devrait être modifiée de manière que le Comité mixte permanent d'examen de la réglementation puisse obtenir, évaluer et rendre un verdict public sur tout règlement promulgué dans le cadre du projet de réforme de la *Loi sur les télécommunications*. Le Comité devrait également être habilité à obtenir, évaluer et rendre un verdict public sur les règlements relatifs à la *Loi sur les télécommunications* et qui sont modifiés conformément à l'article 18 de la *Loi sur les textes réglementaires*.

2.3. Une procédure de contrôle judiciaire déficiente

Dans les cas où les fournisseurs de services de télécommunication ne sont pas d'accord avec les décrets pris en vertu de l'article 15.1, les arrêtés pris en vertu de l'article 15.2 ou les règlements pris en vertu de l'alinéa 15.8(1)a), ils peuvent demander un contrôle judiciaire. Plus précisément, lorsqu'un fournisseur de services de télécommunication

« estime qu'une certaine autorité gouvernementale a exercé ses pouvoirs de manière

---

[32] La *Loi sur les textes réglementaires* a été modifiée pour permettre l'intégration de documents (ou d'autres éléments d'information) dans un règlement sans que le Comité mixte permanent d'examen de la réglementation ait à se pencher sur la question. Voir : « Projet de loi S-2 : Lois du Canada (2015) – Loi modifiant la *Loi sur les textes réglementaires* et le *Règlement sur les textes réglementaires* en conséquence », Parlement du Canada. Accessible à : https://www.parl.ca/Content/Bills/412/Government/S-2/S-2_4/S-2_4.PDF. Article 18.

[33] Comité mixte permanent d'examen de la réglementation. (2022). « À propos », Parlement du Canada. Accessible à : https://www.parl.ca/Committees/fr/REGS/About.

Le Comité évalue chaque règlement en fonction de 13 critères. Cela consiste à évaluer si un règlement donné : « 1. n'est pas autorisé par les dispositions de la législation habilitante ou n'est pas conforme à toute condition prescrite dans la législation; 2. n'est pas conforme à la *Charte canadienne des droits et libertés* ou à la *Déclaration canadienne des droits*; 3. a un effet rétroactif en l'absence d'autorisation formelle dans la législation habilitante; 4. impose des frais au Trésor public ou exige qu'un paiement soit versé à la Couronne ou à toute autre autorité, ou prescrit le montant quelconque de ces frais ou paiements, en l'absence d'autorisation formelle dans la législation habilitante; 5. impose une amende, une peine d'emprisonnement ou une autre pénalité en l'absence d'autorisation formelle dans la législation habilitante; 6. tend directement ou indirectement à exclure la juridiction des tribunaux en l'absence d'autorisation formelle dans la législation habilitante; 7. n'est pas conforme à la *Loi sur les textes réglementaires*; 8. paraît pour une raison quelconque enfreindre le principe de la légalité;
9. empiète indûment sur les droits et libertés de la personne; 10. assujettit indûment les droits et libertés de la personne au pouvoir discrétionnaire de l'Administration ou n'est pas conforme aux règles de justice naturelle; 11. utilise de manière inhabituelle ou inattendue les pouvoirs que confère la législation habilitante; 12. représente l'exercice d'un pouvoir législatif de fond qui devrait faire l'objet d'une loi par le Parlement; 13. est défectueux dans sa rédaction ou, pour toute autre raison, nécessite des éclaircissements quant à sa forme ou à son objet. »

arbitraire, discriminatoire ou autrement déraisonnable, il peut intenter une action devant un tribunal pour demander le "contrôle judiciaire", c'est-à-dire demander que le tribunal examine la décision administrative. Si le tribunal donne raison au plaignant, il peut annuler la décision administrative[34] ». Toutefois, selon le projet de loi, la procédure de contrôle judiciaire pourrait être réalisée en secret.

Dans un premier temps, le ministre de l'Industrie, des Sciences et de la Technologie peut demander que certaines preuves du gouvernement soient entendues exclusivement par le juge. Si le gouvernement fait cette demande et que le juge conclut que « la divulgation de ces éléments de preuve ou renseignements pourrait porter atteinte, selon lui, aux relations internationales, à la défense nationale, à la sécurité nationale ou à la sécurité d'autrui », le juge doit alors faire droit à la demande [alinéa 15.9(1)a)]. Le juge doit garantir la confidentialité de ces preuves lorsque « la divulgation porterait atteinte, selon lui, aux relations internationales, à la défense nationale, à la sécurité nationale ou à la sécurité d'autrui » [alinéa 15.9(1)b)].

Le demandeur du contrôle doit recevoir « un résumé des éléments de preuve ou autres renseignements dont il dispose et qui permet au demandeur d'être suffisamment informé de la thèse du gouvernement du Canada », mais le demandeur n'est pas autorisé à accéder aux renseignements « dont la divulgation porterait atteinte, selon [le juge], aux relations internationales, à la défense nationale, à la sécurité nationale ou à la sécurité d'autrui » [alinéa 15.9(1)c)]. Bien que le demandeur et le ministre doivent avoir la possibilité d'être entendus [alinéa 15.9(1)d)], la décision sans appel du juge peut être prise en fonction d'éléments de preuve qui n'ont pas été présentés au demandeur [alinéa 15.9(1)e)]. La décision ne peut pas être fondée sur des preuves qui ont été retirées ou jugées non pertinentes [alinéa 15.9(1)f)]. Tous les éléments de preuve présentés par le ministre, y compris ceux qui sont retirés, doivent rester confidentiels [alinéa 15.9(1)g)]. Tout appel doit comporter les mêmes dispositions en matière de secret [paragraphe 15.9(2)].

Analyse

Il est possible qu'un décret, un arrêté ministériel ou un règlement soit fondé sur des preuves obtenues par une agence de sécurité ou de renseignement canadienne ou fournies au gouvernement canadien par un État ou un organisme étranger. La communauté de la sécurité et du renseignement protège avec zèle ses sources et ses méthodes, ainsi que celles des organismes étrangers, par crainte que leur divulgation nuise à une collecte de renseignements en cours ou compromette l'échange

[34] Centre d'études constitutionnelles. (2019). « Judicial Review », Centre d'études constitutionnelles. Accessible à : https://www.constitutionalstudies.ca/2019/07/judicial-review/.

d'information avec des États et des organismes étrangers. La raison d'être du secret de l'article 15.9 est probablement qu'en l'absence de ces protections, le gouvernement devrait soigneusement évaluer s'il souhaite présenter des preuves qui pourraient justifier de contraindre des organismes privés à modifier leurs pratiques techniques ou commerciales, ou ne pas contraindre à la modification et préserver le secret des sources et des méthodes pertinentes.

En d'autres termes, l'article 15.9 est conçu, du moins en partie, pour permettre au gouvernement d'utiliser des preuves ou des renseignements secrets pour élaborer des décrets, des arrêtés et des règlements sans courir le risque que ces preuves ou ces renseignements soient rendus publics ou révélés à des parties non gouvernementales.

Cependant, le projet de loi aurait pour effet d'empêcher les fournisseurs de services de télécommunication de présenter des arguments convaincants pour justifier le caractère arbitraire, discriminatoire ou déraisonnable d'une décision gouvernementale. Prenons l'exemple suivant : le gouvernement apprend qu'il existe une vulnérabilité dans une partie d'une mise à jour logicielle, et la communauté de la sécurité et du renseignement soupçonne qu'elle pourrait être exploitée par des adversaires motivés pour interférer, manipuler ou perturber le système de télécommunication canadien. En réponse, le ministre prend un décret ou arrêté interdisant aux fournisseurs de services de télécommunication de mettre à jour les produits [alinéa 15.2(2)g)] et les obligeant, par la suite, à respecter des conditions particulières pour les futures mises à jour logicielles [alinéa 15.2(2)b)]. Le décret ou arrêté ne peut toutefois pas expliquer ou justifier la proportionnalité ou le caractère raisonnable de la directive, ni décrire les éléments particuliers du correctif qui ont suscité des inquiétudes, ce qui peut amener le fournisseur de services de télécommunication à demander un contrôle judiciaire.

Le fournisseur de services de télécommunication pourrait s'opposer au décret ou arrêté pour les raisons suivantes :

- Si les mises à jour *ne sont pas* appliquées, toutes les autres vulnérabilités qui sont corrigées dans le correctif logiciel seront connues des adversaires, qui pourront alors s'en servir pour tenter d'exploiter les réseaux ou les systèmes des fournisseurs.
- Il est impossible, voire irréalisable, d'isoler uniquement le ou les éléments exploitables de la mise à jour logicielle et, selon toute probabilité, il est plus important de sécuriser la plus grande partie possible du réseau ou du système, en dépit des vulnérabilités potentiellement exploitables qui seraient également présentes.

Dans l'un ou l'autre de ces cas, le fournisseur en question pourrait faire valoir ses arguments sans avoir accès à des preuves secrètes. Toutefois, à moins qu'un décret ou arrêté du gouvernement ne désigne une *partie* précise d'une mise à jour qui pose problème, le fournisseur peut être incapable de proposer d'autres méthodes plus proportionnées pour atténuer la menace en question. Par exemple, il est possible qu'une mise à jour logicielle donnée soit mise en œuvre *et* que la menace soit atténuée, mais pour qu'un fournisseur puisse faire valoir cet argument, il doit comprendre le vecteur de menace particulier et exploitable afin d'élaborer une politique d'atténuation.

Il existe d'autres situations dans lesquelles le gouvernement peut émettre une demande, mais où les fournisseurs ne peuvent pas présenter un argument complet contre la directive du gouvernement sans avoir accès aux preuves secrètes de ce dernier. Par exemple, le gouvernement pourrait émettre des décrets ou arrêtés qui s'alignent sur sa position hostile ou politique à l'égard de fournisseurs et de services particuliers qui mènent des activités à partir de la République populaire de Chine. Un juge fédéral pourrait décider qu'un décret ou arrêté interdisant l'accès à ZTE et Huawei est légitime à la lumière des preuves publiées par le National Cyber Security Centre (NCSC) du Royaume-Uni, mais comment le même juge devrait-il évaluer les risques potentiels posés par d'autres fournisseurs chinois pour lesquels moins d'informations sont publiées? De même, comment un juge pourrait-il évaluer les situations dans lesquelles les services dont dépend un fournisseur de services de télécommunication utilisent un code créé par des personnes de citoyenneté chinoise qu'on croit agir pour se conformer à la loi chinoise en matière de sécurité nationale, qui a une très grande portée? Lorsque les preuves précises du gouvernement ne sont pas présentées aux fournisseurs, ceux- ci peuvent être incapables de démontrer de façon convaincante que les arguments du gouvernement découlent moins des preuves présentées que de suppositions entourant ces preuves.

Enfin, il est possible que la vulnérabilité perçue ne soit pas elle-même une vulnérabilité. En d'autres termes, les preuves techniques sur lesquelles le gouvernement fonde son décret, son arrêté ou son règlement peuvent être déficientes. Dans toute situation où la révélation des preuves est considérée par le gouvernement comme préjudiciable à la défense nationale du Canada et donc exclue de la vue d'un fournisseur, ce dernier pourrait être incapable de présenter les raisons pour lesquelles les conclusions techniques auxquelles le gouvernement est parvenu ne répondraient pas à l'exigence de nécessité associée à un décret ou arrêté, sans parler de sa proportionnalité ou de son caractère raisonnable.

De manière générale, le problème des preuves secrètes pouvant constituer la base d'une décision sans contrôle judiciaire est que les fournisseurs peuvent être contraints

d'entreprendre des actions ou de cesser certaines activités lorsque les preuves en question ne soutiennent pas pleinement la directive du gouvernement. Que pourrait- on faire pour remédier à cette situation? Au minimum, la loi devrait indiquer de façon explicite que lorsque les preuves sont suffisamment sensibles pour empêcher l'avocat d'un fournisseur de services de télécommunication de les entendre, un intervenant désintéressé pourrait être nommé pour entendre et éventuellement contester les preuves en question[35]. Il n'est pas nécessaire d'***exiger*** qu'un intervenant désintéressé soit nommé – il est possible que, dans certains cas, les preuves soient telles qu'il est clair qu'un décret ou arrêté n'est pas arbitraire, discriminatoire ou déraisonnable – mais le fait d'intégrer explicitement l'intervenant désintéressé dans la loi pourrait réduire l'opacité du processus d'examen et, par conséquent, améliorer la perception du caractère raisonnable des décrets et arrêtés du gouvernement et de la justesse des décisions judiciaires.

Recommandation 12 : Le contrôle judiciaire devrait explicitement permettre la désignation d'un intervenant désintéressé

La loi devrait être modifiée de manière que, à la discrétion de la Cour, des intervenants désintéressés puissent être nommés pour contester et répondre aux informations fournies par le gouvernement à l'appui d'un décret, d'un arrêté ministériel ou d'un règlement visé à l'article 15.8.

2.4. Échange intensif de renseignements au sein des agences canadiennes et au-delà

Le ministre de l'Industrie, des Sciences et de la Technologie dispose de moyens étendus pour obliger les fournisseurs de services de télécommunication à divulguer des renseignements et ensuite les diffuser largement au sein du gouvernement fédéral ainsi qu'à l'échelle internationale. Toute personne peut être tenue de fournir au ministre de l'Industrie, des Sciences et de la Technologie des renseignements dont le ministre

« a des motifs raisonnables de croire qu'ils sont pertinents dans le cadre de la prise, de la modification ou de la révocation d'un décret visé à l'article 15.1, d'un arrêté visé à l'article 15.2 ou d'un règlement visé à l'alinéa 15.8(1)a) ou de la vérification du respect ou de la prévention du non-respect de l'un ou l'autre de ces textes » (article 15.4).

---

[35] Comme l'a noté le juge Mosley, « l'intervenant désintéressé aidera la Cour fédérale à examiner les informations contestées et à répondre aux arguments du procureur général […] L'intervenant désintéressé aura accès aux documents contestés à titre confidentiel et pourra contester les affirmations du gouvernement selon lesquelles la divulgation publique des informations en question nuirait à la sécurité nationale, à la défense nationale ou aux relations internationales. L'intervenant désintéressé peut également présenter des observations au nom de la personne accusée ou de la partie intéressée en ce qui concerne l'exercice d'évaluation qui doit être effectué par le juge désigné. » Voir : L'honorable Richard G. Mosley. (2015). « A View from the Bunker: The Role of the Federal Court in National Security », Cour fédérale du Canada. Accessible à : https:// www.fct-cf.gc.ca/Content/assets/pdf/base/Mosley%20J%20lecture%20-%20A%20View%20from%20 the%20Bunker%20-%20for%20posting%20(ENG).pdf.

Les renseignements confidentiels sont définis à l'article 15.5(1) et comprennent a) les secrets industriels; b) les renseignements financiers, commerciaux, scientifiques ou techniques qui sont de nature confidentielle et qui sont traités comme tels de façon constante par elle; c) les renseignements dont la communication risquerait vraisemblablement soit de causer à une autre personne ou à elle-même des pertes ou profits financiers appréciables ou de nuire à sa compétitivité, soit d'entraver des négociations menées par cette autre personne ou elle-même en vue de contrats ou à d'autres fins. La définition n'indique pas explicitement que les renseignements personnels constituent nécessairement des renseignements confidentiels.

Bien qu'il soit interdit de « sciemment communiquer des renseignements désignés comme confidentiels, ni en autoriser la communication », il existe des exceptions. Ils peuvent être divulgués lorsque la loi l'exige [alinéa 15.5(3)a)], lorsque la partie qui les a désignés comme confidentiels consent à leur divulgation [alinéa 15.5(3)b)], ou lorsque

« le ministre estime que la communication est nécessaire pour sécuriser le système canadien de télécommunication, notamment face aux menaces d'ingérence, de manipulation ou de perturbation » [alinéa 15.5(3)c)].

L'article 15.6 indique clairement qu'un large éventail de parties peut, nonobstant l'article 15.5, recueillir ou divulguer des renseignements aux fins liées « à la prise, à la modification ou à la révocation d'un décret visé à l'article 15.1, d'un arrêté visé à l'article 15.2 ou d'un règlement visé à l'alinéa 15.8(1)a) » ou « à la vérification du respect ou à la prévention du non-respect de l'un ou l'autre de ces textes ». Cet éventail de parties comprend :

(a) le ministre;

(b) le ministre de la Sécurité publique et de la Protection civile;

(c) le ministre des Affaires étrangères;

(d) le ministre de la Défense nationale;

(e) le chef d'état-major de la Défense;

(f) le chef ou un employé du Centre de la sécurité des télécommunications;

(g) le directeur ou un employé du Service canadien du renseignement de sécurité;

(h) le président ou un employé du Conseil;

(i) toute personne désignée en vertu de l'article 15.4;

(j) toute autre personne ou entité prévue par règlement.

En outre, conformément à l'article 15.7(1) :

> Le ministre peut communiquer aux termes d'accords, d'ententes ou d'arrangements conclus par écrit entre, d'une part, l'administration fédérale et, d'autre part, l'administration d'une province ou d'un État étranger, une organisation internationale

> d'États ou une organisation internationale établie par des gouvernements, ou l'un de leurs organismes […] s'il croit qu'ils pourraient être utiles pour sécuriser le système canadien de télécommunications ou un système de télécommunications étranger, notamment face aux menaces d'ingérence, de manipulation ou de perturbation[36].

Si des renseignements sont communiqués à un gouvernement étranger, des entreprises ou des particuliers canadiens peuvent subir des conséquences non pénales. Si un fournisseur de services de télécommunication a adopté un comportement contraire à celui d'un décret visé à l'article 15.1, d'un arrêté visé à l'article 15.2 ou d'un règlement visé par la Loi et qu'une loi d'un État étranger traite d'un comportement qui est essentiellement similaire à celui d'un tel décret, arrêté ou règlement [paragraphe 15.7(2)], l'État étranger ne peut pas utiliser les renseignements pour poursuivre des enquêtes criminelles. Toutefois, l'État étranger pourrait engager des procédures réglementaires ou disposer de droits d'action privés. Par exemple, si un fournisseur de services de télécommunication a des obligations réglementaires dans un État étranger qui sont parallèles aux exigences énoncées dans un décret visé à l'article 15.1, un arrêté visé à l'article 15.2 ou un règlement visé à l'article 15.8, l'autorité réglementaire étrangère pourrait intenter une action. Si, par exemple, le gouvernement des États-Unis avait interdit les services logiciels d'un fournisseur donné ou imposé des exigences de déclaration particulières parallèles à celles du Canada et qu'un fournisseur n'avait pas respecté ces exigences, ce dernier pourrait faire l'objet de reproches de la part des autorités de réglementation américaines[37]. Le paragraphe 15.7(2) risque donc d'exposer les fournisseurs de services de télécommunication qui mènent des activités au Canada à des poursuites judiciaires à l'étranger.

Analyse

Le pouvoir d'exiger des renseignements confidentiels est nécessaire pour permettre, faire appliquer et évaluer les décrets et arrêtés visés aux articles 15.1 et 15.2, ainsi que les règlements visés à l'article 15.8. Cependant, alors que le projet de loi habiliterait le ministre à recueillir et à divulguer largement les renseignements des fournisseurs de services de télécommunication et les renseignements confidentiels, la loi n'impose pas au gouvernement de rendre des comptes. Chacune des recommandations de cette section du rapport soutient l'ajout d'une responsabilité gouvernementale dans la loi.

---

[36] [Souligné par l'auteur].

[37] Bien qu'elles sortent du cadre de ce rapport, certaines exigences imposées aux fournisseurs de services de télécommunication et aux fournisseurs d'infrastructures essentielles figurent dans les documents suivants : Maison-Blanche. (2021). « Executive Order 14028: Improving the Nation's Cybersecurity », Maison-Blanche. Accessible à : https://www.whitehouse. gov/briefing-room/presidential- actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/; ou le Department of Home Affairs. (2022). « Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 », gouvernement de l'Australie. Accessible à : https://www.homeaffairs. gov.au/reports- and-publications/submissions-and-discussion-papers/slacip-bill-2022.

Tout d'abord, la loi précise que si le ministre exige des renseignements (y compris des renseignements confidentiels) de la part d'un fournisseur de services de télécommunication, ces renseignements peuvent être largement diffusés au sein du gouvernement du Canada. À l'échelle nationale, l'alinéa 15.6j) signifie que toute partie peut théoriquement recevoir les renseignements en question[38]. Cela peut avoir pour effet d'accorder au gouvernement un accès beaucoup plus approfondi à la configuration, au fonctionnement et à la gestion des systèmes des fournisseurs de services de télécommunication, tout en augmentant les risques que des renseignements confidentiels, ainsi que des renseignements personnels ou dépersonnalisés, soient diffusés ou divulgués de manière inappropriée, simplement en raison du nombre de parties ou de personnes qui peuvent prendre connaissance de ces renseignements. Aucune sanction particulière n'est appliquée au gouvernement canadien si la partie qui reçoit les renseignements confidentiels, ou les renseignements personnels ou dépersonnalisés, en permet la divulgation sans le savoir ou de façon accidentelle.

Recommandation 13 : Des indemnisations devraient être prévues si le gouvernement ne gère pas correctement les renseignements confidentiels

La loi devrait être modifiée pour permettre aux fournisseurs de services de télécommunication de demander une indemnisation si le gouvernement ou une partie à laquelle le gouvernement a divulgué des renseignements confidentiels perd involontairement le contrôle de ces renseignements et si cette perte de contrôle a des conséquences matérielles sur les activités commerciales ou techniques d'un fournisseur de services de télécommunication.

Recommandation 14 : Des indemnisations devraient être prévues si le gouvernement ne gère pas correctement les renseignements personnels ou dépersonnalisés

La loi devrait être modifiée pour permettre aux particuliers de demander une indemnisation si le gouvernement ou une partie à laquelle le gouvernement a divulgué leurs renseignements personnels ou dépersonnalisés perd involontairement le contrôle de ces renseignements et si cette perte de contrôle a des conséquences matérielles sur le particulier.

Il n'y a aucune obligation d'informer le fournisseur de services de télécommunication si ou pourquoi ses renseignements confidentiels sont divulgués à des agences fédérales ou des institutions canadiennes. L'article 15.4 n'exige pas du ministre qu'il explique pourquoi les renseignements sont recueillis ou à qui ils peuvent être communiqués[39].

[38] « 15.6 Malgré l'article 15.5, dans la mesure nécessaire à toute fin liée à la prise, à la modification ou à la révocation d'un décret visé à l'article 15.1, d'un arrêté visé à l'article 15.2 ou d'un règlement visé à l'alinéa 15.8(1)a) ou à la vérification du respect ou à la prévention du non- respect de l'un ou l'autre de ces textes, les personnes ou entités ci-après peuvent recueillir les unes auprès des autres ou se communiquer les unes aux autres des renseignements, notamment des renseignements confidentiels […] j) toute autre personne ou entité prévue par règlement. » [39] « 15.4 Le ministre peut exiger de toute personne qu'elle fournisse, selon les modalités qu'il précise, à la personne qu'il désigne ou à lui-même
les renseignements à l'égard desquels il a des motifs raisonnables de croire qu'ils sont pertinents dans le cadre de la prise, de la modification ou

Cette omission peut placer les fournisseurs de services de télécommunication dans des situations où ils ne savent pas ce qui est précisément demandé par le ministre, ni qui examinera ou utilisera les renseignements fournis.

Recommandation 15 : Le gouvernement devrait expliquer comment il utilisera les renseignements et révéler les agences nationales auxquelles les renseignements sont divulgués

Le gouvernement devrait être tenu de fournir aux fournisseurs de services de télécommunication concernés au moins un résumé général de la manière dont il entend utiliser les renseignements qu'il obtient d'eux, y compris les renseignements confidentiels, ainsi qu'une description des parties auxquelles les renseignements seront ou pourront être divulgués.

La loi ne limite pas étroitement la manière dont les agences gouvernementales peuvent utiliser les renseignements qu'elles reçoivent des fournisseurs de services de télécommunication, par rapport aux pouvoirs conférés au ministre de l'Innovation, des Sciences et de l'Industrie en vertu du projet de loi C-26. Dans le cas du Centre de la sécurité des télécommunications (CST), par exemple, les renseignements qu'il reçoit pourraient être utilisés pour faciliter n'importe quel aspect de son mandat, et pas seulement les éléments de cybersécurité et d'assurance de l'information de ce mandat. Les renseignements provenant des fournisseurs de services de télécommunication pourraient être utilisés pour éclairer certains éléments des activités de renseignement d'origine électromagnétique du CST, des opérations de cybersécurité et d'assurance de l'information, de l'assistance à d'autres agences fédérales désignées, ou même de ses opérations cybernétiques actives ou de défense. La loi devrait préciser comment les agences destinataires peuvent utiliser les renseignements des fournisseurs de services de télécommunication et interdire à ces agences d'utiliser ces renseignements pour des activités qui ne sont pas au service de la cybersécurité ou de l'assurance de l'information.

Recommandation 16 : Les renseignements obtenus auprès des fournisseurs de services de télécommunication ne doivent être utilisés que pour des activités de cybersécurité et d'assurance des renseignements

La loi devrait être modifiée pour limiter les organismes gouvernementaux à l'utilisation exclusive des renseignements obtenus auprès des fournisseurs de services de télécommunication en vertu du projet de loi C-26 pour les activités de cybersécurité et d'assurance de l'information. Les renseignements ne devraient pas être utilisés à des fins de renseignement d'origine électromagnétique ou étranger, de soutien interministériel non relatif à la cybersécurité ou d'opérations cybernétiques actives ou de défense. Ces restrictions devraient s'appliquer à toutes les agences, y compris, mais sans s'y limiter, celles qui relèvent du ministre de la Sécurité publique et de la Protection civile (p. ex. la Gendarmerie royale du Canada et le Service canadien du renseignement de sécurité) et du ministre de la Défense nationale (p. ex. les Forces armées canadiennes et le Centre de la sécurité des télécommunications).

---

de la révocation d'un décret visé à l'article 15.1, d'un arrêté visé à l'article 15.2 ou d'un règlement visé à l'alinéa 15.8(1)a) ou de la vérification du respect ou de la prévention du non-respect de l'un ou l'autre de ces textes. »

La loi ne contient aucune disposition obligeant les agences canadiennes à supprimer ou à détruire les données ou les renseignements confidentiels obtenus auprès des fournisseurs de services de télécommunication après une période donnée ou après qu'un événement se soit produit (p. ex. l'évaluation du respect d'un décret ou arrêté). Il en résulte que les agences gouvernementales pourraient conserver indéfiniment des renseignements provenant d'entreprises de télécommunication, ce qui constituerait une intégration insuffisante de dispositions relatives à la responsabilité dans les nouveaux pouvoirs gouvernementaux proposés.

Recommandation 17 : Des périodes de conservation des données devraient être imposées aux données des fournisseurs de services de télécommunication

La loi devrait être modifiée afin de préciser que les renseignements obtenus auprès des fournisseurs de services de télécommunication ne seront conservés que pendant la période nécessaire à la prise, à la modification ou à la révocation d'un décret visé à l'article 15.1, d'un arrêté visé à l'article 15.2 ou d'un règlement visé à l'alinéa 15.8(1)a) ou à la vérification du respect ou à la prévention du non-respect d'un tel décret, arrêté ou règlement.

Les périodes de conservation doivent être communiquées aux fournisseurs de services de télécommunication auprès desquels le ministre a recueilli des renseignements.

La loi n'oblige pas le gouvernement canadien à imposer des exigences en matière de conservation et de suppression des données aux États, agences ou organismes étrangers auxquels il divulgue des renseignements des fournisseurs de services de télécommunication. Tout comme le gouvernement devrait être contraint d'adopter des périodes de conservation, les organismes étrangers qui reçoivent des renseignements des fournisseurs devraient également être contraints de le faire.

Recommandation 18 : Des périodes de conservation des données devraient être imposées aux divulgations de renseignements à l'étranger

La loi devrait être modifiée pour exiger que le gouvernement ajoute des dispositions de conservation et de suppression des données dans les ententes ou les protocoles d'entente conclus avec des agences étrangères.

Il n'existe aucune obligation d'informer un fournisseur de services de télécommunication de l'éventail des parties étrangères avec lesquelles ses renseignements ont été divulgués. Étant donné que les parties étrangères peuvent utiliser les renseignements pour lancer des enquêtes et engager des poursuites non pénales contre les fournisseurs, le gouvernement devrait signaler que les renseignements des fournisseurs de services de télécommunication sont, ou ont été, divulgués à des fins de cybersécurité.

Recommandation 19 : Les fournisseurs de services de télécommunication devraient être informés des parties étrangères qui reçoivent leurs renseignements

La loi devrait être modifiée de manière que les fournisseurs de services de télécommunication soient explicitement informés du moment et, le cas échéant, de l'entité à qui les renseignements peuvent être divulgués lorsque le destinataire est un État étranger ou une agence, une organisation ou une partie étrangère.

Texte original	Modification proposée
15.7(1) Le ministre peut communiquer aux termes d'accords, d'ententes ou d'arrangements conclus par écrit entre, d'une part, l'administration fédérale et, d'autre part, l'administration d'une province ou d'un État étranger, une organisation internationale d'États ou une organisation internationale établie par des gouvernements, ou l'un de leurs organismes, des renseignements recueillis ou obtenus dans le cadre de la présente loi, à l'exception de renseignements désignés comme confidentiels en vertu du paragraphe 15.5(1), s'il croit qu'ils pourraient être utiles pour sécuriser le système canadien de télécommunications ou un système de télécommunications étranger, notamment face aux menaces d'ingérence, de manipulation ou de perturbation.	15.7(1) Le ministre peut seulement communiquer aux termes d'accords, d'ententes ou d'arrangements conclus par écrit entre, d'une part, l'administration fédérale et, d'autre part, l'administration d'une province ou d'un État étranger, une organisation internationale d'États ou une organisation internationale établie par des gouvernements, ou l'un de leurs organismes, des renseignements recueillis ou obtenus dans le cadre de la présente loi, à l'exception de renseignements désignés comme confidentiels en vertu du paragraphe 15.5(1), s'il croit qu'ils ~~pourraient être~~ sont utiles pour sécuriser le système canadien de télécommunications ou un système de télécommunications étranger ~~notamment~~ face aux menaces d'ingérence, de manipulation ou de perturbation.

Le paragraphe 15.7(1) indique clairement que des renseignements non confidentiels peuvent être divulgués dans le cadre d'un protocole d'entente lorsque le ministre

« croit qu'ils pourraient être utiles pour sécuriser le système canadien de télécommunications ou un système de télécommunications étranger, notamment face aux menaces d'ingérence, de manipulation ou de perturbation »[40]. L'utilisation conjointe des termes « croit » et « pourraient » suggère que les conditions qui doivent être remplies avant la divulgation des renseignements ne sont pas particulièrement strictes et pourraient donc permettre un échange important de renseignements privés, sinon confidentiels.

[40] [Souligné par l'auteur].

En outre, l'utilisation du terme « notamment » dans le projet de loi actuel ne délimite pas étroitement ce que l'on entend par « sécuriser » le système canadien de télécommunication ou un système de télécommunication étranger. En effet, si les renseignements peuvent être divulgués pour faire face à des menaces d'ingérence, de manipulation, ou de perturbation, ils pourraient être divulgués pour d'autres menaces qui ne sont pas indiquées explicitement dans la loi. L'ingérence, la manipulation et la perturbation sont déjà des catégories très larges de menaces possibles. Le gouvernement devrait être tenu de publier les modifications à cette liste tripartite au lieu d'être autorisé à ajouter discrètement d'autres types d'activités sans avoir à rendre publics les ajouts à la liste. L'énumération précise des menaces qui justifient la divulgation de renseignements privés, mais non confidentiels, permettra au gouvernement de mieux contrôler l'utilisation future des renseignements des organismes privés.

Recommandation 20 : La loi devrait délimiter les conditions dans lesquelles les renseignements d'un organisme privé peuvent être divulgués

Le gouvernement devrait restreindre les conditions sous lesquelles le ministre peut divulguer les renseignements d'un organisme privé.

2.5. Coûts liés à la conformité en matière de sécurité

Le projet de loi C-26 donne au ministre de l'Innovation, des Sciences et de l'Industrie une capacité extrêmement large d'exiger des fournisseurs de services de télécommunication qu'ils fassent ou qu'ils s'abstiennent de faire quoi que ce soit, pour autant que l'action ordonnée permette de protéger le système canadien de télécommunication contre les menaces, y compris celles liées aux activités ou opérations d'ingérence, de perturbation ou de manipulation. Les fournisseurs qui protestent contre les décrets ou arrêtés, mais qui ne parviennent pas à obtenir un contrôle judiciaire, devront se conformer aux décrets ou arrêtés, même s'ils n'ont pas reçu les preuves utilisées pour les justifier. Les fournisseurs n'auront pas droit à une indemnisation « pour les pertes financières » liée à l'exécution d'un décret visé à l'article 15.1 ou d'un arrêté visé à l'article 15.2 [paragraphes 15.1(5) et 15.2(7)].

Analyse

Premièrement, les coûts associés au respect des décrets, des arrêtés et des règlements peuvent varier considérablement en fonction de ce que le gouvernement exige d'un fournisseur de services de télécommunication, et les petits fournisseurs peuvent avoir du mal à gérer ces coûts. À titre d'exemple, considérons les coûts qui peuvent être subis

lors de l'élaboration d'un plan de sécurité complet qui tient également compte de la détermination et de la gestion des vulnérabilités, des pratiques d'atténuation et de la conformité aux normes. Le coût d'élaboration d'un tel plan peut être globalement plus élevé pour un grand fournisseur de services de télécommunication (p. ex. Bell, Telus, Rogers) que pour un fournisseur plus petit (p. ex. Execulink ou Teksavvy), tout en constituant une plus petite partie des recettes trimestrielles des grands fournisseurs, parce qu'ils peuvent déjà disposer du personnel politique, technique et de sécurité nécessaire qui peut être à nouveau chargé de l'élaboration et du maintien d'une telle politique.

Recommandation 21 : Une indemnisation devrait être incluse pour les petites organisations

Il devrait y avoir un mécanisme par lequel les petits fournisseurs de services de télécommunication (p. ex. ceux qui ont moins de 250 000 ou 500 000 abonnés ou clients) qui ont toujours été consciencieux dans leurs dispositions de sécurité peuvent demander au moins une certaine indemnisation temporaire s'ils sont tenus d'entreprendre de nouvelles pratiques commerciales ou organisationnelles, de modifier les pratiques existantes ou de cesser les pratiques en cours à la suite d'une demande, d'un décret, d'un arrêté ou d'un règlement du gouvernement. Cet allègement peut ne concerner qu'une partie des coûts encourus et, par conséquent, constituer une formule de « réduction des coûts ».

Deuxièmement, dans certaines situations, les coûts liés à l'exécution d'un décret ou arrêté peuvent compromettre certains aspects des activités d'un fournisseur de services de télécommunication. Prenons le cas d'un décret ou arrêté interdisant l'utilisation des produits ou services du fournisseur A et pour lequel il n'existe pas de concurrent équivalent fournissant des services similaires à un coût similaire. Si les produits ou services du fournisseur A sont nécessaires pour atteindre un sous-ensemble de clients (p. ex. le fournisseur A vend un équipement spécialisé qui permet d'offrir un service sans fil en milieu rural), il est possible que les clients concernés perdent leur service de télécommunication en raison de l'absence d'un produit ou d'un service de remplacement comparable et existant. Il en va de même pour les équipements spécialisés vendus par les fournisseurs qui, bien qu'ils présentent des failles de sécurité potentielles ou réelles susceptibles d'être exploitées, sont essentiels pour fournir des services de qualité aux particuliers et aux organisations au Canada. Rien dans la loi, telle qu'elle est actuellement rédigée, ne prend clairement en compte ces considérations, ni la manière dont la suppression de certains secteurs d'activité ou régions de service à la clientèle pourrait avoir des conséquences financières préjudiciables pour les fournisseurs de services de télécommunication, sans parler des personnes et des organisations qui pourraient être touchées par toute suppression de services liée à la sécurité.

Recommandation 22 : Les évaluations de la proportionnalité et de l'équité devraient être incluses dans les décrets, arrêtés ou règlements

Les évaluations de la proportionnalité et de l'équité devraient être incluses dans l'élaboration de tout décret, arrêté ministériel ou règlement en vertu de la Loi. Les résultats de ces évaluations devraient être pris en considération par le gouvernement avant la publication d'un décret, d'un arrêté ou d'un règlement, devraient être fournis aux fournisseurs de services de télécommunication en même temps que les décrets, arrêtés ou règlements associés, et devraient être inclus dans tout dossier de preuve qui pourrait être utilisé si un fournisseur de services de télécommunication demandait un contrôle judiciaire d'un décret, d'un arrêté ou d'un règlement donné.

Les fournisseurs de services de télécommunication peuvent être tenus d'entreprendre une série d'activités afin de renforcer la sécurité de leurs réseaux et de leurs services. Au moins certains fournisseurs seront probablement tenus d'embaucher du personnel ou de faire appel à des consultants pour s'acquitter des exigences définies dans les demandes, les décrets, les arrêtés ou les règlements du gouvernement. Il est déjà difficile de trouver et de conserver du personnel possédant des compétences spécialisées en matière de cybersécurité et, dans le cas des petites entreprises dont les marges de profit sont limitées et qui comptent peu d'employés, il se peut qu'elles aient des difficultés financières à recruter le personnel nécessaire. Ces difficultés peuvent être amplifiées dans le cas des fournisseurs de services de télécommunication qui desservent principalement des collectivités rurales ou éloignées. En effet, on ne sait pas très bien si les fournisseurs de services de télécommunication pourront facilement trouver les talents nécessaires pour se conformer aux demandes, aux décrets, aux arrêtés ou aux règlements du gouvernement en matière de cybersécurité, et encore moins s'ils pourront payer les salaires de ces professionnels.

Par ailleurs, en fonction de la manière dont le gouvernement dotera en personnel ses propres équipes chargées d'évaluer les orientations en matière de cybersécurité, d'élaborer des exigences de conformité, etc., la question de savoir si le gouvernement fédéral devra également embaucher du personnel pour mettre en œuvre ses programmes de sécurité des télécommunications et des infrastructures essentielles reste ouverte. En supposant que le gouvernement doive embaucher davantage de professionnels, cela pourrait créer une situation dans laquelle les secteurs privé et public seraient en concurrence pour les mêmes catégories de professionnels de la cybersécurité, ce qui rendrait encore plus difficile pour les organismes publics ou les organismes privés sous réglementation fédérale d'obtenir le personnel nécessaire pour élaborer et respecter les décrets, les arrêtés et les règlements en matière de sécurité.

Recommandation 23 : Le gouvernement devrait encourager la formation à la cybersécurité

Le gouvernement devrait s'engager à renforcer les bourses d'études, les subventions ou d'autres mesures incitatives pour encourager les personnes au Canada à suivre une formation professionnelle en cybersécurité. Cette formation pourrait inclure une formation ciblée qui atténuerait les difficultés de recrutement pouvant résulter de l'obligation pour les fournisseurs de services de télécommunication et les autres fournisseurs d'infrastructures essentielles d'adopter de nouvelles pratiques proactives et réactives en matière de cybersécurité, associées à des décrets, des arrêtés ministériels ou des règlements liés à la cybersécurité. Ces efforts d'éducation et de formation devraient être conçus de manière à favoriser une main-d'œuvre diversifiée et inclusive.

2.6. Formulation vague du projet de loi

Comme indiqué dans les parties précédentes de ce rapport, le projet de loi ne délimite pas les types précis de menaces pour la sécurité qui pourraient être traitées par des décrets, des arrêtés ministériels ou des règlements. C'est ce qu'indiquent des termes comme « notamment » dans les paragraphes 15.1(1), 15.2(1) et 15.2(2), qui ont pour effet de décrire certains types de menaces pesant sur le système canadien de télécommunication (c.-à-d. l'ingérence, la manipulation ou la perturbation) sans énumérer toutes les menaces potentielles auxquelles la loi pourrait s'attaquer à l'avenir.

De même, d'autres termes ou concepts importants, comme ceux énumérés dans la liste suivante, ne sont pas expliqués ou définis dans la loi :

- ingérence;
- manipulation;
- perturbation.

La loi confère également au ministre de l'Innovation, des Sciences et de l'Industrie un champ de compétences non défini dans la mesure où, en vertu du paragraphe 15.2(2),

« Le ministre peut, par arrêté, ordonner aux fournisseurs de services de télécommunication de faire ou de s'abstenir de faire toute chose qu'il précise »[41]. L'effet est qu'il n'y a pas de limites particulièrement claires à ce qui peut être contenu dans un arrêté, ce qui permet au ministre d'être aussi précis ou vague qu'il le souhaite dans ses arrêtés, y compris en ordonnant à un fournisseur de services de télécommunication de faire ou de s'abstenir de faire quelque chose qui, d'un point de vue fonctionnel, ce fournisseur n'est peut-être pas en mesure de faire ou de ne pas faire.

[41] [Souligné par l'auteur].

Enfin, le projet de loi ne définit pas clairement la manière dont les renseignements personnels identifiables obtenus auprès des fournisseurs de services de télécommunication doivent être traités. C'est ce qui ressort de l'examen de l'article 15.5. Plus précisément, l'alinéa 15.5(1)b) reconnaît que certains renseignements financiers, commerciaux, scientifiques ou techniques sont classés comme confidentiels. Les renseignements confidentiels peuvent également comprendre ceux dont la communication risquerait vraisemblablement de causer à une personne des pertes ou profits financiers appréciables, de nuire à sa compétitivité ou d'entraver des négociations menées par cette personne en vue de contrats ou à d'autres fins. Il est possible que des renseignements personnels entrent parfois, mais pas toujours, dans ces catégories.

Analyse

En l'absence de définitions précises, le gouvernement, les entreprises de télécommunication et les juges qui examinent l'application de la loi peuvent se tourner vers des décisions judiciaires antérieures, des dictionnaires, d'autres lois canadiennes, la jurisprudence et des décisions prises par d'autres administrations pour définir les termes importants de la loi. Néanmoins, chacun des termes essentiels de la loi peut couvrir un très grand éventail d'activités. À titre d'exemple, un arrêté ministériel pourrait imposer une condition au système de téléphonie vocale chiffrée de bout en bout d'un fournisseur de services de télécommunication. Plus précisément, l'arrêté pourrait, en vertu de l'alinéa 15.2(2)b), imposer au fournisseur de permettre l'accès légal à tous ses services vocaux, de sorte que lorsque le fournisseur reçoit un mandat valide, il pourrait divulguer le contenu de la communication dans un format en texte clair/non chiffré aux agences gouvernementales. Cette disposition n'ordonnerait pas explicitement au fournisseur de services de télécommunication de *ne pas* mettre à disposition un service de téléphonie chiffrée de bout en bout, mais elle aurait néanmoins le même objectif.

De même, et à titre d'exemple, un arrêté ministériel pourrait, en vertu de la mention

« entre autres » du paragraphe 15.2(2), exiger que les fournisseurs de services de télécommunication concluent des ententes de cybersécurité avec le Centre canadien pour la cybersécurité (CCCS) afin de mieux se protéger contre les menaces fondées sur les réseaux. Dans une telle situation, les fournisseurs pourraient communiquer avec le CCCS/Centre de la sécurité des télécommunications (CST) et conclure une entente en vertu du paragraphe 27(2) de la *Loi sur le Centre de la sécurité des télécommunications* afin de permettre au CST :

> une autorisation de cybersécurité habilitant ce dernier, dans la réalisation du volet de son mandat touchant la cybersécurité et l'assurance de l'information et malgré toute autre loi fédérale, à accéder à une infrastructure de l'information désignée comme

étant d'importance pour le gouvernement fédéral en vertu du paragraphe 21(1) ou à acquérir de l'information qui provient ou passe par cette infrastructure, qui leur est destinée ou y est stockée afin d'aider à protéger, dans les cas visés à l'alinéa 184(2)e) du *Code criminel*, cette infrastructure contre tout méfait, toute utilisation non autorisée ou toute perturbation de leur fonctionnement.

Il est important de noter qu'en vertu de la *Loi sur le Centre de la sécurité des télécommunications*, les types de menaces à prendre en compte sont plus clairs – méfait, utilisation non autorisée ou perturbation selon le *Code criminel* – alors que les mêmes définitions ne sont pas fournies dans les réformes de la *Loi sur les télécommunications* prévues par le projet de loi C-26. En effet, le gouvernement n'a pas expliqué pourquoi, en vertu de la *Loi sur le Centre de la sécurité des télécommunications*, les autorisations en matière de cybersécurité sont limitées aux méfaits, à l'utilisation non autorisée ou à la perturbation, alors que les réformes à la *Loi sur les télécommunications* proposées utilisent la formulation « notamment face aux menaces d'ingérence, de manipulation ou de perturbation ». On peut dire que la formulation du projet de loi C-26 est beaucoup plus large que celle de la *Loi sur le Centre de la sécurité des télécommunications*.

Recommandation 24 : Tout le contenu de la loi doit être clair

Le gouvernement devrait préciser comment les menaces envisagées dans le projet de loi (« notamment face aux menaces d'ingérence, de manipulation ou de perturbation ») se comparent aux actions précises visées au paragraphe 27(2) de la *Loi sur le Centre de la sécurité des télécommunications* (« tout méfait, toute utilisation non autorisée ou toute perturbation »), dans le but d'expliquer si les réformes de la *Loi sur les télécommunications* élargiraient, réduiraient ou concerneraient les mêmes catégories d'actions que celles envisagées dans la *Loi sur le Centre de sécurité des télécommunications*.

Lorsque l'intention est de refléter les actions décrites au paragraphe 27(2), une formulation similaire devrait être adoptée, et si l'objectif est de s'écarter intentionnellement de cette formulation, le gouvernement devrait clarifier comment et pourquoi il le fait afin d'encourager le débat public sur cet écart.

Recommandation 25 : Des définitions claires devraient être présentes dans la loi ou rendues publiques

La loi devrait être modifiée pour fournir des définitions claires des termes « ingérence », « manipulation » et « perturbation », ou pour préciser que les définitions se trouvent dans d'autres lois particulières, ou encore pour ordonner au gouvernement de partager publiquement ces définitions et toute mise à jour ultérieure de ces définitions en dehors de la loi.

Si l'exemple consistant à obliger les fournisseurs de services de télécommunication à conclure des ententes avec le CST est peut-être un peu exagéré, il permet néanmoins de montrer ce que l'expression « entre autres » pourrait englober dans le cadre du projet de loi. Si la flexibilité est certainement nécessaire pour permettre au gouvernement de répondre aux nouvelles menaces, il n'a pas, à ce stade, expliqué clairement pourquoi la liste actuelle des activités possibles en vertu des alinéas 15.2(2)a)-l) est insuffisante. Si le gouvernement estime qu'une certaine flexibilité intégrée est nécessaire, il pourrait adopter une modification qui lui permettrait d'obliger les entreprises à prendre des mesures en réponse à une situation d'urgence et, par la suite, faire contrôler la nécessité, le caractère raisonnable et la proportionnalité du décret ou arrêté d'urgence par la Cour fédérale, avec l'obligation de publier l'examen de la Cour.

Recommandation 26 : La flexibilité ministérielle doit être limitée

La loi devrait être modifiée pour délimiter les capacités et les pouvoirs précis du ministre en vertu de la loi.

Texte original	Modification proposée
15.2(2) Le ministre peut, par arrêté, ordonner aux fournisseurs de services de télécommunication de faire ou de s'abstenir de faire toute chose qu'il précise – à l'exception d'une chose prévue aux paragraphes (1) ou 15.1(1) – et qu'il estime nécessaire pour sécuriser le système canadien de télécommunication, notamment face aux menaces d'ingérence, de manipulation ou de perturbation. Il peut, entre autres, par le même arrêté :	15.2(2) Le ministre peut, par arrêté, ordonner aux fournisseurs de services de télécommunication de faire ou de s'abstenir de faire toute chose qu'il précise – à l'exception d'une chose prévue aux paragraphes (1) ou 15.1(1) – et qu'il estime nécessaire pour sécuriser le système canadien de télécommunication, notamment face aux menaces d'ingérence, de manipulation ou de perturbation. Il peut, ~~entre autres,~~ par le même arrêté :

Recommandation 27 : Situations d'urgence

La loi pourrait être modifiée de telle sorte que, si la recommandation 26 est adoptée, le ministre conserverait un certain degré de flexibilité, avec la garantie que les nouveaux types de décrets ou arrêtés seront soumis à un contrôle judiciaire effectué par la Cour fédérale. Ces contrôles devraient évaluer la nécessité, le caractère raisonnable et la proportionnalité, et les décisions qui en découlent devraient être publiées par la Cour fédérale.

Enfin, le projet de loi devrait être modifié pour, au minimum, rendre explicite le fait que les renseignements personnels et les renseignements dépersonnalisés doivent être traités de manière confidentielle. En outre, les modifications devraient établir qu'une autorisation judiciaire préalable est requise avant que le gouvernement ne puisse contraindre les fournisseurs de services de télécommunication à divulguer de tels renseignements. Dans l'état actuel de la loi, il y a probablement des cas où les renseignements personnels seraient confidentiels, par exemple, si leur divulgation par un fournisseur de services de télécommunication avait des conséquences matérielles sur les finances, les positions concurrentielles, les contrats ou les négociations d'un particulier. Toutefois, ces catégories ne couvrent probablement qu'un nombre infime de situations, de sorte que, dans la plupart des cas, les renseignements personnels et les renseignements dépersonnalisés ne font pas partie de ces catégories.

Par ailleurs, les fournisseurs de services de télécommunication eux-mêmes peuvent désigner les renseignements personnels ou les renseignements dépersonnalisés de leurs abonnés comme constituant des renseignements financiers, commerciaux, scientifiques ou techniques, bien que, là encore, les renseignements eux-mêmes ne correspondent pas toujours clairement à ces catégories. Ainsi, le gouvernement devrait préciser que les renseignements personnels et dépersonnalisés obtenus auprès des fournisseurs de services de télécommunication constituent des renseignements confidentiels et que le gouvernement doit obtenir l'approbation préalable de la Cour fédérale dans les cas où il tente d'obtenir ces renseignements auprès des fournisseurs afin de prendre, de modifier ou de révoquer un décret visé à l'article 15.1, un arrêté visé à l'article 15.2 ou un règlement visé à l'alinéa 15.8(1)a) ou de vérifier le respect ou empêcher le non-respect d'un tel décret, arrêté ou règlement. Le gouvernement devrait être empêché de divulguer des renseignements personnels ou dépersonnalisés à des gouvernements

ou organismes étrangers.

Recommandation 28 : Les renseignements personnels sont des renseignements confidentiels

La loi devrait être modifiée pour préciser que tous les renseignements personnels et les renseignements dépersonnalisés qui sont divulgués par les fournisseurs de services de télécommunication sont classés comme des renseignements confidentiels.

Texte original	Modification proposée
Renseignements confidentiels – désignation 15.5(1) La personne qui fournit des renseignements en application de l'article 15.4 peut désigner comme confidentiels : ...	Renseignements confidentiels – désignation 15.5(1) La personne qui fournit des renseignements en application de l'article 15.4 peut désigner comme confidentiels : ... d) les renseignements personnels ou dépersonnalisés

Recommandation 29 : Autorisation judiciaire préalable pour l'obtention de renseignements personnels ou dépersonnalisés

La loi devrait être modifiée de telle sorte qu'avant que le gouvernement puisse contraindre un fournisseur de services de télécommunication à divulguer des renseignements personnels ou dépersonnalisés, il doit d'abord obtenir une ordonnance judiciaire pertinente de la Cour fédérale, lorsque les renseignements doivent être utilisés exclusivement pour prendre, modifier ou révoquer un décret visé à l'article 15.1, un arrêté visé à l'article 15.2 ou un règlement visé à l'alinéa 15.8(1)a), ou pour vérifier le respect ou empêcher le non-respect d'un tel décret, arrêté ou règlement.

Recommandation 30 : Interdire la divulgation de renseignements personnels ou dépersonnalisés à des organismes étrangers

La loi devrait être modifiée pour préciser que le gouvernement ne peut pas divulguer à des gouvernements ou organismes étrangers des renseignements personnels ou dépersonnalisés qu'il a obtenus auprès de fournisseurs de services de télécommunication.

3. Contrepoids à la sécurité

Tel qu'il est rédigé, le projet de loi C-26 aurait pour effet de conférer au gouvernement des pouvoirs insuffisamment délimités qui pourraient contraindre les fournisseurs de services de télécommunication à faire quoi que ce soit, et ce, sous un épais voile de secret entourant ce qui est ordonné et la façon dont les fournisseurs y répondent. Les renseignements que le gouvernement exige des fournisseurs de services de télécommunication pourraient être largement diffusés, et certains de ces renseignements pourraient comprendre des renseignements personnels identifiables ou dépersonnalisés. En outre, les coûts liés au respect des décrets ou arrêtés peuvent avoir des conséquences matérielles sur les fournisseurs de services de télécommunication, comprenant le risque que certaines entreprises soient incapables de continuer à fournir des services à l'ensemble de leurs clients.

Le plus remarquable est peut-être que les réformes à la *Loi sur les télécommunications* proposées ne font aucune référence à des organismes indépendants qui pourraient aider le gouvernement à évaluer la nécessité, la proportionnalité ou le caractère raisonnable d'un décret, d'un arrêté ministériel ou d'un règlement. Le gouvernement pourrait remédier à cette situation en précisant les rôles du Commissariat à la protection de la vie privée du Canada, du Comité des parlementaires sur la sécurité nationale et le renseignement ou de l'Office de surveillance des activités en matière de sécurité nationale et de renseignement aux différents stades du processus d'élaboration des décrets, arrêtés ou règlements. De même, alors que les fournisseurs de services de télécommunication peuvent demander un contrôle judiciaire des décrets, des arrêtés ou des règlements qu'ils doivent respecter, les particuliers ou les collectivités susceptibles d'être touchées par ces décrets et arrêtés n'ont aucun recours. Que peuvent faire des particuliers ou des collectivités, par exemple, si un décret ou arrêté a pour effet de mettre fin à des services dont ils dépendent? Aussi, dans le cas où un décret, un arrêté ou un règlement annule certains éléments d'une décision du CRTC, comment les fournisseurs de services de télécommunication ou les membres du public qui participent aux processus décisionnels du CRTC connaîtront-ils et prendront-ils en compte les effets de ces décrets, arrêtés ou règlements lorsqu'ils prendront part aux processus réglementaires en matière de télécommunication?

En plus de ne pas indiquer ce que les particuliers ou les collectivités peuvent faire si un

décret ou arrêté du gouvernement a des effets délétères sur eux, le gouvernement a refusé de publier un énoncé concernant la Charte pour accompagner la loi[42]. Le résultat est que la loi est manifestement axée sur la sécurité à l'exclusion de tout autre intérêt, et à aucun endroit la loi réformant la *Loi sur les télécommunications* n'aborde la façon dont les intérêts de la vie privée ou de l'équité devraient être protégés. S'il est important que les infrastructures essentielles du Canada, y compris les réseaux de télécommunication, soient à l'abri des ingérences adverses, ces efforts doivent être équilibrés avec les normes démocratiques concurrentes qui exigent que le gouvernement rende compte de ses activités et que celles-ci soient lisibles pour le public.

En évaluant comment modifier le projet de loi C-26, les parlementaires et le gouvernement du Canada devraient réfléchir au rôle que la vie privée et les autres intérêts fondés sur les droits devraient jouer lors de l'élaboration ou de l'émission d'une demande, d'un décret, d'un arrêté ou d'un règlement qui pourrait avoir une incidence sur la façon dont les particuliers ou les collectivités utilisent les systèmes de télécommunication. Bien qu'il soit possible que la politique gouvernementale existante exige que des analyses axées sur la vie privée ou sur l'égalité des sexes soient intégrées dans tout décret, arrêté ou règlement, en plus d'autres évaluations fondées sur l'équité, la loi, telle qu'elle est actuellement rédigée, n'exige pas que de telles évaluations soient effectuées. De nombreux membres du gouvernement pourraient se plaindre que de telles évaluations auraient pour effet de restreindre la capacité du Canada à répondre aux menaces en matière de cybersécurité. Cependant, le fait de ne pas procéder à ces évaluations peut amener le gouvernement – et ceux qui souhaitent défendre les intérêts canadiens – à prendre des mesures qui ont une incidence négative sur les résidents du Canada. Il en résulte que les réseaux de télécommunication du Canada pourraient être sécurisés au prix d'une incidence disproportionnée sur les particuliers et les collectivités qui dépendent le plus de ces réseaux.

En d'autres termes, les efforts en matière de cybersécurité devraient d'abord se concentrer sur la manière dont les actions permettront l'épanouissement des particuliers et des collectivités au Canada, plutôt que de se concentrer sur le fonctionnement sécurisé des systèmes d'infrastructures essentielles. Le risque que les actions aient des conséquences involontaires et préjudiciables, notamment pour les particuliers et les collectivités historiquement privées de leurs droits, est amplifié par l'absence actuelle d'exigences en matière de proportionnalité dans le projet de loi. La combinaison des exigences de nécessité et de proportionnalité pourrait avoir comme effet de conditionner des décrets, arrêtés ou règlements qui pourraient autrement

[42] Voir : Ministère de la Justice du Canada. (2022). « Énoncés concernant la Charte », *Gouvernement du Canada*. Accessible à : https://www.justice.gc.ca/fra/sjc-csj/pl/charte-charter/index.html.

avoir des conséquences inéquitables pour les résidents du Canada.

Le projet de loi C-26, tel qu'il est actuellement rédigé, menace d'affaiblir encore davantage la confiance entre le gouvernement et les experts en cybersécurité non gouvernementaux, sans parler de l'affaiblissement de la confiance entre le gouvernement et le public. Ce dernier élément est particulièrement important, car l'existence d'une loi susceptible de modifier de manière importante les caractéristiques commerciales et techniques des réseaux de télécommunication canadiens pourrait être utilisée par des acteurs irresponsables pour attiser les craintes que le gouvernement fédéral utilise ses vastes pouvoirs au détriment des droits des résidents canadiens garantis par la Charte. L'intégration de garanties appropriées dans le projet de loi C-26 pourrait contribuer à atténuer au moins certaines de ces préoccupations tout en démontrant l'engagement du gouvernement à protéger les droits garantis par la Charte et à élaborer une loi conforme aux valeurs démocratiques et aux normes de transparence et de responsabilité.

4. Conclusion

Le projet de loi C-26 : Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois vise à doter le gouvernement canadien de pouvoirs lui permettant d'obliger les fournisseurs de services de télécommunication à accomplir ou à s'abstenir d'accomplir des mesures précises afin de protéger le système canadien de télécommunication contre les menaces, telles que celles liées à l'ingérence, à la manipulation ou à la perturbation. Cette loi fait écho aux lois et aux mesures exécutives de certains alliés et amis du Canada. Toutefois, jusqu'à présent, le gouvernement n'a pas clairement expliqué pourquoi il a besoin de cette loi en premier lieu. Dans quelle mesure les fournisseurs de services de télécommunication du Canada (et d'autres fournisseurs d'infrastructures essentielles) répondent-ils actuellement aux attentes du gouvernement du Canada en matière de cybersécurité et dans quelle mesure ces attentes sont-elles appropriées ou raisonnables? Le projet de loi C-26 est-il destiné à relever les défis existants ou historiques ou, au contraire, est-il tourné vers l'avenir et destiné à faire face aux menaces prévues? Ou bien est-il censé faire les deux? Le gouvernement doit expliquer aux résidents et aux entreprises du Canada les raisons pour lesquelles il cherche à obtenir de nouveaux pouvoirs et expliquer les raisons sous-jacentes à la création de cette loi sur la cybersécurité.

Citizen Lab a déjà fait valoir que le gouvernement devrait avoir la possibilité d'obliger les organismes privés à adopter des normes afin de sécuriser au mieux les infrastructures essentielles. De même, le gouvernement devrait pouvoir discipliner et dissuader les acteurs qui mènent des activités qui mettent en danger les particuliers et les collectivités au Canada ou qui risquent de compromettre les systèmes de télécommunication qui sont au cœur de l'économie de l'information, et imposer des coûts à ces acteurs. Aussi, lorsque les entreprises de télécommunication refusent d'expliquer comment elles sécurisent leurs systèmes, il est logique que le gouvernement soit en mesure d'exiger ces informations.

Toutefois, les pouvoirs demandés par le gouvernement ne sont pas suffisamment délimités, sont accompagnés de dispositions de confidentialité trop larges et risquent d'entraver la capacité des entreprises privées à contester les demandes, les décrets, les arrêtés ou les règlements émis par le gouvernement. De même, il existe un risque réel que le CRTC crée un droit public par l'intermédiaire de ses décisions, alors qu'une sorte de droit secret, promulgué par l'intermédiaire de décrets, d'arrêtés et de règlements, guide les comportements des fournisseurs de services de

télécommunication en matière de cybersécurité. Les pouvoirs proposés par le gouvernement dans le projet de loi C-26 doivent donc être réduits à certains endroits, les dispositions et la terminologie essentielles doivent être définies, et les exigences en matière de responsabilité et de transparence doivent être plus présentes dans une version modifiée de la loi.

Si le gouvernement refuse de modifier de manière significative sa loi et de se rendre à la fois plus responsable et plus transparent vis-à-vis des fournisseurs de services de télécommunication et du public, il aura adopté une mauvaise loi. Les gouvernements autoritaires seraient en mesure d'invoquer un projet de loi C-26 non modifié pour justifier leur propre loi en matière de sécurité, qui n'est pas soumise à l'obligation de rendre des comptes et qui est secrète et répressive. Alors que la forme actuelle du projet de loi C-26 pourrait permettre de lutter contre les menaces pesant sur les systèmes de télécommunication du Canada, elle portera simultanément atteinte à la légitimité du droit en empêchant les particuliers au Canada de comprendre réellement ce que le droit signifie et comment et quand il est appliqué.

Certains membres du gouvernement peuvent penser qu'il est impératif de maintenir le secret sur la manière dont les entreprises de télécommunication sont obligées de sécuriser leurs systèmes et leurs réseaux, au motif que ce secret serait bénéfique pour la cybersécurité. Ces personnes et ces groupes doivent adopter une vision plus large et examiner comment le secret qui entoure actuellement le projet de loi C-26 n'est pas compatible avec un système démocratique sain. Ce rapport montre comment le gouvernement pourrait modifier le projet de loi C-26 afin de mieux sécuriser le système de télécommunication du Canada tout en ajoutant dans la loi des dispositions relatives à la responsabilité et à la transparence. La sécurité peut et doit être alignée sur les principes démocratiques du Canada. Il appartient maintenant au gouvernement de modifier sa loi en conséquence.

Gary Miller et Christopher Parsons. « *Finding You: The Network Effect of Telecommunications Vulnerabilities for Location Disclosure* », rapport de recherche du Citizen Lab nº 171, Université de Toronto, octobre 2023.

Vous localiser

L'effet de réseau des vulnérabilités liées aux télécommunications permettant la divulgation de l'emplacement

Par Gary Miller et Christopher Parsons

26 OCTOBRE 2023
RAPPORT DE RECHERCHE Nº 171

munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY

UNIVERSITY OF TORONTO

THECITIZENLAB

Droit d'auteur

Version électronique publiée pour la première fois par Citizen Lab en 2023. Ce rapport peut être consulté à l'adresse https://citizenlab.ca/2023/10/finding-you-telecommunications-vulnerabilities-for-location-disclosure/.

Version du document : 1.1

- La figure 7 a été mise à jour par des caviardages supplémentaires.

À propos du Citizen Lab, Munk School of Global Affairs and Public Policy, Université de Toronto

Le Citizen Lab est un laboratoire interdisciplinaire établi à la Munk School of Global Affairs and Public Policy de l'Université de Toronto. Il met l'accent sur la recherche, le développement et les politiques stratégiques de haut niveau ainsi que l'engagement juridique au croisement des technologies de l'information et des communications, des droits de la personne et de la sécurité mondiale.

Nous utilisons une approche « mixte » pour la recherche combinant les méthodes des sciences politiques, du droit, de l'informatique et des études régionales. Nos recherches comprennent les enquêtes sur l'espionnage numérique contre la société civile; la documentation du filtrage d'Internet et d'autres technologies et pratiques qui ont une incidence sur la liberté d'expression en ligne; l'analyse des contrôles de protection de la vie privée, de la sécurité et de l'information des applications populaires; ainsi que l'examen des mécanismes de transparence et de responsabilisation pertinents pour la relation entre les entreprises et les organismes d'État concernant les données personnelles et d'autres activités de surveillance.

À propos des auteurs

Gary Miller a contribué à ce rapport alors qu'il était chercheur au Citizen Lab. Il est actuellement le fondateur de la Mobile Intelligence Alliance, un organisme de recherche sur la sécurité mobile à but non lucratif établi aux États-Unis. De plus, il était auparavant responsable de la sécurité des réseaux mobiles et il est considéré comme un expert de l'espionnage sur les réseaux mobiles. Il est titulaire d'un baccalauréat en économie de l'Université de Washington et collabore à des recherches journalistiques visant à enquêter sur l'espionnage sur les réseaux mobiles avec les principaux organes de presse mondiaux.

Christopher Parsons a contribué à ce rapport alors qu'il était associé de recherche principal au Citizen Lab du Munk School of Global Affairs and Public Policy de l'Université de Toronto. Il a obtenu son baccalauréat et sa maîtrise à l'Université de Guelph et son doctorat à l'Université de Victoria. Il est actuellement gestionnaire intérimaire de la politique technologique au Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario.

Remerciements

Nous tenons à remercier les organisations de la société civile, les journalistes d'investigation et les experts en sécurité des réseaux mobiles qui ont gracieusement accepté de nous faire part de leur point de vue et de transmettre des artefacts d'enquête dans le cadre de l'élaboration de ce rapport.

Nous tenons à remercier tout particulièrement Siena Anstis, Kate Robertson, Jakub Dalek, Celine Bauwens, Levi Meletti et Mohamed Ahmed pour leurs réflexions et leur expertise, leurs révisions et l'examen par les pairs de ce rapport.

Nous tenons également à remercier Mari Zhou pour son aide à la conception et à la publication, ainsi que Snigdha Basu pour son soutien en matière de communication. Ce rapport a été réalisé sous la supervision du professeur Ronald Deibert.

Corrections et questions

Veuillez envoyer toutes vos questions et corrections à : inquires@citizenlab.ca.

Citation suggérée

Gary Miller et Christopher Parsons. *Vous localiser : l'effet de réseau des vulnérabilités liées aux télécommunications permettant la divulgation de l'emplacement*, rapport de recherche du Citizen Lab nº 171, Université de Toronto, octobre 2023.

5

Encadrés de renseignements

Encadré 1 : Explication de l’identifiant de réseau IMSI	p. 5
Encadré 2 : Attaques de signalisation interprotocoles	p. 11
Encadré 3 : L’avenir de la location d’adresses globales	p. 25
Encadré 4 : Types de messages de signalisation équivalents utilisés pour demander l’emplacement d’un appareil mobile	p. 28

Table des matières

Introduction 1

1. Itinérance, cartes SIM et services 101 3

1.1. Du module d'identité d'abonné (SIM) aux services – créer la voie vers la surveillance des réseaux 4

2. Attaques de géolocalisation contre les réseaux de télécommunications 7

2.1 Attaques actives 7

2.1.1 Comment les acteurs accèdent-ils aux réseaux en vue de suivre la géolocalisation? 8

2.1.2. Vulnérabilités liées à la recherche dans le registre des abonnés locaux et à l'identification du réseau 10

2.1.3. Menaces nationales – innocence jusqu'à preuve du contraire 11

2.2 Attaques passives 13

2.2.1. Sondes de signalisation et outils de surveillance du réseau 13

2.2.2. Exemples de capture de paquets pour la surveillance de l'emplacement 14

3. Études de cas et statistiques 16

3.1 Étude de cas – l'Arabie saoudite suit les voyageurs aux États-Unis 16

3.2. Statistiques actuelles – suivi de la géolocalisation par rapport à d'autres types de menaces 19

4. Mesures incitatives permettant les attaques de géolocalisation 21

4.1. Moteurs économiques 22

4.2 Moteurs du secteur 22

4.3. Moteurs gouvernementaux 26

5. Suivi de la géolocalisation dans les réseaux 5G et mesures défensives non mises en œuvre 28

5.1. Amélioration de la confidentialité de l'identité de l'abonné 28

5.2. Amélioration de la sécurité de la signalisation internationale et de l'interconnexion 29

6. Conclusion 31

Introduction

Les renseignements recueillis par les réseaux mobiles et stockés sur ceux-ci peuvent constituer l'un des portraits les plus actuels et les plus complets de notre vie. Nos téléphones mobiles sont connectés à ces réseaux et révèlent nos comportements, nos données démographiques, nos communautés sociales, nos habitudes d'achat, nos habitudes de sommeil, nos lieux de résidence et de travail ainsi que l'historique de nos déplacements. Toutefois, dans leur ensemble, ces renseignements sont compromis par les vulnérabilités techniques des réseaux de communications mobiles. Ces vulnérabilités peuvent être utilisées pour exposer des renseignements personnels à de nombreux acteurs et sont étroitement liées à la manière dont les téléphones mobiles se connectent aux réseaux des opérateurs de téléphonie mobile lorsque nous voyageons. Plus précisément, ces vulnérabilités sont le plus souvent liées aux messages de signalisation envoyés entre les réseaux de télécommunications, qui exposent les téléphones à différents modes de divulgation de l'emplacement.

Les réseaux de télécommunications ont été conçus pour s'appuyer sur des connexions de signalisation privées, bien qu'ouvertes. Ces connexions permettent l'itinérance nationale et internationale, c'est-à-dire qu'un téléphone mobile peut passer en toute transparence d'un réseau à un autre. Les protocoles de signalisation utilisés à cette fin permettent également aux réseaux d'obtenir des renseignements sur l'utilisateur, par exemple si un numéro est actif, quels services sont disponibles, à quel réseau national l'utilisateur est inscrit et où il se trouve. Ces connexions et les protocoles de signalisation associés sont toutefois constamment ciblés et exploités par les acteurs de la surveillance, ce qui a pour effet d'exposer nos téléphones à de nombreuses méthodes de divulgation de l'emplacement.

La plupart des divulgations illégales de l'emplacement à l'aide de réseaux sont rendues possibles par la façon dont les réseaux de télécommunications mobiles interagissent entre eux. Les services de renseignement et de sécurité étrangers, ainsi que les sociétés de renseignement privées, tentent souvent d'obtenir des renseignements sur l'emplacement, tout comme les acteurs nationaux comme les organismes d'application de la loi. Notamment, les méthodes dont disposent les organismes d'application de la loi et les services de renseignement sont similaires à celles utilisées par les acteurs illégaux, et celles-ci leur permettent d'obtenir les renseignements de géolocalisation des personnes dans le plus grand secret. Dans le présent rapport, nous désignerons généralement tous ces acteurs par le terme « acteurs de la surveillance » pour refléter leur intérêt pour la surveillance de la géolocalisation des réseaux mobiles.

Malgré l'omniprésence des réseaux 4G dans le monde et l'expansion rapide de l'empreinte des réseaux 5G, il existe de nombreux appareils mobiles (et leurs propriétaires) qui utilisent les anciens réseaux 3G. C'est particulièrement le cas dans les régions de l'Europe de l'Est, du Moyen-Orient et de l'Afrique subsaharienne, où le taux de pénétration des abonnés 3G est de 55 % selon la GSMA[1], une organisation qui fournit des renseignements, des services et des lignes directrices aux membres du secteur de la téléphonie mobile. En outre, à la fin de 2021, la société britannique de renseignement sur le marché mobile Mobilesquared a estimé que seulement un quart des opérateurs de réseaux mobiles dans le monde ont déployé un pare-feu de signalisation[2] conçu pour nuire à la surveillance de la géolocalisation. Les initiés des télécommunications savent que les vulnérabilités du protocole de signalisation SS7 utilisé pour l'itinérance sur le réseau 3G ont permis l'élaboration de produits de surveillance commerciaux qui offrent à leurs opérateurs l'anonymat, de multiples points d'accès et vecteurs d'attaque, un réseau omniprésent et accessible dans le monde entier disposant d'une liste illimitée de cibles, ainsi que pratiquement aucun risque financier ou juridique.

Ce rapport présente une vue d'ensemble des menaces liées à la géolocalisation associées aux réseaux contemporains qui dépendent des protocoles utilisés par les opérateurs de réseaux 3G, 4G et 5G, ainsi que des preuves de la prolifération de ces menaces. La partie 1 présente le contexte historique de la divulgation non autorisée de l'emplacement dans les réseaux mobiles et l'importance des identifiants de cibles utilisés par les acteurs de la surveillance. La partie 2 explique comment les réseaux mobiles sont rendus vulnérables par les protocoles de signalisation utilisés pour l'itinérance internationale et de quelles manières les réseaux sont mis à la disposition des acteurs de la surveillance pour qu'ils puissent mener des attaques. Une vue d'ensemble de l'écosystème mobile jette les bases des détails techniques de la surveillance des réseaux nationaux et internationaux, alors que les vecteurs des techniques de surveillance active et passive ainsi que des preuves d'attaques montrent de quelle manière les renseignements de localisation sont présentés à l'acteur. La partie 3 détaille une étude de cas tirée d'un rapport de presse qui montre des preuves d'une surveillance généralisée parrainée par des États, suivie de données de renseignement sur les menaces qui révèlent des sources de réseau attribuées aux attaques détectées en 2023. Ces études de cas soulignent l'importance et la pertinence de ce type d'opérations de surveillance.

Les lacunes en matière de surveillance et de responsabilité de la sécurité des réseaux sont abordées dans la partie 4. Cette partie décrit les mesures incitatives et les moyens mis à la disposition des acteurs de la surveillance par les organisations sectorielles et les organismes de réglementation gouvernementaux. La partie 5 démontre que

[1] Kenechi Okeleke, Harry F. Ballon et James Joiner. (2023). *The Mobile Economy 2023*. https://data. gsmaintelligence.com/research/research/research-2023/the-mobile-economy- 2023.
[2] Mobileum, Mobilesquared. (2021). The State of the Signaling Firewall Landscape November 2021. https://www.mobilesquared.co.uk/wp- content/uploads/2023/04/Mobileum_Security-Research_Nov21-FINAL-VERSION.pdf.

l’adoption des technologies du réseau 5G n’atténuera pas les risques de surveillance futurs si les décideurs politiques ne prennent pas rapidement de mesures pour obliger les fournisseurs de télécommunications à adopter les dispositifs de sécurité disponibles concernant les normes et les équipements du réseau 5G. Si les décideurs politiques n’agissent pas rapidement, les acteurs de la surveillance pourraient continuer à s’en prendre aux utilisateurs de téléphones mobiles en suivant leur emplacement physique. Un tel avenir donne une image sombre de la protection de la vie privée des utilisateurs et doit être évité.

1. Itinérance, cartes SIM et services 101

Les utilisateurs de téléphones mobiles s'attendent à ce que leur téléphone fonctionne partout où ils voyagent au-delà des frontières de leur pays d'origine. Toutefois, c'est lorsque des personnes voyagent à l'étranger qu'elles sont les plus vulnérables au suivi de la géolocalisation à l'aide de réseaux.

Lorsqu'une personne voyageant à l'étranger possède un téléphone mobile, celui-ci continue à fonctionner en dehors de son réseau mobile d'origine (c.-à-d. l'opérateur de réseau mobile national auquel il est associé). Cette opération continue s'effectue par l'entremise d'une série d'interconnexions et d'ententes entre les opérateurs de réseaux du monde entier. Ces interconnexions et ces ententes sont souvent propres à chaque type de réseau (3G, 4G et 5G), et ces réseaux sont reliés par des protocoles de signalisation téléphonique mis au point depuis les années 1970 afin de former le système de signalisation n° 7 (réseau SS7), puis le réseau de technologie d'évolution à long terme (LTE ou 4G) qui utilise le protocole de signalisation Diameter.

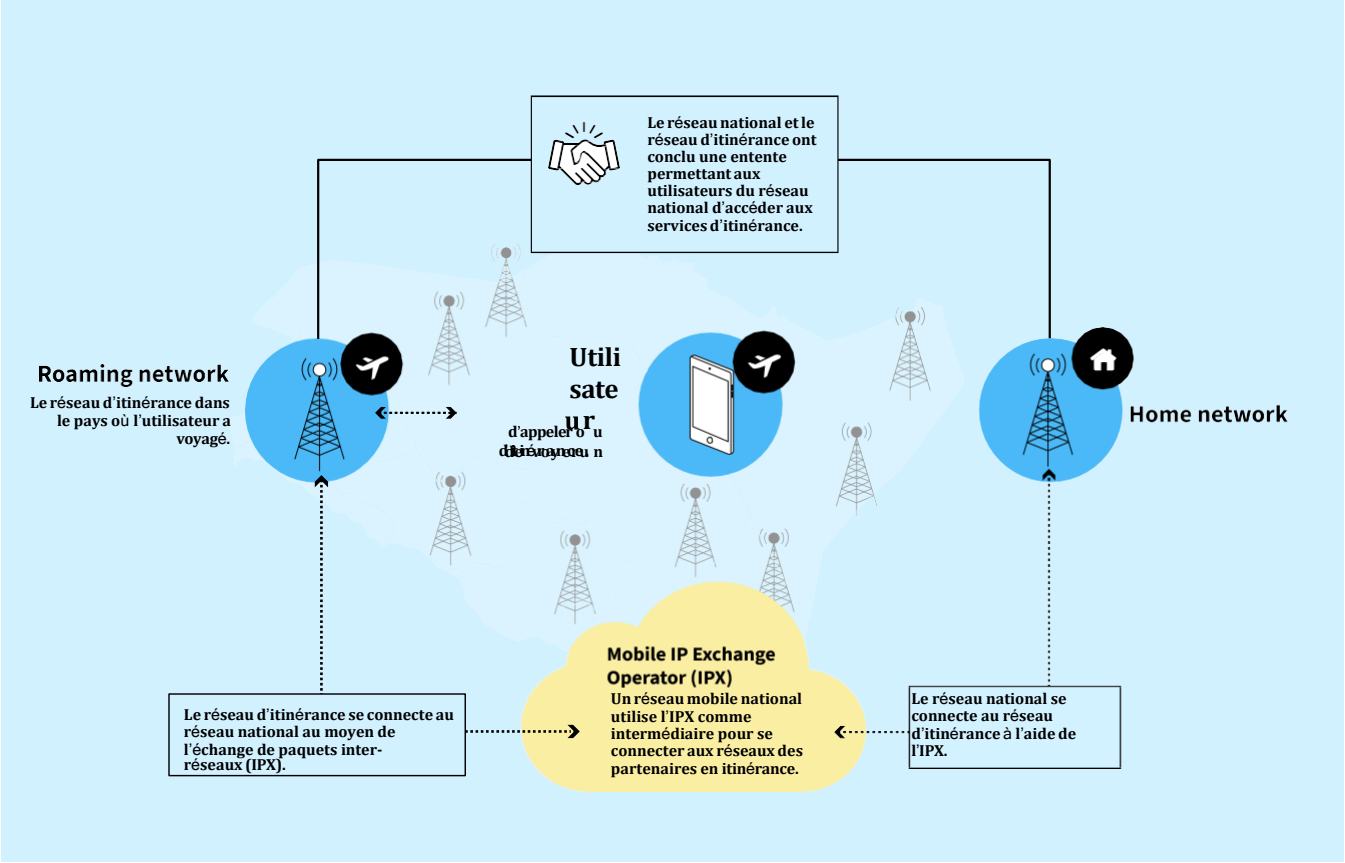


Figure 1 : Processus d'itinérance internationale.

En cas d'itinérance sur différents réseaux étrangers, ces derniers facturent différents tarifs pour les services téléphoniques, de données et de messagerie aux utilisateurs en itinérance sur leurs réseaux. Pour fournir ces services, les opérateurs de réseaux

concernés ouvrent leurs réseaux les uns aux autres afin qu'ils puissent interopérer. C'est cela qui permet aux utilisateurs de passer des appels, d'envoyer des messages texte ou d'utiliser des données de manière transparente lorsqu'ils sont en itinérance sur un réseau étranger.

D'une manière générale, les ententes d'itinérance, comme les informations incluses dans le cadre de la GSMA[3], sont utilisées pour établir les aspects commerciaux et opérationnels de l'envoi et de la réception de messages de signalisation pour l'échange de services entre les partenaires en itinérance du réseau. Les messages de signalisation sont des messages échangés entre les opérateurs qui sont utilisés pour authentifier et gérer la mobilité des utilisateurs. Sur le plan fonctionnel, les opérateurs utilisent les messages de signalisation pour établir et maintenir des sessions fournissant des services aux utilisateurs. Or, si les pratiques exemplaires en matière de sécurité indiquent que les opérateurs de réseaux mobiles doivent rejeter les messages envoyés par des partenaires qui ne sont pas en itinérance ou empêcher les messages abusifs d'exposer les utilisateurs au suivi de leur emplacement, ces pratiques ne sont ni obligatoires ni appliquées. Cet aspect volontaire de la sécurité des messages de signalisation échangés entre les opérateurs offre aux acteurs de la surveillance une voie d'entrée dans le réseau cible. En outre, les réseaux se connectent généralement à au moins deux opérateurs de réseaux par pays (et souvent beaucoup plus) afin de minimiser les coûts d'itinérance et de maximiser la résilience du réseau. Si ces connexions ouvertes sont une condition préalable à la mise en place de services d'itinérance, elles présentent également des risques pour le suivi de la géolocalisation.

1.1. *Du module d'identité d'abonné (SIM) aux services – créer la voie vers la surveillance des réseaux*

Pour comprendre les points de vulnérabilité que les acteurs de la surveillance exploitent pour suivre la géolocalisation des utilisateurs, il faut comprendre comment les utilisateurs sont identifiés de manière globale et unique sur les réseaux mobiles. Ces identifiants jouent un rôle essentiel dans le processus d'acheminement et de distribution des messages de suivi de la géolocalisation malveillants depuis le logiciel de l'acteur de la surveillance jusqu'au réseau du téléphone cible, ainsi que dans le renvoi de ces informations à l'acteur.

Le point de départ pour comprendre l'identité du téléphone d'un utilisateur est l'émission de la carte SIM par l'opérateur de réseau mobile. Alors que nous sommes habitués à insérer des cartes de plus en plus petites dans nos appareils mobiles, ces cartes matérielles sont rapidement remplacées par des cartes SIM embarquées qui s'appuient sur des logiciels. Les cartes SIM, qu'elles soient matérielles ou logicielles, utilisent une identité unique appelée identifiant de carte SIM. Les opérateurs de réseaux mobiles utilisent cet identifiant de carte SIM pour attribuer au téléphone une identité

[3] Les ententes d'itinérance internationale pertinentes de la GSMA sont les suivantes : AA.12, AA.13 et AA.14.

de réseau unique mondiale qui lui est propre, appelée identité internationale d'abonnement mobile (IMSI), lors de l'activation du service. Cet IMSI unique au monde et propre au réseau est l'élément crucial de la fourniture de services au téléphone à partir de n'importe quel réseau d'itinérance mondial. L'IMSI est également au cœur des méthodes de ciblage utilisées dans les opérations de suivi de la géolocalisation à partir de réseaux étrangers.

Une fois que la carte SIM normale ou embarquée a été attribuée au compte de l'utilisateur, un numéro de téléphone – désigné par le secteur des télécommunications sous le nom de Mobile Subscriber Integrated Services Digital Network Number (MSISDN) – est également associé à l'IMSI défini par l'opérateur de réseau. Ces renseignements combinés – le MSISDN et l'IMSI – sont intégrés dans les systèmes de fourniture de services, d'autorisation et d'authentification de l'opérateur de réseau. Un élément clé de ces systèmes est le Home Subscriber Service (HSS) ou le registre des abonnés locaux (HLR) du réseau 3G ou 4G, et le Unified Data Manager (UDM) du réseau 5G. Il s'agit de bases de données principales qui contiennent les règles d'autorisation des services associés au plan d'abonnement qu'une personne paie mensuellement ou au fur et à mesure de son utilisation.

Une fois la carte SIM attribuée et approvisionnée, l'appareil mobile peut communiquer avec le réseau de l'opérateur pour les appels téléphoniques, les messages textes et les données d'application qui peuvent être acheminées à l'échelle mondiale. C'est également à ce stade que des messages de signalisation malveillants peuvent être dirigés vers l'appareil, ce qui a pour effet d'exposer son emplacement.

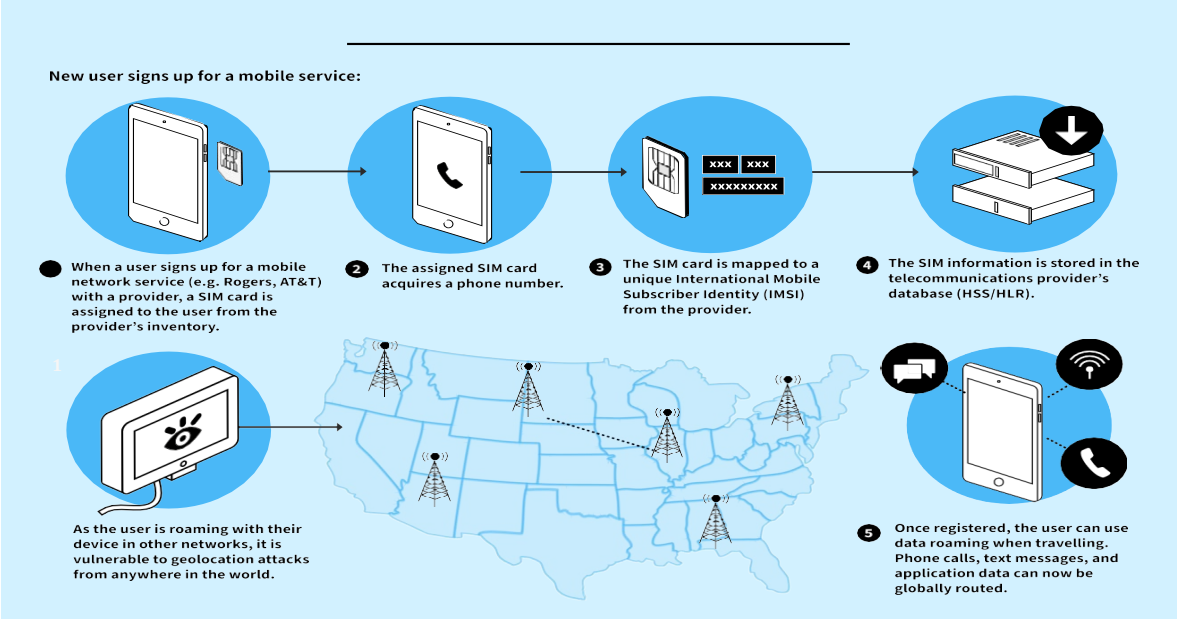


Figure 2 : Manière dont les identités mobiles sont fournies pour permettre les opérations de surveillance.

L'IMSI du téléphone cible est un élément d'information essentiel pour la surveillance, et

il est souvent utilisé dans la procédure initiale de l'opération pour localiser l'identifiant de cellule, qui est le numéro unique utilisé pour identifier la tour d'une station de base d'un réseau donné. L'identifiant de cellule peut ensuite être associé à un emplacement en utilisant l'un des nombreux services de base de données d'identifiant de cellule[4].

Encadré de renseignements 1 : Explication de l'identifiant de réseau IMSI

Les réseaux utilisent soit des identités de réseau 3G ou 4G, soit des identités de réseau 5G. Les réseaux 3G et 4G utilisent l'IMSI, qui comprend généralement 15 chiffres, comme dans l'exemple suivant :

- 222-333-444444444
- Les trois premiers chiffres (222) sont l'indicatif de pays de la station mobile (IPSM).
- Les deux ou trois chiffres suivants (333) correspondent au code de réseau mobile (CRM).
- Les chiffres restants (444444444) identifient la ligne de service complémentaire.

En revanche, les réseaux 5G disposent d'un Subscription Permanent Identifier (SUPI) au lieu d'un IMSI. Le SUPI est équivalent à l'IMSI afin d'assurer la compatibilité avec l'infrastructure de réseau 4G. Cette compatibilité est particulièrement importante, car le réseau 4G est à la base d'une grande partie de l'itinérance internationale actuelle du réseau 5G.

Le réseau 5G ajoute une fonctionnalité de sécurité appelée Subscription Concealed Identifier (SUCI), qui comporte un schéma de chiffrement pour empêcher la transmission ouverte de l'identité du réseau de l'utilisateur sur l'interface radio. Cela a pour effet de déjouer les acteurs de la surveillance qui se trouvent physiquement à proximité d'un appareil mobile et qui utilisent des outils comme des intercepteurs d'IMSI pour intercepter les communications radio afin de révéler le numéro IMSI d'un appareil. Les intercepteurs d'IMSI sont utilisés par divers acteurs, notamment les organismes d'application de la loi, les services de sécurité et les services de renseignement étrangers, ainsi que par des criminels, pour obtenir l'identité des utilisateurs du réseau à des fins de surveillance[5].

[4] De nombreux services commerciaux et publics de base de données d'identifiant de cellule sont disponibles : https://en.wikipedia.org/wiki/GSM_Cell_ID.
[5] Pour en savoir plus sur les intercepteurs d'IMSI, voir : Christopher Parsons et Tamir Israel. (2016). « Gone Opaque? An Analysis of Hypothetical IMSI Catcher Overuse in Canada ».
Citizen Lab et CIPPIC. Disponible à l'adresse suivante : https://citizenlab.ca/wp-content/uploads/2016/09/20160818-Report-Gone_Opaque.pdf.

2. Attaques de géolocalisation contre les réseaux de télécommunications

Ce rapport se concentre principalement sur les menaces de géolocalisation qui résultent du ciblage des réseaux de signalisation mobiles. Les acteurs de la surveillance peuvent utiliser des méthodes de surveillance actives ou passives pour obtenir des renseignements à partir des réseaux de signalisation mobiles, ce qui a pour effet d'exposer l'emplacement d'un utilisateur. Dans certains cas, ces acteurs peuvent combiner plusieurs méthodes pour atteindre cet objectif.

La distinction entre les deux approches est notable. La surveillance active nécessite qu'un acteur utilise un logiciel pour communiquer avec un réseau mobile en vue d'obtenir une réponse indiquant l'emplacement du téléphone cible, alors que la surveillance passive utilise un dispositif de collecte pour obtenir l'emplacement des téléphones directement à partir du réseau. En ce qui concerne les attaques actives, un réseau d'attaque utilise un logiciel pour envoyer des messages de signalisation spécialement conçus à des réseaux mobiles cibles vulnérables pour demander et obtenir l'emplacement actuel du téléphone cible. De telles attaques sont possibles lorsque les réseaux ciblés ne disposent pas de contrôles de sécurité correctement déployés ou configurés. De plus, un acteur qui accède à un réseau par l'intermédiaire d'une entente de location ne peut utiliser que des méthodes de surveillance active, à moins qu'il ait la capacité d'installer ou d'accéder d'une autre manière à des dispositifs de collecte passifs situés sur des réseaux ailleurs dans le monde.

Il est toutefois possible qu'un opérateur de réseau mobile ou d'autres acteurs soient contraints de procéder à une surveillance active et passive. Dans cette situation, l'opérateur de réseau peut être légalement contraint de faciliter la surveillance ou, au contraire, être la cible d'un initié hostile qui accède aux systèmes mobiles de manière illicite ou illégale. En outre, si un tiers accède à l'opérateur ou au fournisseur, par exemple en compromettant l'accès au réseau privé virtuel (RPV) des systèmes de réseau ciblés, il est possible qu'il soit en mesure d'obtenir des renseignements sur l'emplacement des utilisateurs ciblés, tant en mode actif que passif.

2.1 *Attaques actives*

Dans les cas des attaques actives, un acteur de la surveillance national ou étranger utilise un logiciel pour émettre des messages de signalisation destinés à l'identité du téléphone mobile de l'utilisateur cible (généralement l'IMSI) en manipulant les données de signalisation du réseau afin de déclencher une réponse du réseau d'origine de l'utilisateur cible. Ces mesures de surveillance peuvent être utilisées pour faciliter l'interception d'autres communications, la divulgation de l'emplacement ou l'interruption de services. Dans cette section, nous examinons comment les acteurs peuvent accéder aux réseaux afin de suivre la géolocalisation et nous analysons certaines des vulnérabilités qui peuvent être exploitées par les acteurs de la surveillance qui entreprennent des opérations de surveillance active.

2.1.1 Comment les acteurs accèdent-ils aux réseaux en vue de suivre la géolocalisation?

Le suivi de la géolocalisation à l'aide de réseaux nécessite le plus souvent trois éléments interconnectés :

1. un logiciel de surveillance spécialisé;
2. une adresse de signalisation utilisée pour acheminer des messages malveillants vers le ou les réseaux cibles afin d'extraire les données de géolocalisation de l'appareil ciblé;
3. une connectivité au SS7 du réseau mondial 3G, ainsi qu'au réseau Diameter 4G.

Ce réseau SS7 ou Diameter mondial est connu sous le nom d'échange de paquets inter-réseaux (IPX). L'objectif de l'IPX est de faciliter l'interconnexion entre les réseaux d'opérateurs de téléphonie mobile pour l'acheminement de messages de signalisation conformément aux définitions de services interexploitables et aux ententes commerciales convenues[6]. En outre, l'architecture de l'IPX stipule que seuls les fournisseurs de services qui sont des opérateurs de réseaux mobiles peuvent se connecter au réseau[7]. Par conséquent, les tiers qui ne font pas partie de la communauté des opérateurs de réseaux mobiles ne devraient pas être autorisés à se connecter et à envoyer des messages de signalisation mobiles, dont les vulnérabilités peuvent exposer les utilisateurs mobiles à une surveillance non autorisée de la géolocalisation.

Les connexions des acteurs de la surveillance au réseau de l'IPX se font généralement par l'entremise d'ententes commerciales secrètes conclues avec un opérateur de téléphonie mobile, un service de transit de l'IPX ou d'autres fournisseurs de services tiers, comme des fournisseurs de messagerie texte, des opérateurs de réseaux mobiles privés ou des fournisseurs de services de l'Internet des objets parrainés qui disposent de connexions à l'IPX. Si l'IPX est conçu pour permettre l'itinérance entre les réseaux de différents opérateurs, il peut également être utilisé de manière abusive pour permettre une surveillance subreptice de la géolocalisation. L'IPX est utilisé par plus de 750 réseaux mobiles[8] couvrant 195 pays dans le monde[9]. Diverses entreprises ayant des connexions à l'IPX peuvent accepter de se rendre explicitement complices ou ne pas dénoncer des acteurs de la surveillance qui exploitent les vulnérabilités des réseaux et des points d'interconnexion un à plusieurs pour faciliter le suivi de la géolocalisation.

Les entreprises de télécommunications mobiles peuvent « louer » l'accès à leurs réseaux. Cela a pour effet d'augmenter considérablement le nombre d'entreprises qui peuvent offrir un accès à l'IPX à des fins malveillantes. En outre, un locataire peut sous-louer l'accès à l'IPX, ce qui a pour effet de créer d'autres possibilités pour un

[6] Document IR.34 de la GSMA - Guidelines for IPX Provider Networks, Section 3 « IPX Network Architecture ».
[7] Document IR.34 de la GSMA, section 3.5.
[8] *About the GSMA - Represents the interests of mobile operators worldwide*. (12 juin 2023). About Us. https://www.gsma.com/aboutus
[9] *États Membres*. (n. d.). Organisation des Nations unies. https://www.un.org/fr/about-us/member-states

acteur de la surveillance d'utiliser une connexion à l'IPX tout en dissimulant son identité par l'entremise de plusieurs locations et sous-locations.

Plus précisément, les opérateurs de télécommunications d'un pays donné demandent et obtiennent des plages de numéros de téléphone en vrac selon un plan de numérotage administré par leur organisme national de réglementation en matière de télécommunications. Ces plages sont souvent utilisées à des fins diverses comme les téléphones fixes, les numéros mobiles ou les numéros gratuits. Une fois que l'opérateur s'est vu attribuer des numéros, il peut utiliser et attribuer une partie des numéros comme adresses, connues sous le nom d'adresses globales, aux équipements de son réseau qui sont nécessaires pour rendre opérationnelle l'itinérance nationale et internationale avec d'autres partenaires du réseau. Il s'agit d'équipements comme l'enregistreur de localisation de visiteurs, le registre des abonnés locaux ainsi que d'autres équipements du réseau central.

Les exploitants peuvent également céder ces adresses globales à des tiers locataires. Un locataire malveillant peut :

- configurer un logiciel de surveillance afin d'utiliser les adresses globales louées en vue d'effectuer sa propre surveillance;
- utiliser les adresses louées dans une solution hébergée dans le nuage pour fournir un service de surveillance commerciale;
- cloisonner davantage les adresses globales pour les sous-louer à d'autres acteurs de la surveillance.

Notamment, un acteur de la surveillance pourrait louer des adresses globales auprès d'un seul opérateur de télécommunications ou d'une série d'opérateurs issus de différentes administrations. Dans ce dernier cas, l'acteur de la surveillance peut alterner les attaques entre les différentes adresses globales sous-louées, soit pour essayer d'éviter la détection, soit pour augmenter les chances de réussite de l'opération si les attaques provenant de certaines adresses globales sous-louées sont bloquées par les pare-feu du réseau.

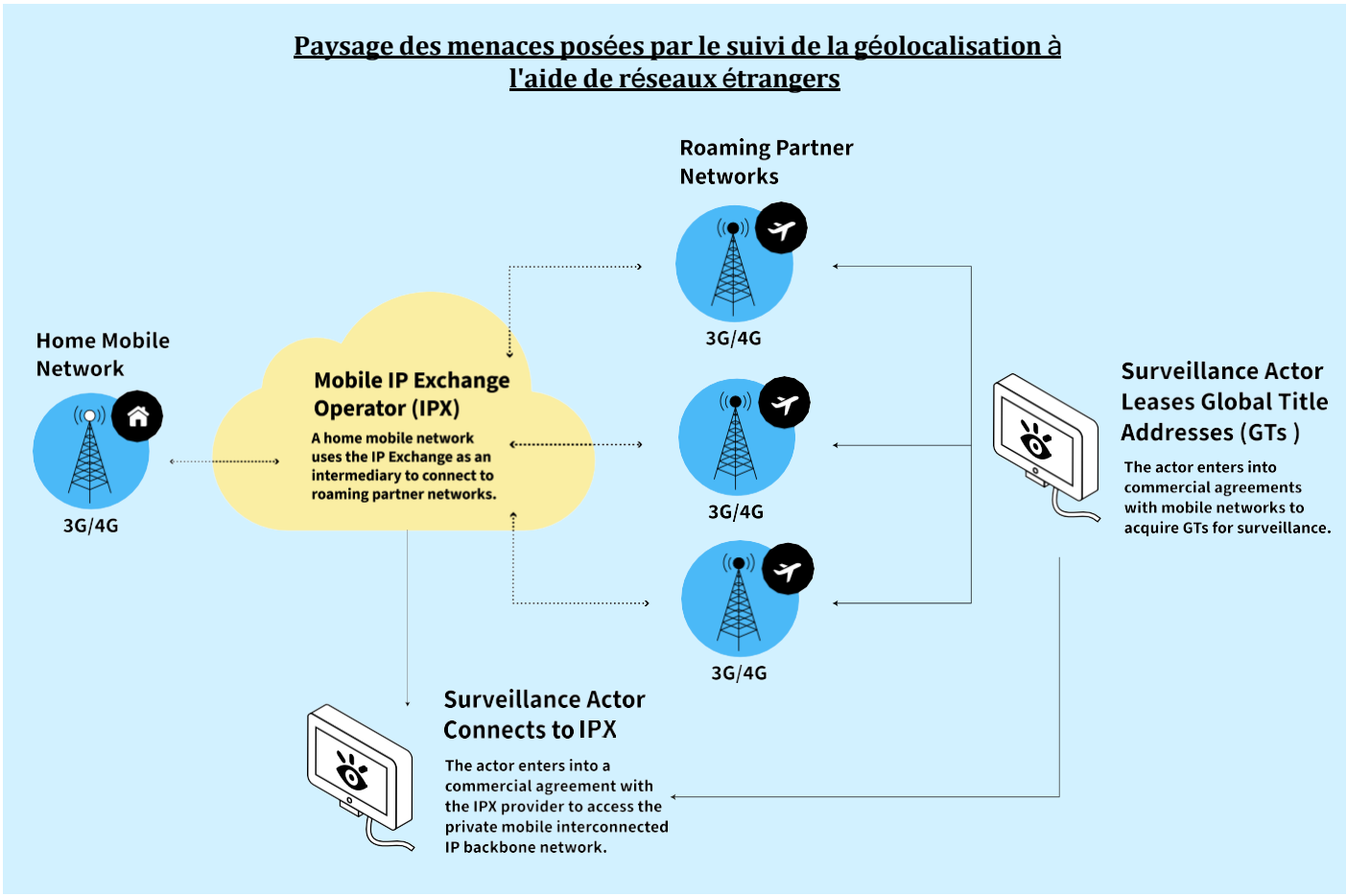


Figure 3 : Paysage des menaces posées par le suivi de la géolocalisation à l'aide de réseaux étrangers.

Les opérations des acteurs de la surveillance sont rendues possibles en raison du modèle en étoile sur lequel repose l'IPX pour faciliter l'itinérance internationale vers d'autres réseaux. Dans ce modèle, l'IPX est responsable d'acheminer et d'envoyer les messages entre le réseau d'origine et le réseau d'itinérance, mais il connecte également d'autres fournisseurs de services, comme ceux qui envoient des messages textes et les fournisseurs de services à valeur ajoutée (SVA) qui proposent des services de consultation de numéros de téléphone mobile et de recherche dans le registre des abonnés locaux, de mobilité de l'Internet des objets ou de suivi de véhicules. Le modèle connecte aussi des opérateurs de réseaux virtuels mobiles (ORVM) hébergés qui ont conclu des ententes avec les IPX. Le résultat final est qu'un ensemble de tiers ont un accès mondial aux réseaux des opérateurs de réseaux mobiles, bien qu'ils n'aient aucune relation commerciale directe avec les réseaux étrangers auxquels ils peuvent se connecter.

2.1.2. Vulnérabilités liées à la recherche dans le registre des abonnés locaux et à l'identification du réseau

L'une des méthodes utilisées pour révéler les renseignements de réseau associés à un numéro de téléphone mobile consiste à utiliser un service commercial de recherche dans le registre des abonnés locaux. Ce type de service commercial permet aux organisations qui ne sont pas des opérateurs de télécommunications de vérifier l'état d'un numéro de téléphone mobile en utilisant le réseau SS7 sans avoir à conclure d'entente avec un opérateur de téléphonie mobile. Dans ce type de situation, un acteur de la surveillance paierait une redevance au fournisseur de service de recherche dans le registre des abonnés locaux en fonction du nombre de consultations de numéros de téléphone mobile qu'il soumet au service.

Après avoir reçu les numéros de téléphone à rechercher, le service de recherche émet une requête en utilisant le réseau SS7 et récupère une réponse du réseau. Cette réponse permet de savoir si le numéro ciblé est valide et s'il est activement enregistré sur un réseau mobile. Si le numéro est valide et actif, la réponse indiquera également le réseau auquel il est rattaché et s'il est en état d'itinérance. Les renseignements clés de la requête renverront l'IMSI cible associée au MSISDN et l'adresse de l'enregistreur de localisation de visiteurs du réseau d'itinérance associée au téléphone cible. En disposant de ces renseignements, l'acteur peut émettre des demandes de suivi de la géolocalisation en connaissant précisément le pays, le réseau et l'enregistreur de localisation de visiteurs utilisés par le téléphone cible.

Par ailleurs, si l'acteur de la surveillance a déjà accès au réseau SS7 dans le cadre d'une entente de location conclue avec un réseau mobile, il peut effectuer la même recherche dans le registre des abonnés locaux, mais sans dépendre d'un service commercial de recherche intermédiaire.

Encadré 2 : Attaques de signalisation interprotocoles

Les vulnérabilités du réseau 3G sont particulièrement graves en raison de la généralisation des ententes de location d'adresses[10], bien que les réseaux 4G puissent également attribuer et louer des adresses du nœud avec le même effet. Dans certains cas, les acteurs utilisent les réseaux 3G et 4G pour cibler simultanément le même utilisateur; c'est ce que nous appelons les « attaques interprotocoles

L'effet est double : premièrement, les acteurs de la surveillance peuvent directement demander et recevoir des renseignements de géolocalisation associés à l'IMSI de l'appareil ciblé. Deuxièmement, comme l'adresse source doit être indiquée dans les messages de signalisation afin de renvoyer le message à la source, elle laisse également

[10] Crofton Black, Stephanie Kirchgaessner et Dan Sabbagh. (16 décembre 2020). Israeli spy firm suspected of accessing global telecoms via Channel Islands. *The Guardian.* https://www.theguardian. com/world/2020/dec/16/israeli-spy-firm-suspected-accessing-global-telecoms-channel-islands

une empreinte de l'attaque. Cela signifie que les pare-feu de réseau exploités par les fournisseurs de télécommunications peuvent surveiller le réseau à partir duquel les messages de recherche dans le registre des abonnés locaux et de suivi de l'emplacement ont été envoyés.

2.1.3. Menaces nationales – innocence jusqu'à preuve du contraire

Le risque de menaces liées à la divulgation de l'emplacement à l'échelle nationale peut parfois être plus préoccupant que celui provenant de sources étrangères lorsque des tiers sont autorisés par les opérateurs de téléphonie mobile à se connecter à leur réseau. Ces problèmes peuvent être particulièrement préoccupants dans les pays où l'État de droit est faible et où les organismes d'application de la loi ou de sécurité nationaux peuvent abuser de cet accès, ou encore lorsque des institutions étatiques, même dans les pays où l'État de droit est élevé, choisissent d'exploiter les vulnérabilités des réseaux de télécommunications mondiaux au lieu de s'efforcer de les sécuriser et de les défendre activement.

Les pare-feu de signalisation utilisés par les fournisseurs de télécommunications pour empêcher les opérateurs étrangers ou les acteurs de la surveillance de demander de manière illicite l'emplacement de leurs abonnés peuvent être moins efficaces contre les menaces nationales. Plus précisément, si les pare-feu de signalisation ne sont pas configurés de manière appropriée, les attaques provenant du même réseau peuvent ne pas être détectées parce que l'activité – qui provient du réseau de l'opérateur – est censée être fiable, et qu'il est possible que les réseaux ne filtrent et ne bloquent pas les messages de suivi de l'emplacement provenant de sources situées dans leur propre réseau. Il en résulte que les tiers qui se voient accorder des adresses de réseaux 3G et 4G dans les réseaux nationaux peuvent parfois avoir la capacité de géolocaliser les utilisateurs silencieusement, sans être remarqués ou filtrés par le fournisseur de télécommunications.

Dans certains pays, les organismes d'application de la loi ou de sécurité sont autorisés à se connecter directement au réseau du pays d'origine afin de pouvoir envoyer des messages de suivi de l'emplacement à l'échelle nationale et internationale. Dans ce cas, les messages de suivi de l'emplacement envoyés à partir de l'adresse du réseau de l'opérateur national peuvent être autorisés à utiliser les réseaux de ce pays pour suivre l'emplacement d'utilisateurs dans d'autres réseaux à l'intérieur du pays ou dans des réseaux étrangers.

Un exemple des risques associés à l'intervention d'un État auprès d'un opérateur de télécommunications peut être démontré par des données de renseignement sur les menaces récentes, qui montrent des attaques de suivi de l'emplacement effectuées par l'opérateur de téléphonie mobile vietnamien Gmobile, détenu par GTel Mobile, qui

appartient lui-même au ministère vietnamien de la Sécurité publique[11]. Ayant pour rôle d'enquêter sur les questions de sécurité nationale, le ministère de la Sécurité publique a été accusé de diverses violations des droits de la personne, ainsi que de censure et de restrictions de la liberté d'Internet[12].

De novembre 2022 à juin 2023, cinq adresses globales SS7 attribuées à GTel et à Gmobile ont été vues en train de mener des opérations de surveillance ciblant des utilisateurs de téléphones mobiles dans des pays africains en s'appuyant sur des résultats de télémétrie des menaces provenant de pare-feu déployés dans plusieurs réseaux mobiles. Parmi les tentatives de surveillance observées à partir des données, la majorité des messages de signalisation malveillants étaient associés à la divulgation de l'emplacement[13].

Ces conclusions sont tirées des données présentées à la figure 4 et issues du projet Mobile Surveillance Monitor[14], qui suit les activités de surveillance à partir de sources de données de renseignement sur les menaces. Ces données ont révélé que les menaces ont été détectées et bloquées par les pare-feu de réseau de signalisation de Cellusys[15] déployés dans les réseaux des opérateurs de téléphonie mobile. Les graphiques montrent la distribution des différents types d'opérations de messages SS7 utilisés par Gmobile pour tenter de suivre l'emplacement des utilisateurs à partir de chacune des adresses globales sources qui ont été détectées comme ciblant les téléphones des réseaux mobiles africains. Comme le montre la figure, différents types de messages ont été utilisés pour tenter les opérations de suivi de l'emplacement. La technique consistant à utiliser différents types de messages pour suivre l'emplacement est couramment utilisée pour tenter de contourner un pare-feu de signalisation ou pour augmenter les chances de réussite de la géolocalisation des appareils ciblés.

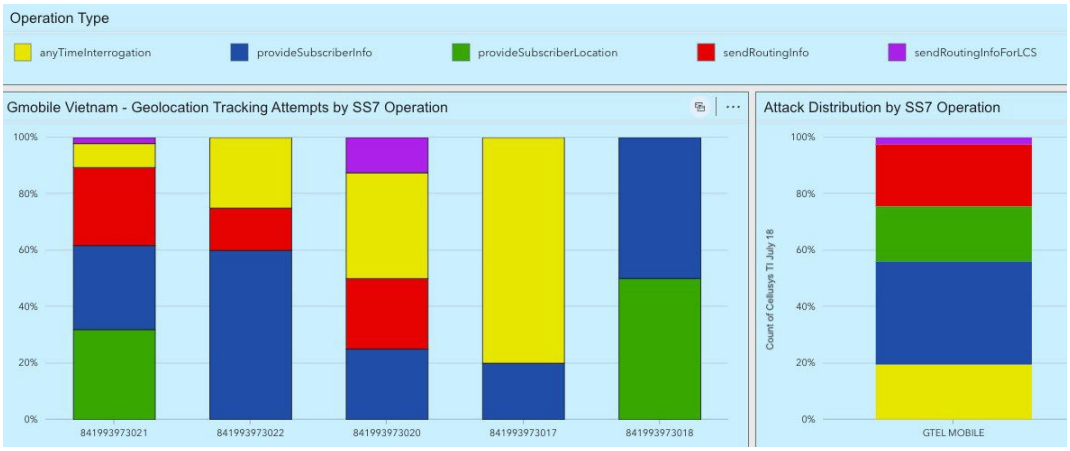


Figure 4 : Types de messages SS7 utilisés par les adresses globales de l'entreprise vietnamienne Gmobile pour suivre la géolocalisation des utilisateurs.

[11] Entreprises vietnamiennes relevant du ministère de la Sécurité publique (MPS) : https://www.trade. gov/country-commercial-guides/vietnam-defense-and-security-sector
[12] 2022 Country Reports on Human Rights Practices: Vietnam (2022). Département d'État des États-Unis. https:// www.state.gov/reports/2022-country-reports-on-human-rights- practices/vietnam/
[13] Les données télémétriques de signalisation mobile proviennent de Cellusys et ont été analysées par Mobile Surveillance Monitor, un projet de renseignement sur les menaces géré par l'auteur Gary Miller.
[14] Tracking Digital Privacy Threats With Intelligence : https://surveillancemonitor.org
[15] Cellusys : https://www.cellusys.com

Gmobile est le seul réseau vietnamien à avoir effectué une surveillance SS7 ciblée au cours de cette période. Étant donné que le ministère de la Sécurité publique est propriétaire de l'opérateur de télécommunications, le ciblage a été effectué soit en connaissance de cause ou avec l'autorisation du ministère, soit en dépit du fait que l'opérateur de télécommunications est la propriété de l'État.

2.2 *Attaques passives*

Les attaques de localisation passives surviennent lorsqu'un réseau mobile national ou étranger collecte des renseignements sur l'utilisation ou sur l'emplacement associés à un téléphone mobile cible à l'aide de dispositifs de collecte installés dans le réseau. Les dispositifs recueillent et transmettent les données de communication et de réseau à un entrepôt de données ou à une installation de commande et de contrôle gérée par l'acteur de la surveillance.

2.2.1. Sondes de signalisation et outils de surveillance du réseau

Les sondes de signalisation et les outils de surveillance du réseau sont généralement placés dans les réseaux mobiles par les entreprises de télécommunications à des fins opérationnelles, comme le dépannage des réseaux. Ces dispositifs sont généralement placés à des endroits stratégiques du réseau afin de capturer le trafic réseau à l'échelle de l'utilisateur lorsqu'il passe d'un équipement du réseau à un autre. Ce processus nécessite que les sondes ingèrent des messages de signalisation bruts ou du trafic IP envoyé au sein d'un réseau national ou entre le réseau national et les réseaux des partenaires en itinérance où l'utilisateur est actuellement enregistré. Les échanges entre les réseaux sont recueillis et fournis à une plateforme en amont où ils sont traités et stockés. Une fois dans cette plateforme, les messages peuvent être agrégés pour créer des indicateurs de rendement clé (IRC) opérationnels aux fins d'analyse ou ils peuvent être enregistrés dans un format permettant de retracer l'activité de l'utilisateur, à l'aide d'un outil de capture de paquets ou d'analyse comme Wireshark[16]. Comme les sondes interceptent les informations de signalisation de l'utilisateur, elles peuvent suivre l'emplacement général d'un téléphone mobile, même si celui-ci n'est pas activement engagé dans un appel vocal ou dans une session de données.

2.2.2. Exemples de capture de paquets pour la surveillance de l'emplacement

Les figures suivantes (5 et 6) montrent des exemples de captures de paquets effectuées à partir d'un réseau mobile. Les captures sont dérivées d'une source anonyme afin de démontrer comment les acteurs de la surveillance peuvent extraire des données de

[16] Wireshark est un outil d'analyse de réseau très répandu, qui permet de lire et d'interpréter le trafic réseau capturé.

localisation à partir de réseaux de signalisation mobiles. Les deux premiers types de messages affichés sont Provide Subscriber Location (PSL) et Provide Subscriber Information (PSI). Il ne s'agit là que de deux exemples parmi les nombreux types d'opérations de suivi de l'emplacement. Le dernier exemple de la figure 7 montre comment un dispositif passif capturant une session de données d'un utilisateur sur le réseau mobile pourrait révéler l'emplacement du téléphone.

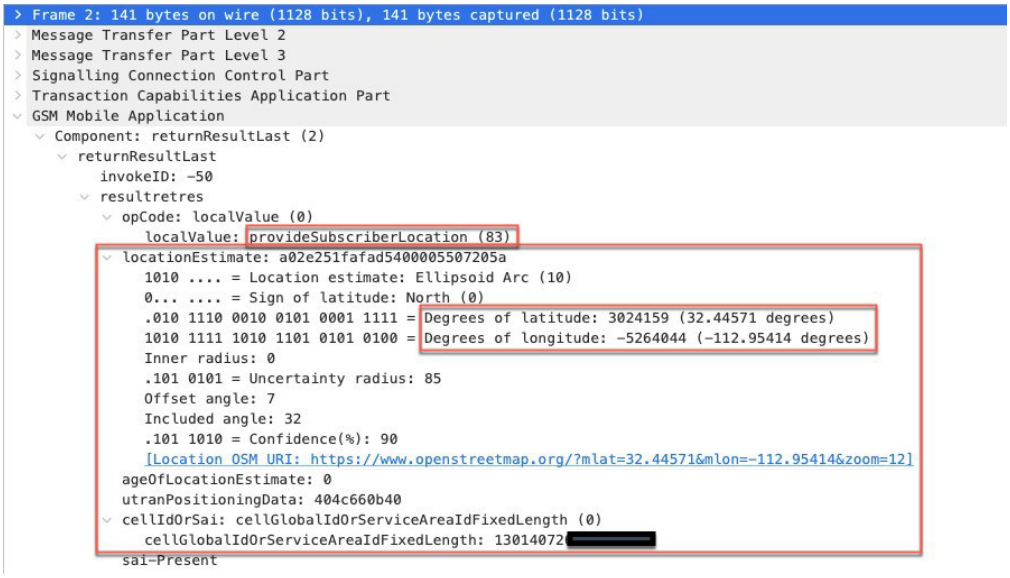


Figure 5 : Exemple de suivi actif de l'emplacement à l'aide d'un message de signalisation PSL.

Dans la réponse au message PSL, les coordonnées GPS de latitude et de longitude de l'emplacement du téléphone sont divulguées dans le message renvoyé à l'adresse globale source, qui pourrait être exploitée par un acteur de la surveillance.

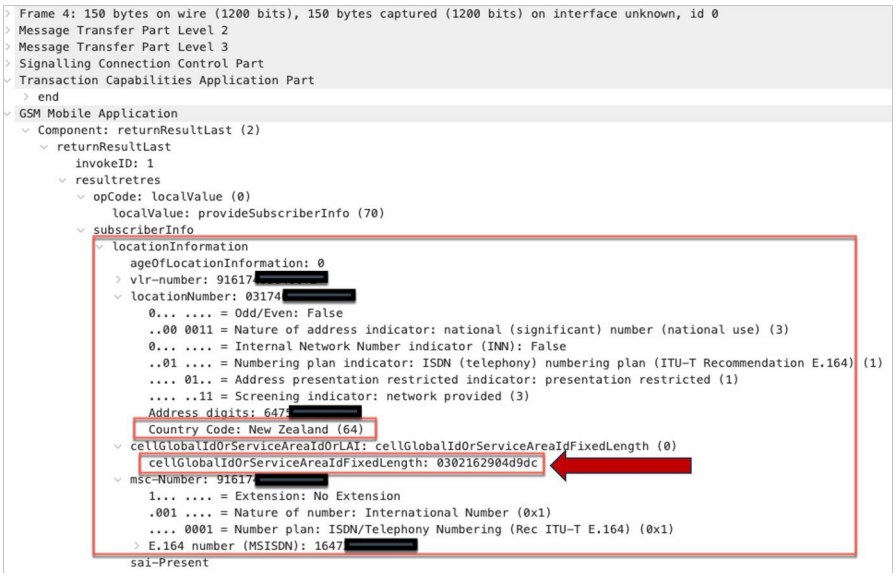


Figure 6 : Exemple de suivi actif de l'emplacement à l'aide d'un message de signalisation PSI.

Dans la figure 6, un utilisateur en itinérance internationale dont le numéro de téléphone est établi à Toronto, au Canada, a été localisé par un message PSI alors qu'il utilisait

un réseau mobile en Nouvelle-Zélande. Cela a pour effet d'exposer l'emplacement du téléphone à l'échelle de l'identifiant de cellule. Les informations de localisation de l'utilisateur sont codées dans le paramètre cellGlobalIdOrServiceAreaIdFixedLength[17], qui est une chaîne d'octets comprenant l'IPSM actuel, le CRM, l'indicatif de zone de localisation[18] et l'identifiant de cellule. En effet, avec la chaîne d'octets en main, il est possible de géolocaliser l'appareil mobile.

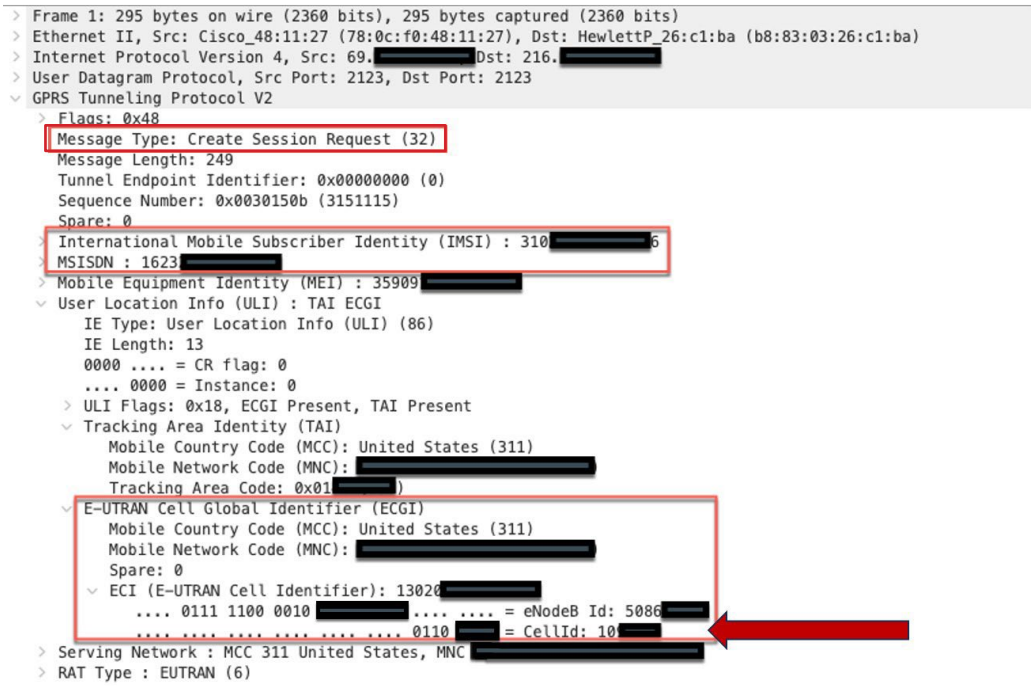


Figure 7 : Emplacement de l'utilisateur et informations identifiables révélées lors des sessions de données mobiles (remarque : l'image a été mise à jour par des caviardages supplémentaires le 8 novembre 2023).

La capture de paquets présentée à la figure 7 indique que l'IMSI, le MSISDN et l'identité internationale d'équipement mobile d'un utilisateur mobile ont été révélés lors d'une tentative d'établissement d'une session de données, comme l'indique le message

« Create Session Request » du protocole de tunnellisation GPRS. La demande spécifie les informations de localisation de l'utilisateur, qui fournissent les renseignements nécessaires pour dériver l'emplacement mondial actuel de l'utilisateur, y compris le pays, l'opérateur de réseau mobile, la station de base et l'identifiant de cellule de l'utilisateur enregistré.

[17] Défini dans le document de normes mobiles 3GPP TS 23.003.
[18] Défini dans le document de normes mobiles 3GPP TS 24.008.

3. Études de cas et statistiques

L'étude de cas suivante révèle une tactique utilisée pour localiser des utilisateurs ciblés sur un réseau mobile. Elle montre comment un acteur de la surveillance parrainé par un État peut surveiller l'emplacement des téléphones de voyageurs internationaux en dehors de leur pays.

3.1 Étude de cas – l'Arabie saoudite suit les voyageurs aux États-Unis

The Guardian a révélé un exemple particulièrement remarquable de suivi de la géolocalisation parrainé par un État lorsqu'il a dévoilé des activités vraisemblablement menées par le royaume d'Arabie saoudite. Le média a rapporté que le pays aurait suivi les mouvements d'individus qui se déplaçaient d'Arabie saoudite aux États-Unis et qui étaient abonnés à des fournisseurs de télécommunications saoudiens en exploitant le réseau SS7[19].

Cette surveillance a été effectuée par l'envoi d'un grand nombre de messages Provide Subscriber Information (PSI) ciblant les appareils mobiles en itinérance aux États-Unis. Ces messages ont été émis par les trois plus grands opérateurs de téléphonie mobile d'Arabie saoudite, Saudi Telecom Company (STC), Mobily (Etisalat) et Zain KSA. Lorsqu'un réseau reçoit un message PSI, il répond en indiquant l'identifiant de cellule de l'appareil ciblé. Cet identifiant permet d'identifier de manière unique la station de base à laquelle l'appareil est enregistré à un moment donné. En effet, le réseau des États-Unis a traité les messages PSI, ce qui a eu pour effet d'exposer l'emplacement des téléphones aux États-Unis aux acteurs de la surveillance en Arabie saoudite. Les acteurs de la surveillance peuvent relier l'identifiant de cellule à une base de données d'identifiant de cellule pour déterminer les coordonnées GPS de celui-ci. Dans l'ensemble, tous les messages PSI autorisés sur le réseau ont donc servi à déterminer l'emplacement des individus au moment de la surveillance, ainsi que la durée des voyages des personnes ciblées aux États-Unis. Cela aurait eu pour effet de révéler les habitudes de mobilité des résidents de l'Arabie saoudite aux États-Unis. Cette opération est décrite dans la figure ci-dessous.

[19] Stephanie Kirchgaessner. (2020). Revealed: Saudis suspected of phone spying campaign in US. *The Guardian.* https://www.theguardian.com/world/2020/mar/29/revealed-saudis- suspected-of-phone- spying-campaign-in-us

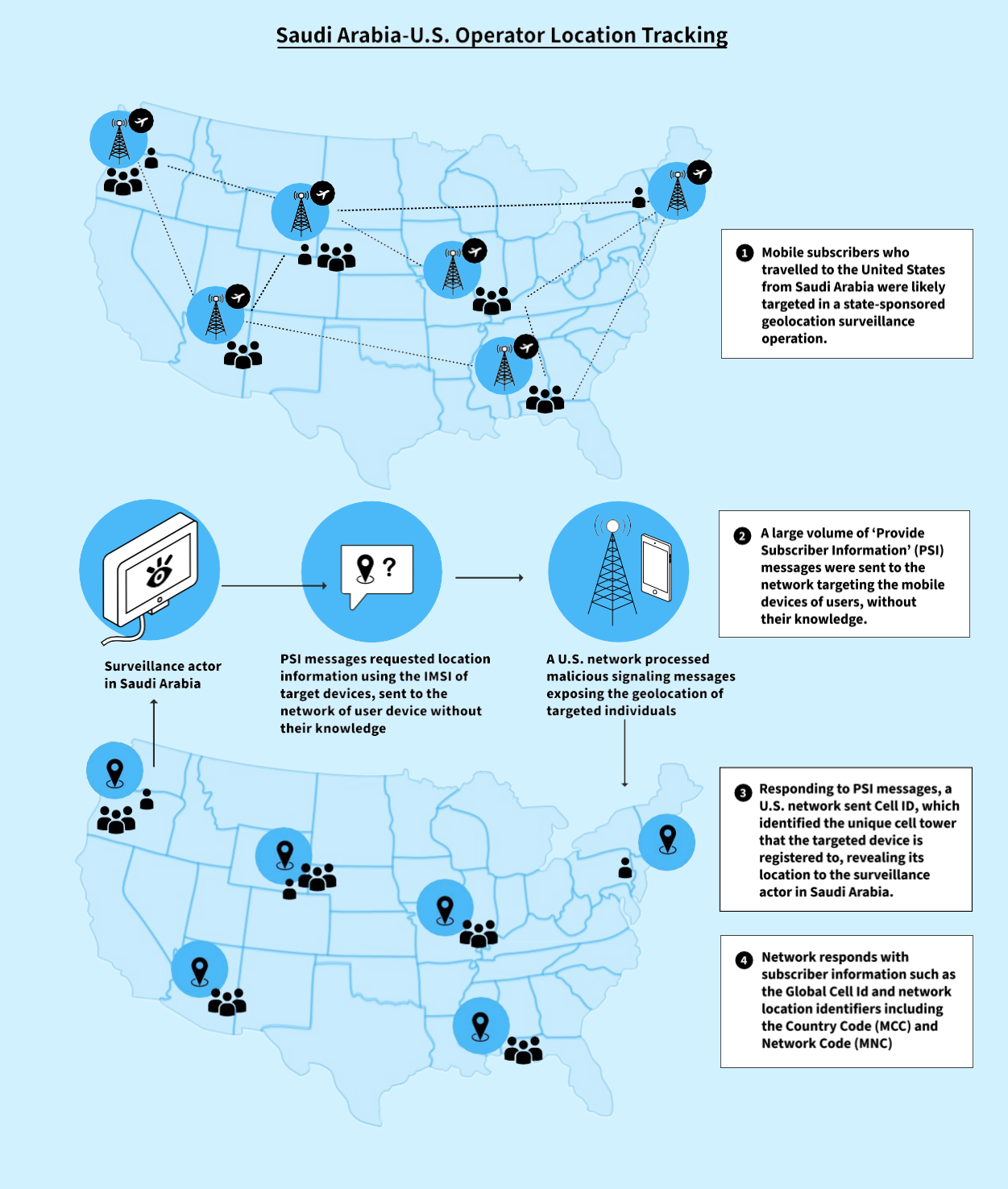


Figure 8 : Suivi de l'emplacement de voyageurs saoudiens aux États-Unis.

L'article note que ces messages ont été envoyés à chaque téléphone saoudien ciblé plusieurs fois par heure et que cette activité anormale ne pouvait être expliquée ou justifiée par les procédures normales de fonctionnement du réseau.

Les échanges présentés dans le tableau 1 ont été agrégés sur la période d'octobre à décembre 2019. Ceux-ci révèlent le nombre de messages PSI envoyés par les trois opérateurs de téléphonie mobile d'Arabie saoudite à un réseau mobile des États-Unis

particulier, en ciblant les IMSI des téléphones saoudiens en itinérance sur ce réseau. Le nombre total d'IMSI correspond au nombre de téléphones uniques du partenaire en itinérance vus dans le réseau au cours de la même période[20].

Nom du partenaire en itinérance	IPSM, CRM	Échanges de PSI	Total des IMSI
Saudi Telecom Company (STC)-SAUAJ	420.01	4 741 919	32 536
Etihad Etisalat Mobily-SAUET	420.03	2 821 709	11 362
Zain KSA-SAUZN	420.04	417 412	3 658
Total		7 981 040	47 556

Tableau 1 : Suivi de l'emplacement de l'Arabie saoudite vers un opérateur de téléphonie mobile aux États-Unis – octobre à décembre 2019

Les données du tableau 2 calculent le nombre total de messages de suivi reçus des opérateurs de réseau d'Arabie saoudite au cours d'une période de 24 heures, divisée en segments d'une heure. Selon ces statistiques, chaque téléphone mobile a été géolocalisé environ toutes les 11 minutes.

Date de l'événement	Échanges de PSI	Total des IMSI	IMSI réussis	Demandes par téléphone
29 nov. 2019 à minuit	1750	265	262	6.60
29 nov. 2019 à 1 h	1469	242	241	6.07
29 nov. 2019 à 2 h	1491	223	221	6.69
29 nov. 2019 à 3 h	1469	214	212	6.86
29 nov. 2019 à 4 h	1199	209	207	5.74
29 nov. 2019 à 5 h	1441	250	247	5.76
29 nov. 2019 à 6 h	1231	222	222	5.55
29 nov. 2019 à 7 h	1249	270	266	4.63
29 nov. 2019 à 8 h	1125	229	229	4.91
29 nov. 2019 à 9 h	1523	306	303	4.98
29 nov. 2019 à 10 h	1260	290	288	4.34
29 nov. 2019 à 11 h	1358	304	304	4.47
29 nov. 2019 à 12 h	1325	298	297	4.45
29 nov. 2019 à 13 h	1677	368	367	4.56
29 nov. 2019 à 14 h	1567	380	378	4.12
29 nov. 2019 à 15 h	1684	406	403	4.15
29 nov. 2019 à 16 h	2191	443	439	4.95
29 nov. 2019 à 17 h	2560	507	504	5.05
29 nov. 2019 à 18 h	2426	484	484	5.01
29 nov. 2019 à 19 h	2368	467	465	5.07
29 nov. 2019 à 20 h	2363	422	417	5.60
29 nov. 2019 à 21 h	2196	407	402	5.40
29 nov. 2019 à 22 h	2397	409	400	5.86
29 nov. 2019 à 23 h	2387	354	348	6.74

Tableau 2 : Arabie saoudite : suivi de l'emplacement de PSI au cours d'une seule journée ciblant un opérateur de téléphonie mobile des États-Unis – 29 novembre 2019

[20] Le tableau 1 indique le nombre total d'IMSI uniques observés sur une période de trois mois. Le tableau 2 indique le nombre total d'IMSI uniques observés chaque heure.

En général, les messages de signalisation PSI provenant de réseaux étrangers sont bloqués par un pare-feu de réseau. Cette mesure défensive vise à empêcher les recherches de géolocalisation non autorisées. Toutefois, cela ne s'est pas produit dans cette étude de cas, car les téléphones mobiles ciblés étaient en itinérance sur un réseau des États-Unis par l'entremise de leurs réseaux nationaux respectifs en Arabie saoudite. En revanche, si les messages avaient été envoyés à partir d'un réseau étranger à un abonné n'appartenant pas à ce même réseau, comme si un opérateur britannique avait interrogé les mêmes utilisateurs saoudiens alors qu'ils se déplaçaient sur des réseaux américains, ces messages auraient dû être bloqués.

La raison de la surveillance généralisée décrite dans cette étude de cas n'est pas tout à fait claire. Nous pouvons néanmoins conclure qu'il s'agissait probablement d'une activité parrainée par l'État et destinée à déterminer les habitudes de mobilité des utilisateurs saoudiens qui voyageaient aux États-Unis.

3.2. Statistiques actuelles – suivi de la géolocalisation par rapport à d'autres types de menaces

L'absence de réglementation efficace, de responsabilité et de transparence a été bénéfique pour la surveillance de la géolocalisation à l'aide de réseaux. Les figures ci-dessous fournissent un contexte et une vue d'ensemble du paysage mondial des réseaux mobiles.

Alors que certains experts du secteur pensent que les opérateurs de téléphonie mobile utilisent des pare-feu pour bloquer la majorité des suivis de la géolocalisation, ce qui a pour effet de limiter l'utilité des méthodes de surveillance SS7 habituelles, les statistiques fournies par Mobile Surveillance Monitor indiquent que la divulgation de l'emplacement est de loin le type de menace le plus répandu sur les réseaux.

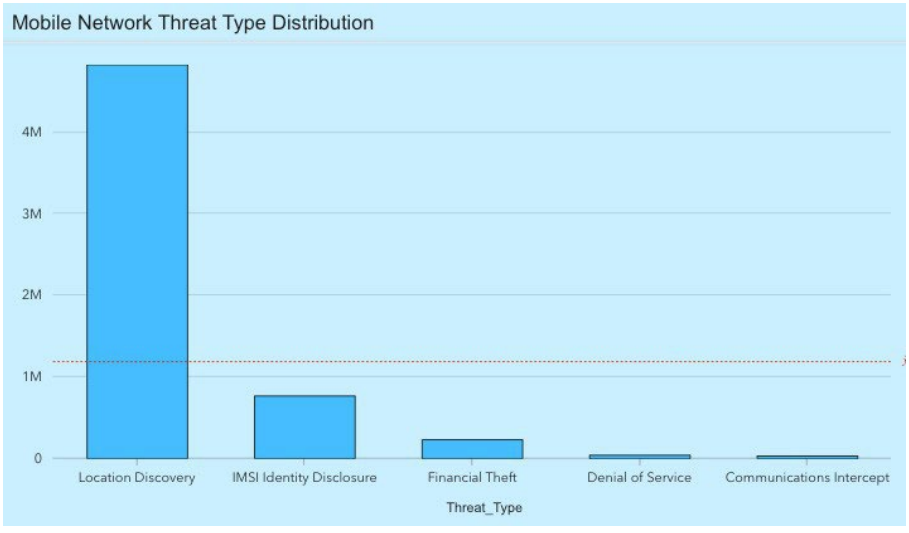


Figure 9 : Répartition des attaques de réseau par type de menace.

Mobile Surveillance Monitor a également déterminé qu'environ 171 réseaux de 100 pays sources ont envoyé des messages de suivi de la géolocalisation ciblés à des réseaux d'opérateurs de téléphonie mobile situés en Afrique au cours de la première moitié de 2023, ce qui indique que les tentatives de surveillance SS7 généralisée se poursuivent. Les principaux réseaux malveillants à l'origine de ces messages en 2023 sont présentés dans la figure 10. La disparité de volume entre les deux premières sources de réseau et le reste de la liste indique que les adresses globales de Millicom Tchad et de Celtel RDC tentent probablement de recueillir les données de localisation des utilisateurs. Les activités de ces adresses globales contrastent avec celles d'autres sources, comme Fink Telecom Services, qui a été démasquée pour avoir vendu des services de surveillance téléphonique commerciale ciblée dans le rapport « Ghost in the network » de la société de journalisme d'investigation Lighthouse Reports[21].

Network Threat Sources - Location Disclosure

Source Country	Source Network	Sum of Count (SUM)
Chad	MILLICOM CHAD	3,623,713
Congo DRC	CELTEL DRC	969,960
Zimbabwe	TELECEL ZIMBABWE	68,498
India	BHARAT SANCHAR NIGAM CELONE	53,436
Mozambique	MOCAMBIQUE CELULAR MOZAMBIQUE	35,614
Iceland	NOVA	16,979
Saudi Arabia	MOBILY ETIHAD ETILSAT	5,478
Jamaica	DIGICEL JAMAICA	4,884
Uganda	UGANDA TELECOM	3,784
Malaysia	CELCOM AXIATA BERHAD	3,773
Sweden	FINK TELECOM SERVICES	3,387
Italy	TELECOM ITALIA MOBILE	3,358
Saudi Arabia	ZAIN	3,141
Ghana	MILLICOM GHANA	2,699

Figure 10 : Menaces de divulgation de l'emplacement du réseau SS7 – classement en fonction du réseau source.

[21] Ghost in the network – Lighthouse Reports. (2023). *Lighthouse Reports*. https://www.lighthousereports. com/investigation/ghost-in-the-network/. Voir aussi : Crofton Black et Omar Benjakob. (14 mai 2023). How a secretive Swiss dealer is enabling Israeli spy firms. *Haaretz.com*. https://www.haaretz.com/israel-news/security-aviation/2023-05-14/ty- article-magazine/.highlight/global-surveillance-the-secretive-swiss-dealer-enabling-israeli-spy- firms/00000188-0005-dc7e-a3fe-22cdf2900000

4. Mesures incitatives permettant les attaques de géolocalisation

D'un point de vue extérieur, la sécurisation des périmètres des réseaux mobiles semble être un processus simple. Les entreprises placent couramment des contrôles de sécurité et des filtres rigides à la périphérie de leurs réseaux à l'aide d'un pare-feu, alors pourquoi la même approche ne serait-elle pas appliquée aux réseaux mobiles? De plus, pourquoi ne pas suivre les normes industrielles et les lignes directrices largement acceptées en matière de sécurité des réseaux mobiles? Dans la pratique, la sécurité des télécommunications mobiles n'est pas aussi claire qu'elle devrait l'être. Un examen plus approfondi de certains des éléments moteurs de cet espace d'infrastructure essentielle peut mettre en évidence certains contrôles qui sont plus faciles à mettre en œuvre que d'autres.

Alors que les politiques d'itinérance nationale peuvent être imposées par les organismes de réglementation de chaque pays, comme les politiques réglementaires sur les télécommunications du Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC)[22] ou la UK Telecommunications Security Act (Loi sur la sécurité des télécommunications du Royaume-Uni)[23], l'itinérance internationale repose sur des négociations bidirectionnelles indépendantes et des échanges d'informations d'adressage qui ne font pas périodiquement l'objet d'un suivi ou d'une mise à jour. À l'échelle sectorielle, l'interopérabilité technique et les aspects commerciaux sont facilités par le groupe de travail Wholesale Agreements and Solutions (WAS) de la GSMA[24], et les renseignements relatifs à l'interopérabilité et à l'adressage qui sont échangés entre les opérateurs sont conservés dans des documents appelés IR.21[25]. De plus, ces renseignements sont échangés électroniquement dans le cadre de l'échange d'ententes d'itinérance (RAEX)[26]. Les renseignements relatifs au réseau contenus dans l'IR.21 comprennent l'attribution d'adresses globales ou de plages à des équipements particuliers du réseau de l'opérateur dans le but d'informer chaque partenaire en itinérance aux fins de routage, d'interopérabilité et de sécurité.

Dans le secteur des télécommunications mobiles, l'absence d'exigences strictes concernant la tenue d'un inventaire des adresses attribuées aux équipements du réseau central a entraîné un manque de diligence de la part des opérateurs de téléphonie mobile du monde entier en ce qui concerne la mise à jour des renseignements relatifs aux adresses d'itinérance. Le fait de créer une ambivalence quant à la fiabilité du RAEX

[22] Conseil de la radiodiffusion et des télécommunications canadiennes. (2021). Examen des services sans fil mobiles. https://crtc.gc.ca/fra/archive/2021/2021-130.htm
[23] *Loi sur la sécurité des télécommunications de 2021*. (2021). https://www.legislation.gov.uk/ukpga/2021/31/ enacted.

[24] Wholesale Agreements and Solutions Group - Working Groups. (15 juin 2023). *Working Groups*.https://www.gsma.com/aboutus/workinggroups/wholesale-agreements-and- solutions-group
[25] IR.21 GSM Association Roaming Database, Structure and Updating Procedures.
[26] RAEX IR.21 Management System - RoamSmart. (18 juin 2019). *RoamSmart*. https://roam-smart. com/raex-ir-21-management-system/

et des adresses de réseau énumérées dans l'IR.21 réduit en fin de compte sa fiabilité en tant que ressource de sécurité mobile. L'absence d'une liste autorisée et validée de partenaires en itinérance contenant des renseignements vérifiés sur le réseau va à l'encontre des principes fondamentaux de la mise en place d'un dispositif de sécurité fondé sur la vérification systématique[27]. Si un système de conformité stricte était correctement tenu à jour par chaque opérateur dans le monde, les réseaux pourraient l'utiliser pour créer de meilleurs contrôles de sécurité périmétrique.

4.1. *Moteurs économiques*

Lorsque les opérateurs de téléphonie mobile ont déployé des outils d'analyse pour surveiller le trafic échangé entre les réseaux de leurs partenaires en itinérance, il est rapidement apparu que le modèle de confiance était rompu. Des millions de messages non autorisés provenant de réseaux étrangers ont été découverts[28], ce qui a incité le secteur à définir les exigences d'un pare-feu pour le réseau de signalisation. Si des lignes directrices et des spécifications en matière de sécurité ont été élaborées et publiées par le Fraud and Security Group (FASG) de la GSMA[29], il n'existe pas, à ce jour, de mécanismes universels de responsabilisation ou d'application des exigences. C'est à chaque opérateur de réseau mobile – et peut-être à leurs organismes de réglementation des télécommunications et de cybersécurité nationaux – de décider s'il doit protéger ses réseaux et ses abonnés, et de quelle manière.

L'attention portée aux messages de signalisation non autorisés est devenue plus élevée après la présentation du projet Carmen Sandiego à l'évènement Blackhat 2010[30] et la présentation de Tobias Engel au Chaos Communication Congress de 2014[31]. La première a révélé des points de vulnérabilité en matière de sécurité et la seconde a montré de quelles manières un logiciel de base et une connectivité au réseau SS7 pouvaient permettre des opérations de surveillance illimitées.

Ces présentations, ainsi que l'attention médiatique qui les a accompagnées, ont poussé les fournisseurs à commencer à mettre au point et à vendre des pare-feu de signalisation. Toutefois, l'adoption de ces pare-feu a souvent été retardée, car certains opérateurs de réseaux mobiles louaient déjà leurs réseaux à des fournisseurs de services à valeur ajoutée (SVA) tiers. Cela signifie qu'ils n'étaient pas incités à adopter une posture de sécurité susceptible d'avoir une incidence négative sur ces relations commerciales et sur les revenus qui en découlent. Ce n'est qu'après que la GSMA ait terminé les lignes directrices sur la sécurité du réseau SS7 en 2017 que les opérateurs de réseau ont commencé à déployer des pare-feu. À cette époque, les acteurs de la surveillance ont toutefois loué des adresses globales et déployé des capacités dans les

[27] Selon le National Security Telecommunications Advisory Committee (NSTAC) des États-Unis, la vérification systématique est décrite comme une stratégie de cybersécurité fondée sur l'idée qu'aucun utilisateur ou actif ne doit faire l'objet d'une confiance implicite : https://www.cisa.gov/resources-tools/groups/presidents-national-security-telecommunications- advisory-committee/presidents-nstac-publications

[28] De nombreux messages découverts indiquaient l'emplacement d'un téléphone, les appels en cours et d'autres renseignements à l'auteur de la requête.

[29] Fraud and Security Group – Working Groups. (23 mars 2023). *Working Groups*. https://www.gsma. com/aboutus/workinggroups/fraud-security-group.

[30] The Carmen Sandiego Project. *Blackhat* (4 juillet 2010). https://media.blackhat.com/bh-us-10/ whitepapers/Bailey_DePetrillo/BlackHat-USA-2010-Bailey-DePetrillo-The-Carmen- Sandiego- Project-wp.pdf.

[31] Schedule 31. Chaos Communication Congress. (n. d.). https://fahrplan.events.ccc.de/congress/2014/ Fahrplan/events/6249.html.

réseaux mobiles du monde entier, ce qui a eu pour effet d'atténuer certaines des protections que les pare-feu de signalisation étaient censés fournir.

4.2 Moteurs du secteur

Les revenus mutuellement bénéfiques associés à l'activité dynamique de location d'adresses globales ont fourni aux réseaux mobiles du monde entier d'importantes sources de revenus. En mai 2023, des fournisseurs de réseaux comme l'opérateur de télécommunications suédois Telenabler AB (voir figure 11) continuaient à promouvoir ouvertement la location d'adresses globales SS7 en tant qu'offre commerciale.

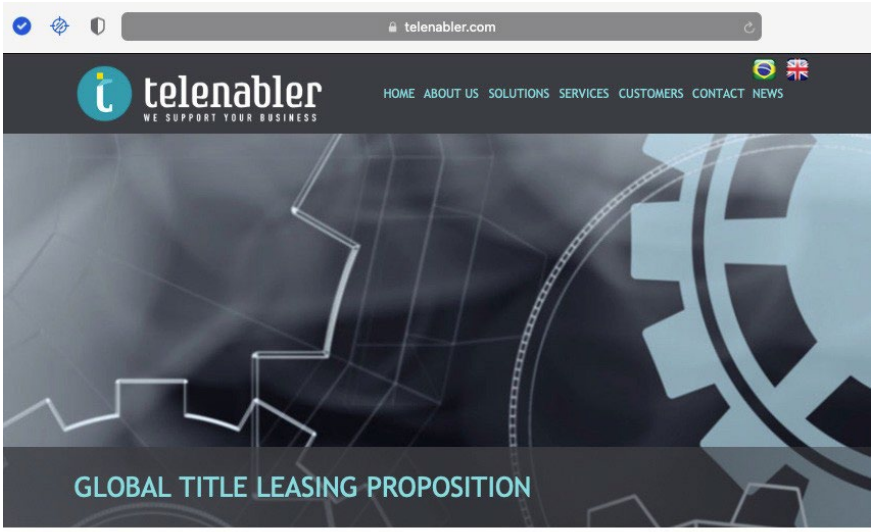
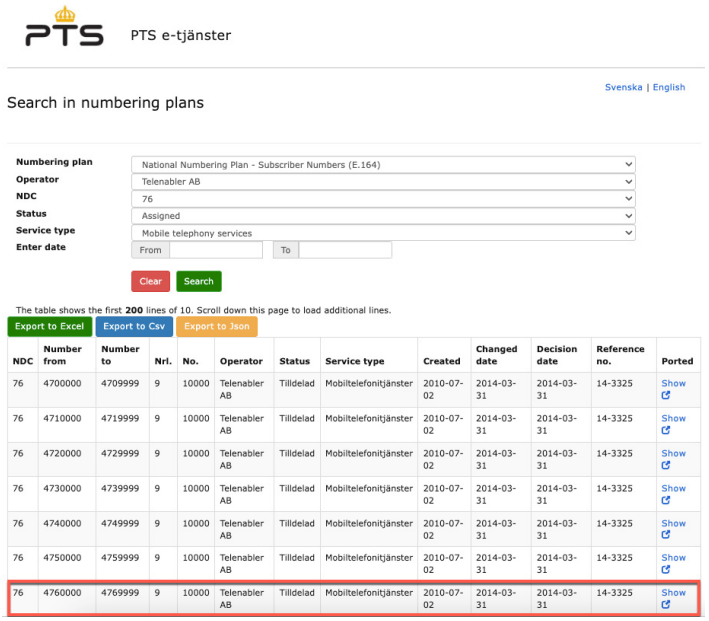


Figure 11 : Page Web de location d'adresses globales de Telenabler.

L'importance des risques liés à la location d'adresses globales apparaît clairement lorsque l'on examine les adresses globales attribuées à Telenabler par le Swedish Post and Telecom Authority (PTS), comme le montre la figure 12 ci-dessous. La plage de numéros décrite comprend un bloc précis de 10 000 numéros attribués à Telenabler, où un sous-ensemble de ces numéros a été considéré comme la source d'opérations de suivi de l'emplacement.



PTS e-tjänster

Svenska | English

Search in numbering plans

Numbering plan: National Numbering Plan - Subscriber Numbers (E.164)
Operator: Telenabler AB
NDC: 76
Status: Assigned
Service type: Mobile telephony services
Enter date: From To

Clear Search

The table shows the first **200** lines of 10. Scroll down this page to load additional lines.

Export to Excel Export to Csv Export to Json

NDC	Number from	Number to	Nri.	No.	Operator	Status	Service type	Created	Changed date	Decision date	Reference no.	Ported
76	4700000	4709999	9	10000	Telenabler AB	Tilldelad	Mobiltelefonitjänster	2010-07-02	2014-03-31	2014-03-31	14-3325	Show
76	4710000	4719999	9	10000	Telenabler AB	Tilldelad	Mobiltelefonitjänster	2010-07-02	2014-03-31	2014-03-31	14-3325	Show
76	4720000	4729999	9	10000	Telenabler AB	Tilldelad	Mobiltelefonitjänster	2010-07-02	2014-03-31	2014-03-31	14-3325	Show
76	4730000	4739999	9	10000	Telenabler AB	Tilldelad	Mobiltelefonitjänster	2010-07-02	2014-03-31	2014-03-31	14-3325	Show
76	4740000	4749999	9	10000	Telenabler AB	Tilldelad	Mobiltelefonitjänster	2010-07-02	2014-03-31	2014-03-31	14-3325	Show
76	4750000	4759999	9	10000	Telenabler AB	Tilldelad	Mobiltelefonitjänster	2010-07-02	2014-03-31	2014-03-31	14-3325	Show
76	4760000	4769999	9	10000	Telenabler AB	Tilldelad	Mobiltelefonitjänster	2010-07-02	2014-03-31	2014-03-31	14-3325	Show

Figure 12 : La plage de numéros suédois attribués à Telenabler est considérée comme la source des opérations de suivi de l'emplacement.

Quatre des numéros de téléphone attribués à Telenabler ont mené des tentatives de surveillance de la géolocalisation jusqu'au 29 juin 2023, comme le montre la figure 13 ci-dessous. Comme c'est le cas pour de nombreux acteurs de la surveillance, les numéros sources utilisés comme adresses globales attribués à Telenabler utilisent plusieurs types d'opérations de messages de signalisation SS7, comme le montre la figure 13. Bien que différents types de messages de signalisation aient été utilisés, chacun d'entre eux avait pour objectif de divulguer l'emplacement du téléphone d'un utilisateur cible.

Mobile Network Threat Summary

Source Network	Source Node	Operation	Sum of Count (SUM)
TELENABLER AB	467647531812	anyTimeInterrogation	10
		provideSubscriberInfo	383
		provideSubscriberLocation	116
		sendRoutingInfo	37
	46764753182	anyTimeInterrogation	15
		provideSubscriberInfo	2
	46764753183	anyTimeInterrogation	27
		provideSubscriberInfo	33
		provideSubscriberLocation	17
		sendRoutingInfo	4
	467647531851	anyTimeInterrogation	35
		sendRoutingInfo	6
			Total 685

Figure 13 : Surveillance de l'emplacement des événements menaçants attribués aux adresses globales louées par les opérateurs de téléphonie mobile.

Les tarifs de location d'adresses globales ont été supprimés de la plupart des sites Web en raison des conséquences négatives perçues de la mise à disposition de réseaux en échange d'argent. Toutefois, les frais se situent habituellement entre 5 000 et 15 000 $ par mois[32]. Les bailleurs d'adresses globales affirment que leurs engagements commerciaux présentent un certain nombre d'avantages. Premièrement, ils affirment pouvoir offrir un accès au réseau SS7 à des tiers qui ne disposent pas des ressources nécessaires pour obtenir des plages de numéros. Deuxièmement, ils affirment pouvoir offrir un accès aux opérateurs de réseaux virtuels mobiles et aux fournisseurs de services mondiaux de module d'identité d'abonné (SIM) au moyen d'un réseau central, alors qu'ils ne pourraient pas l'obtenir autrement en raison d'exigences réglementaires locales. Troisièmement, ils affirment qu'en permettant la location d'adresses globales, ils peuvent offrir une connectivité aux réseaux mobiles mondiale facilement accessible aux fournisseurs de services de messagerie et de services à valeur ajoutée. Indépendamment de la mesure dans laquelle ces avantages sont réalisés, ils ouvrent également la porte aux opérateurs malveillants, qui peuvent mettre les adresses globales à la disposition des acteurs de la surveillance afin d'entreprendre une surveillance subreptice de la géolocalisation.

Encadré 3 : L'avenir de la location d'adresses globales

La location de réseaux à des tiers par des réseaux mobiles étrangers reste une pratique non réglementée et opaque dans le secteur de la téléphonie mobile. Les opérateurs de réseaux ne peuvent pas déterminer quels réseaux et quelles adresses ont été loués à des tiers. En outre, ils n'ont pas la possibilité de vérifier la légitimité de ces tiers ou s'ils ont conclu d'autres ententes de sous-location avec des acteurs de la surveillance comme des groupes criminels ou des entités parrainées par un État. Par conséquent, il n'y a guère de responsabilité dans le cas où un opérateur de réseau étranger vendrait, sciemment ou non, un accès au réseau à un acteur de la surveillance qui cible des utilisateurs de téléphones mobiles.

Le statu quo pourrait toutefois changer. En mars 2023, la GSMA a publié un document intitulé *Global Title Leasing Code of Conduct*[33]. Ce document énumère un certain nombre de questions et de préoccupations liées à la pratique commerciale de la location d'adresses globales, que nous avons détaillées dans le présent rapport, et poursuit en déclarant que la location d'adresses globales a évolué en raison de l'émergence de relations commerciales qui se sont construites au fil du temps sans aucune normalisation, spécification ou recommandation du secteur. Il est également mentionné dans le document qu'il n'existe par conséquent pas de cadre convenu régissant les relations entre les bailleurs d'adresses globales et les réseaux auxquels ils sont interconnectés[34]. Le document poursuit en indiquant très clairement que la GSMA conseille vivement de ne pas utiliser la location d'adresses globales[35].

[32] Global Title leasing (fixed price per month). (n. d.). Freelancer. https://www.freelancer.com/projects/ network-administration/global-title-leasing-fixed-price
[33] Document officiel de la GSMA FS.52 Global Title Leasing Code of Conduct.
[34] Document officiel de la GSMA FS.52, Section 2.4 Issues and Concerns with GT Leasing.
[35] Document officiel de la GSMA FS.52, Section 3 Global Title Leasing Use Cases.

Bien qu'il ne s'agisse que d'une recommandation, elle représente un changement important dans la position officielle de la GSMA et montre clairement que l'association est au moins disposée à modifier ses positions politiques. Il n'est toutefois pas certain que cela aura une incidence sur le secteur de la revente de réseaux tiers, qui est à l'origine de millions d'événements de suivi de la géolocalisation annuels sur les réseaux mobiles du

En cas de trafic de signalisation malveillant causant un préjudice à l'opérateur cible, le *Global Title Leasing Code of Conduct* de la GSMA présenté dans l'encadré 3 attribue la responsabilité juridique au bailleur d'adresses globales. En faisant peser la responsabilité juridique sur le bailleur d'adresses globales qui permet des activités cybernétiques malveillantes comme le suivi de la géolocalisation, il est difficile de concevoir que les avantages pour l'opérateur qui effectue la vente l'emportent sur les risques en matière de sécurité, d'opérations et de finances. La réglementation des télécommunications est cependant une affaire d'État et, en tant que tel, il peut être difficile d'élaborer des politiques sectorielles ou des mandats uniformes qui limitent ces activités à l'échelle de plusieurs pays. Par conséquent, chaque opérateur est tenu de maintenir des contrôles de sécurité et des pare-feu stricts pour protéger son réseau et ses abonnés.

Historiquement, l'incidence des organisations sectorielles pour encourager les restrictions sur la location d'adresses globales s'est avérée insuffisante. Si des groupes de travail sectoriels comme le FASG de la GSMA ont été créés pour élaborer des lignes directrices visant à encourager les opérateurs de réseaux mobiles à déployer des contrôles de sécurité, ils n'assurent pas l'application de la loi, ne divulguent pas publiquement les statistiques relatives aux attaques et n'offrent pas de renseignements sur les menaces pertinents avec la participation active des opérateurs. La GSMA fournit le Telecommunication Information Sharing and Analysis Center (T-ISAC) à titre de centre d'échange de renseignements sur les menaces, dans le but de diffuser les renseignements relatifs aux attaques de cybersécurité. Ce service n'est toutefois disponible que pour les membres de la GSMA et l'accès à ces renseignements nécessite donc une contribution financière annuelle. En 2023, cette contribution se situait entre 14 306 et 136 460 $, servant effectivement de barrière de paiement pour l'accès aux renseignements utiles à la sécurité et à la protection de la vie privée de la société civile[36].

Les opérateurs mobiles peuvent s'adresser directement à l'opérateur mobile fautif dont les réseaux sont considérés comme la source de messages de signalisation malveillants ciblant leurs abonnés. Ce processus nécessite habituellement que l'opérateur mobile ciblé contacte l'opérateur à l'origine des messages de signalisation malveillants et l'informe que s'il ne constate pas de mesures d'atténuation

[36] Voir : Membership Categories and Contributions – Membership. (20 mars 2023). Membership. https:// www.gsma.com/membership/membership-categories-contributions/

responsables, il bloquera le trafic ultérieur envoyé par l'adresse mondiale source incriminée. Toutefois, si l'opérateur du réseau ciblé bloque les messages de signalisation de l'opérateur de l'adresse mondiale source, l'acteur de la surveillance peut simplement envoyer ces messages en utilisant une autre adresse globale louée au même opérateur ou à d'autres opérateurs avec lesquels il a conclu des ententes de location. Ce processus peut se poursuivre, l'attaquant utilisant toutes les adresses globales disponibles jusqu'à ce qu'elles soient épuisées. Par ailleurs, les attaques peuvent être réparties uniformément sur plusieurs réseaux dans le monde, ce qui permet d'éviter la détection. Ce processus finit par devenir une sorte de jeu du chat et de la souris à forte intensité opérationnelle où l'opérateur ciblé abandonne tout simplement ou configure le pare-feu pour bloquer les types de messages utilisés dans les attaques.

4.3. Moteurs gouvernementaux

Outre le fait que certains opérateurs de réseaux sont financièrement motivés à conclure des ententes de location avec des acteurs de la surveillance et que le secteur est largement incapable d'assurer sa propre règlementation, les gouvernements ont généralement adopté une approche non interventionniste en matière de sécurité des réseaux mobiles. L'adoption de cette approche peut être liée à l'absence d'autorité claire conférée aux organismes de réglementation des télécommunications et à l'idée que les opérateurs de téléphonie mobile sont les mieux placés pour résoudre les problèmes de sécurité au sein de leurs réseaux. Dans d'autres cas, cette situation peut être liée à certains organismes gouvernementaux qui profitent des vulnérabilités des réseaux de téléphonie mobile et de la faiblesse des protocoles de sécurité des opérateurs.

Dans le premier cas, certains organismes de réglementation nationaux commencent à jouer un rôle plus actif en exigeant des normes de sécurité pour les réseaux mobiles. Les règlementations sur les infrastructures essentielles sont en cours d'adoption et les organismes de cybersécurité sont de plus en plus actifs en exigeant des opérateurs de télécommunications qu'ils fournissent des détails sur la manière dont ils sécurisent leurs systèmes[37]. Il reste cependant à voir si la vague de règlementations qui sont en train d'être adoptées mènera nécessairement à des mesures gouvernementales efficaces ou si, au contraire, elle ne fera que fournir une série de pouvoirs et d'outils que les gouvernements ne sont pas prêts à utiliser ou qui pourraient conduire à une ingérence gouvernementale insuffisamment responsable dans les réseaux de télécommunications[38].

Dans le second cas, si les États s'affirment davantage en ce qui concerne les mesures de sécurité que les opérateurs de télécommunications doivent adopter, il est possible

[37] Voir : UK Telecommunications (Security) Act 2021, UK (DRAFT) Telecommunications Security Code of Practice.
[38] Christopher Parsons. (2022). « Cybersecurity Will Not Thrive in Darkness: A Critical Analysis of Proposed Amendments in Bill C-26 to the Telecommunications Act », *Citizen Lab*. Disponible à l'adresse suivante : https://citizenlab. ca/2022/10/a-critical-analysis-of-proposed-amendments-in-bill-c-26-to-the-telecommunications-act/

que ces derniers ripostent. Ils peuvent s'opposer à une nouvelle activité gouvernementale au motif que les normes et exigences proposées sont trop intrusives, généralement inutiles ou tout simplement inadaptées à l'environnement actuel des menaces. Dans des pays comme le Canada, il existe depuis longtemps des forums volontaires dans lesquels les opérateurs de téléphonie mobile et le gouvernement établissent des normes de haut niveau qui s'accompagnent de processus d'examen de la sécurité par des organismes gouvernementaux[39]. Il se peut que de telles mesures soient insuffisantes étant donné l'état actuel de la précarité des réseaux.

Dans le troisième cas, peut-être plus inquiétant, les organismes de renseignement et de sécurité qui s'appuient sur les réseaux mobiles pour la surveillance pourraient se montrer réticents à l'idée de renforcer les mesures de sécurité des réseaux de télécommunications nationaux. Ils pourraient également avoir l'avantage lorsqu'il s'agit de déterminer quels types d'éléments de sécurité sont les plus appropriés, car ils pourraient effectivement s'opposer à des solutions de cybersécurité qui entraveraient leurs capacités de surveillance à l'intérieur et à l'extérieur du pays. Si les services de renseignement et de sécurité sont le plus à même de comprendre comment exploiter les réseaux de télécommunications à des fins de suivi de la géolocalisation, les décideurs politiques devraient également être attentifs à la possibilité que les organismes d'application de la loi fassent de même avec l'accès aux réseaux de télécommunications, en particulier dans les cas où les organismes d'application de la loi nationaux ont l'habitude d'exercer leurs pouvoirs de manière inappropriée en l'absence d'un contrôle adéquat et d'une autorisation judiciaire.

[39] Comité consultatif canadien pour la sécurité des télécommunications (CCCST). (30 juin 2020). https://ised-isde.canada.ca/site/gestion-spectre-telecommunications/fr/savoir- plus/comites-intervenants/conseils-comites/comite-consultatif-canadien-pour-securite-telecommunications-cccst

5. Suivi de la géolocalisation dans les réseaux 5G et mesures défensives non mises en œuvre

Les acteurs de la surveillance s'intéressent en permanence aux réseaux mobiles et adaptent donc leurs méthodes en fonction des capacités du réseau cible. Si les technologies et les normes en matière de télécommunications mobiles évoluent constamment, bon nombre des principes et des fonctionnalités sous-jacents de l'architecture du réseau et des méthodes de surveillance restent les mêmes.

Encadré 4 : Types de messages de signalisation équivalents utilisés pour demander l'emplacement d'un appareil mobile

Dans le cas des recherches pour localiser l'utilisateur, chacun de ces messages effectue une action similaire et pourrait être exploité par un adversaire; un adversaire pourrait même utiliser tous ces vecteurs simultanément pour cibler un seul utilisateur si les opérateurs de télécommunications exposent ceux-ci en raison de la façon dont ils ont configuré leurs réseaux.

Type de réseau	Nœud d'envoi	Exemple de message
SS7 2G ou 3G	Registre des abonnés locaux	MAP_Provide-Subscriber-Information (PSI)
4G Diameter	HSS	Diameter Insert_Subscriber_Data_ Request (IDR)
5G	UDM	Namf_Location_ ProvideLocationInformation (NPLI)

Compte tenu de l'exposition historique des utilisateurs au suivi de l'emplacement par des adversaires et de l'émergence de nouveaux services dans le réseau 5G, comme les voitures connectées, les maisons intelligentes, les réseaux intelligents et les soins de santé, il est essentiel que les opérateurs de réseaux mobiles adoptent une approche globale pour protéger leurs réseaux s'ils veulent limiter les vulnérabilités que les acteurs de la surveillance exploiteront et utiliseront à mauvais escient.

5.1. *Amélioration de la confidentialité de l'identité de l'abonné*

Les nouvelles fonctionnalités de sécurité disponibles dans les normes du réseau 5G constituent un pas important vers la prévention de la surveillance de la localisation à l'aide de réseaux. Alors que les réseaux 3G et 4G utilisent l'IMSI comme identité du réseau de l'utilisateur, qui a été exposée aux adversaires et obtenue au fil des ans pour mener des attaques de suivi de la géolocalisation, le réseau 5G offre des améliorations en matière de protection de la vie privée. Ces améliorations permettent de masquer l'identité du réseau de l'utilisateur et de son appareil et se présentent sous la forme des identifiants suivants :

- Subscription Permanent Identifier (SUPI) – identifiant unique au monde attribué à chaque abonnement du réseau 5G
- Subscription Concealed Identifier (SUCI) – l'équivalent chiffré du SUPI, qui comprend l'indicatif de pays de la station mobile (IPSM), le code de réseau mobile (CRM) et le Mobile Subscription Identity Number (MSIN)
- Globally Unique Temporary Identifier (5G-GUTI) – identifiant temporaire utilisé dans les réseaux 5G pour identifier un appareil mobile et les renseignements d'abonnement qui lui sont associés

Or, la mise en œuvre des fonctionnalités de sécurité dépend fortement de l'adoption de configurations de réseau correctes et de l'exploitation des fonctions de sécurité du réseau 5G disponibles par les opérateurs de télécommunications. Il existe un risque que certains opérateurs n'adoptent pas ces configurations sous prétexte que cela augmente les coûts de déploiement de l'infrastructure du réseau 5G. En outre, les utilisateurs n'ont pas la possibilité de déterminer si les mesures de protection de la vie privée ou de sécurité disponibles ont été mises en œuvre. Ce jugement commercial préjudiciable au client concernant la mise en œuvre de dispositifs de protection de la vie privée ou de sécurité devrait être évité, car ce faisant, les entreprises pourraient se mettre en danger sur le plan juridique ou réglementaire si des personnes cherchaient à obtenir réparation pour un manque de protection adéquate de leur vie privée ou si les organismes de réglementation imposaient des amendes aux entreprises qui ont délibérément omis de protéger les renseignements personnels de leurs clients.

5.2. *Amélioration de la sécurité de la signalisation internationale et de l'interconnexion*

La capacité des réseaux étrangers à cibler les utilisateurs internationaux au moyen de messages de signalisation révélant l'emplacement constitue l'attaque connue la plus répandue contre les réseaux mobiles. Bien que cette réalité soit bien connue du secteur des télécommunications, il reste à savoir si les opérateurs protègent leurs

clients contre ces menaces.

Dans les déploiements de réseaux 5G entièrement conformes et natifs en nuage[40], les messages de signalisation d'itinérance internationale transitent par des réseaux étrangers à l'aide d'une nouvelle interface appelée N32 et utilisent une fonction de réseau appelée Security Edge Protection Proxy (SEPP). Cette fonction a été introduite dans l'architecture du réseau 5G afin d'ajouter une protection à la communication historiquement vulnérable entre les opérateurs de réseaux étrangers. La fonction SEPP fournit le chiffrement, l'intégrité et l'authentification nécessaires à la frontière entre les réseaux d'itinérance.

Afin d'assurer la protection de la vie privée, les réseaux situés aux deux extrémités de l'interface en itinérance doivent toutefois mettre en œuvre cette fonction. Faire en sorte que tous les partenaires en itinérance mettent en œuvre la fonction SEPP peut être extrêmement difficile; sur les 351 opérateurs de réseau ayant lancé des services de réseau 5G, seuls 41 avaient lancé des architectures de réseau 5G natives en nuage en date d'avril 2023 selon la Global Mobile Suppliers Association (GSA)[41]. Les 310 opérateurs restants utilisaient toujours l'architecture non autonome (NSA) du réseau 5G, qui permet aux opérateurs de téléphonie mobile de contourner la fonction SEPP dans l'itinérance du réseau 5G tout en offrant la vitesse améliorée et les avantages de latence réduits du réseau d'accès radioélectrique 5G.

D'après les entretiens menés auprès des fournisseurs de solutions de sécurité des télécommunications lors du Mobile World Congress (MWC) qui a eu lieu en mars 2023[42], seule une poignée d'opérateurs a déployé la fonction SEPP, sans parler de son utilisation effective. Il en résulte que de nombreux opérateurs n'intègrent pas les avantages des normes du réseau 5G en matière de sécurité et de la protection de la vie privée lorsqu'ils déploient des réseaux 5G.

De nombreuses vulnérabilités des réseaux sont propres à la mise en œuvre des normes de télécommunications par un opérateur de réseau mobile donné. Toutefois, étant donné que de nombreux opérateurs se sont montrés disposés à vendre l'accès à des tiers, il est fort à craindre que les acteurs de la surveillance disposent d'un code logiciel permettant de sonder et de tester l'intégrité des réseaux 5G étrangers. Cela permettra aux acteurs de la surveillance d'adapter leurs tactiques, leurs techniques et leurs procédures aux vulnérabilités des différents types de réseaux pour chaque mise en œuvre du réseau cible. Historiquement, les acteurs de la surveillance ont rapidement appris à modifier leurs attaques pour dissimuler les traces et contourner les pare-feu. De plus, la lenteur des déploiements de sécurité des opérateurs réduit la difficulté pour ces acteurs de trouver et d'exploiter les vulnérabilités évidentes.

[40] L'entière conformité renvoie à la norme 3GPP 5G Standalone (SA) définie dans la spécification technique 29.573 (TS 29.573).
[41] GSA – 5G Public-Networks April 2023 Summary Report. https://gsacom.com/paper/public-networks-april-2023-summary-report/
[42] Briefing HardenStance - MWC23: Taking Stock of Telco Security. https://www.hardenstance.com/wp-content/uploads/2023/03/HardenStance-Briefing-MWC23-Taking-Stock-of- Telco-Security-FINAL. pdf

La lenteur des déploiements de sécurité des opérateurs sur les vecteurs d'attaque les plus vulnérables devrait être un signal d'alarme pour les organismes de réglementation nationaux. Pour contrer rapidement les attaques, il est impératif de respecter les lignes directrices et les normes de sécurité du réseau 5G et de disposer d'outils adéquats pour la détection des menaces. Sans ces mesures, les modalités de déploiement des réseaux 5G pourraient offrir aux utilisateurs une protection contre les attaques des acteurs de la surveillance qui n'est que légèrement supérieure à celle offerte par les réseaux 3G et 4G antérieurs, voire pas du tout.

6. Conclusion

À la lumière des évaluations historiques, actuelles et prospectives de la sécurité des réseaux mobiles, la surveillance de la géolocalisation devrait continuer à préoccuper fortement le public et les décideurs politiques. Des vulnérabilités exploitables existent dans les architectures des réseaux 3G, 4G et 5G, et devraient subsister en l'absence d'une transparence forcée exposant les mauvaises pratiques et de mesures de responsabilisation obligeant les opérateurs à remédier à ces problèmes. La disponibilité des trois types de réseaux offre de multiples options aux acteurs de la surveillance. Si les États et les organisations criminelles peuvent surveiller activement l'emplacement des téléphones mobiles sur le territoire national ou à l'étranger, ces vulnérabilités continueront à représenter un risque pour la sécurité non seulement des groupes à risque, mais aussi du personnel des entreprises, des militaires et des fonctionnaires.

Les quatre dernières années révèlent que la surveillance provient de réseaux opérant dans des pays bien classés en matière de liberté d'Internet, dans de petits pays insulaires éloignés et dans des pays ostensiblement neutres. Les vulnérabilités actuelles des réseaux mobiles sont systématiquement exploitées comme source de collecte de renseignements ou d'espionnage par les acteurs de la surveillance, les services de police et les groupes criminels organisés qui exploitent les vulnérabilités à leurs propres fins. Les menaces émanant de petits pays des Caraïbes, ainsi que les attaques provenant de pays d'Europe de l'Est et d'Afrique, révèlent une utilisation abusive et généralisée des ententes de location d'adresses globales au sein de nombreux réseaux de télécommunications.

Que pouvons-nous faire à la lumière de ces menaces? Bien que ce rapport n'offre pas de recommandations politiques ou de suggestions techniques complètes, il existe une série d'interventions qui devraient être prioritaires.

Premièrement, les attaques qui se produisent souvent au cours de voyages internationaux suggèrent que des tiers transmettent les IMSI des utilisateurs privés. Les organismes d'application de la loi et de la sécurité devraient s'efforcer activement d'empêcher le trafic de ces renseignements, par exemple, sur le Web clandestin.

Deuxièmement, les fournisseurs de services de réseau ainsi que d'autres tiers, comme ceux qui fournissent l'IPX et le règlement de la facturation entre les opérateurs, devraient être tenus de chiffrer les détails uniques de l'IMSI d'un téléphone et les fichiers de données mobiles qui l'accompagnent. Ces activités devraient être accompagnées d'un calendrier strict et périodique de vérifications de la conformité. Ces mesures de protection et de responsabilisation empêcheraient les acteurs malveillants au sein des réseaux de monétiser illicitement ou d'exploiter d'une autre manière les renseignements conservés. Ces vérifications peuvent être réalisées par les autorités

responsables de la protection des données, les commissaires à la protection de la vie privée et les organismes de réglementation des télécommunications ou des droits des consommateurs.

Troisièmement, la perspective d'autoriser de manière inappropriée l'accès de tiers au réseau IPX privé ou le courtage de renseignements obtenus lors de l'échange de trafic de signalisation augmente la probabilité d'une capacité de surveillance malveillante importante[43]. Plus précisément, les opérateurs de la surveillance pourraient connecter et surveiller le trafic des centres de signalisation internationaux entre les réseaux étrangers et jouer un rôle clé dans la capacité d'exécuter ces attaques. Les organismes de réglementation des télécommunications, de la cybersécurité, de la confidentialité des données et des droits des consommateurs devraient tous évaluer si les acteurs de la téléphonie mobile au sein de leurs territoires sont engagés dans des pratiques commerciales douteuses qui mettent en danger la sécurité, la vie privée et les droits des consommateurs. Les législateurs devraient également se demander s'il convient d'accorder des pouvoirs supplémentaires aux organismes de réglementation pour qu'ils puissent discipliner les mauvais acteurs ou les acteurs du secteur de la téléphonie mobile qui privilégient les revenus au détriment de la protection de leurs abonnés.

Quatrièmement, la fréquence croissante des attaques de géolocalisation utilisant les réseaux 4G indique un niveau de sophistication accru parmi les acteurs de la surveillance et une tendance évolutive qui augmente les risques d'espionnage à mesure que le monde entre dans l'ère du réseau 5G. Les déploiements du réseau 5G sont déjà terminés dans de nombreux pays développés et la surveillance de la géolocalisation est observée dans certains de ces pays. Cela remet en question la sécurité des futurs partenariats d'itinérance avec les réseaux des pays occidentaux. Alors qu'une grande attention a été accordée à la question de savoir s'il fallait ou non inclure des équipements Huawei dans les réseaux de télécommunications, nous avons relativement peu parlé de la nécessité de veiller à ce que les équipements non chinois soient bien sécurisés et ne soient pas utilisés pour faciliter les activités de surveillance[44]. Les décideurs politiques, les organismes de réglementation des télécommunications, les organismes de cybersécurité et les législateurs devraient élaborer un ensemble de normes obligatoires de sécurité et de protection de la vie privée neutre à l'attention des fournisseurs et des plateformes. Ils devraient également s'efforcer de faire respecter activement ces normes et d'imposer des sanctions importantes aux entreprises qui refusent délibérément de les respecter.

Les consommateurs peuvent supposer de façon légitime que leur opérateur de télécommunications a déployé et configuré des pare-feu de sécurité pour s'assurer que les messages de signalisation associés aux attaques de géolocalisation, aux attaques d'identité ou à d'autres activités malveillantes ne sont pas dirigés vers leurs téléphones.

---

[43] Jon Brodkin. (6 octobre 2021). Company that routes SMS for all major US carriers was hacked for five years. *Ars Technica.* https://arstechnica.com/information- technology/2021/10/company-that-routes-sms-for-all-major-us-carriers-was-hacked-for-five-years/

[44] Pour plus de renseignements, voir : Christopher Parsons. (2020). « Huawei and 5G: Clarifying the Canadian Equities and Charting a Strategic Path Forward ». *Citizen Lab.* Disponible à l'adresse suivante : https://citizenlab.ca/2020/12/huawei-5g-clarifying-the-canadian-equities-and-charting-a-strategic-path-forward/.

Ce n'est malheureusement pas souvent le cas. Des décennies de manque de responsabilité et de transparence ont contribué à l'environnement actuel dans lequel les attaques de surveillance de la géolocalisation de grande ampleur ne sont pas signalées. Ce statu quo a effectivement créé un marché florissant de la surveillance de la géolocalisation tout en permettant à certains fournisseurs de télécommunications de tirer profit du fait de fermer les yeux sur la disponibilité des interconnexions de leurs réseaux pour le secteur de la surveillance. Bien qu'il soit peu plausible de s'attendre à ce que tous les réseaux de télécommunications adoptent des mesures de sécurité et de protection de la vie privée pour se prémunir contre toutes les menaces, il convient de s'attaquer sans tarder aux menaces de géolocalisation pouvant être facilement traitées qui sont décrites dans le présent rapport.

Les opérateurs devraient être tenus d'adopter et d'agir pour atteindre et démontrer la conformité avec les lignes directrices et les cadres de cybersécurité comme la vérification systématique, de signaler lorsqu'ils subissent des attaques, d'accepter la responsabilité lorsque leurs réseaux sont utilisés de manière abusive par des acteurs de la surveillance, d'œuvrer à l'élaboration d'ententes et d'accréditations de sécurité et d'entreprendre des tests de pénétration pour déterminer les vulnérabilités et y remédier. Dans les cas où les opérateurs refusent d'entreprendre ces activités de leur plein gré, les organismes de réglementation devraient intervenir pour obliger les entreprises à le faire.

Aujourd'hui, les acteurs de la surveillance utilisent la géolocalisation pour révéler des renseignements intimes et personnels. La géolocalisation est utilisée pour suivre des défenseurs des droits de la personne, des dirigeants d'entreprise, des fonctionnaires et des membres de l'armée. À l'avenir, avec l'essor des villes intelligentes, de l'Internet des objets et de la croissance des systèmes connectés à l'Internet, les capacités et les possibilités d'attaque ne feront que croître. Si les organisations n'agissent pas, les défenseurs de la société civile et le monde des affaires au sens large devront faire pression sur les organismes de réglementation, les décideurs politiques et les politiciens pour qu'ils obligent activement les fournisseurs de télécommunications à adopter des mesures de sécurité appropriées afin d'atténuer les menaces pernicieuses et silencieuses associées à la surveillance de la géolocalisation.