~~SECRET//RAC~~

Dossier : 2200-B-2024-02

Bureau du commissaire au renseignement
Office of the Intelligence Commissioner

C.P./P.O. Box 1474, Succursale/Station B
Ottawa, Ontario K1P 5P6
613-992-3044 • télécopieur 613-992-4096

[TRADUCTION FRANÇAISE]

COMMISSAIRE AU RENSEIGNEMENT

DÉCISION ET MOTIFS

AFFAIRE INTÉRESSANT UNE AUTORISATION DE CYBERSÉCURITÉ POUR DES ACTIVITÉS VISANT À AIDER À PROTÉGER DES INFRASTRUCTURES FÉDÉRALES EN VERTU DU PARAGRAPHE 27(1) DE LA *LOI SUR LE CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS* ET DE L'ARTICLE 14 DE LA *LOI SUR LE COMMISSAIRE AU RENSEIGNEMENT*

LE 14 MAI 2024

Canada

TABLE DES MATIÈRES

I. APERÇU 1
II. CONTEXTE 2
III. NORME DE CONTRÔLE 4
IV. ANALYSE 5
A. Paragraphe 34(1) de la *Loi sur le CST* – Déterminer si les activités sont raisonnables et proportionnelles 8
i. Signification du caractère raisonnable et proportionnel 8
ii. Examen de la conclusion du ministre selon laquelle les activités en cause sont raisonnables 8
iii. Examen de la conclusion du ministre selon laquelle les activités en cause sont proportionnelles 11
B. Paragraphe 34(3) de *la Loi sur le CST* – Les conditions nécessaires à la délivrance d'une autorisation 15
i. L'information à acquérir au titre de l'autorisation ne sera pas conservée plus longtemps que ce qui est raisonnablement nécessaire (alinéa 34(3)a)) 15
ii. Le consentement des personnes dont l'information peut être acquise ne peut raisonnablement être obtenu (alinéa 34(3)b)) 18
iii. L'information à acquérir est nécessaire pour découvrir, isoler, prévenir ou atténuer des dommages aux systèmes fédéraux (alinéa 34(3)c))) 18
iv. Les mesures permettant de protéger la vie privée permettront de veiller à ce que l'information acquise au titre de l'autorisation qui est identifiée comme se rapportant à un Canadien ou à une personne se trouvant au Canada soit utilisée, analysée ou consrvée uniquement si elle est essentielle pour découvrir, isoler, prévenir ou atténuer des dommages aux informations électroniques ou aux infrastructures de l'information des institutions fédérales (alinéa 34(3)d)) 20
V. REMARQUES 22
A. […] 22
B. Terminologie utilisée dans les avis destinés aux utilisateurs pour obtenir leur consentement 24
C. Résultats – résultats et rapports envoyés hors du CST 25
D. Rapport de fin d'autorisation – communications entre un avocat et son client 26
VI. CONCLUSIONS 28

I. APERÇU

1. Il s'agit d'une décision concernant les conclusions du ministre de la Défense nationale (le ministre) visant une autorisation de cybersécurité délivrée au titre de la *Loi sur le Centre de la sécurité des télécommunications*, LC 2019, c 13, art 76 (*Loi sur le CST*).

2. Le Centre de la sécurité des communications (le CST) a pour mandat de mener des activités de cybersécurité afin de défendre les systèmes électroniques, les appareils, les réseaux et l'information qu'ils contiennent contre les cybercriminels et les cybermenaces parrainées par des États étrangers. Le CST fournit également des conseils et une orientation en vue de renforcer l'approche des institutions du Parlement et du gouvernement du Canada en matière de cybersécurité, par exemple les ministères fédéraux, les organismes gouvernementaux et les sociétés d'État.

3. Pour mener efficacement ses activités de cybersécurité, le CST peut devoir contrevenir à certaines lois canadiennes. De plus, lorsqu'il mène des activités de cybersécurité pour protéger les infrastructures fédérales, le CST peut acquérir incidemment des communications ou de l'information qui nuisent à l'attente raisonnable en matière de protection de la vie privée d'un Canadien ou d'une personne se trouvant au Canada.

4. Avant d'entreprendre des activités pouvant avoir ces effets, le CST doit obtenir une autorisation de cybersécurité délivrée par le ministre et approuvée par le commissaire au renseignement. En application de la *Loi sur le commissaire au renseignement*, LC 2019, c 13, art 50 (*Loi sur le CR*), le commissaire au renseignement approuve les activités ou catégories d'activités indiquées dans l'autorisation ministérielle s'il est convaincu que les conclusions du ministre sont raisonnables.

5. Le 18 avril 2024, le ministre a délivré une autorisation de cybersécurité en vertu du paragraphe 27(1) de la *Loi sur le CST* pour les activités visant à aider à protéger les infrastructures fédérales (l'autorisation). C'est la sixième année que le ministre délivre une autorisation à cette fin.

6. Le 19 avril 2024, le Bureau du commissaire au renseignement a reçu l'autorisation à des fins d'examen et d'approbation, au titre de la *Loi sur le CR*.

7. D'après mon examen, et pour les motifs ci-après, je suis convaincu que les conclusions tirées par le ministre en vertu des paragraphes 34(1) et (3) de la *Loi sur le CST* relativement aux activités ou aux catégories d'activités énumérées au paragraphe 42 de l'autorisation sont raisonnables.

8. Par conséquent, en application de l'alinéa 20(1)a) de la *Loi sur le CR*, j'approuve l'autorisation ministérielle en matière de cybersécurité pour les activités visant à aider à protéger les infrastructures fédérales.

II. CONTEXTE

9. Le CST est l'organisme national du renseignement électromagnétique en matière de renseignement étranger et l'expert technique de la cybersécurité et de l'assurance de l'information (para15(1), *Loi sur le CST*). Le contexte législatif détaillé des activités de cybersécurité du CST menées pour protéger les systèmes fédéraux, constitués des réseaux et des systèmes, des appareils qui y sont connectés et des diverses combinaisons de matériel informatique et de logiciels est décrit dans les décisions antérieures du commissaire au renseignement en matière de cybersécurité.

10. Dans le cadre du volet de son mandat touchant la cybersécurité et l'assurance de l'information, le CST peut obtenir une autorisation ministérielle lui permettant d'accéder à l'infrastructure d'une institution fédérale (les systèmes fédéraux) pour mener des activités de cybersécurité afin de protéger l'information électronique et les infrastructures de l'institution contre tout méfait, toute utilisation non autorisée ou toute perturbation de leur fonctionnement. L'autorisation ministérielle permet également au CST d'acquérir, d'utiliser, d'analyser et de conserver de l'information qui provient ou passe par cette infrastructure, qui y est destinée ou y est stockée, y compris l'information sur les Canadiens et les personnes se trouvant au Canada (art 27(1), *Loi sur le CST*), qui doit être traitée avec une attention particulière (art 34(3)d),*Loi sur le CST*).

11. Une autorisation ministérielle accorde au CST l'autorité légitime d'exercer des activités de cybersécurité qui contreviennent aux lois du Canada ou qui l'amène à acquérir incidemment de l'information qui nuit à l'attente raisonnable en matière de protection de la vie privée d'un Canadien ou d'une personne se trouvant au Canada (art 22(4), *Loi sur le CST*). En effet, pour comprendre les points d'entrée vulnérables et les atteintes à l'intégrité des systèmes fédéraux, le CST doit accéder à ces systèmes et acquérir de l'information à leur égard.

12. Pour délivrer l'autorisation, le ministre doit entre autres conclure que les activités envisagées sont raisonnables et proportionnelles, et que des mesures sont en place pour protéger la vie privée des Canadiens (art 34, *Loi sur le CST*). L'autorisation est valide jusqu'à un an après l'approbation du commissaire au renseignement (art 28(1), *Loi sur le CST*). Ce n'est qu'à ce moment que le CST peut exercer les activités autorisées.

13. Même si le CST dispose d'une autorisation de renseignement étranger, ses activités ne doivent pas viser des Canadiens ou des personnes se trouvant au Canada et ne peuvent pas porter atteinte à la *Charte canadienne des droits et libertés* (para 22(1), *Loi sur le CST*). Les autorisations de cybersécurité antérieures ont confirmé que les activités de cybersécurité du CST visent les cybermenaces plutôt que des individus en particulier.

14. Conformément à l'article 23 de la *Loi sur le CR*, le ministre a confirmé dans sa lettre de présentation m'avoir fourni tous les renseignements dont il disposait pour accorder l'autorisation en cause. Le dossier est donc composé de ce qui suit :

    a) l'autorisation datée du 18 avril 2024;
    b) les notes d'information de la chef du CST à l'intention du ministre datées du 22 mars 2024 et du 11 décembre 2023;
    c) la demande de la chef du CST datée du 22 mars 2024, y compris cinq annexes :
        i) Liste des institutions fédérales recevant des services de cybersécurité du CST;
        ii) Arrêté ministériel – les désignations pour l'application de l'article 45 de la *Loi sur le CST* datées du 13 juin 2023;
        iii) Résultats des activités 2023;

iv) Ensemble des politiques sur la mission en matière de cybersécurité (les politiques sur la mission) approuvé le 28 février 2022;

v) Tableau de conservation et suppression.

d) Document d'information – Aperçu des activités

e) Documents supplémentaires pour le dossier, y compris les exposés présentés au commissaire au renseignement et au personnel en janvier 2024.

III. NORME DE CONTRÔLE

15. Selon l'article 12 de la *Loi sur le CR*, le commissaire au renseignement procède à un examen quasi judiciaire des conclusions du ministre sur lesquelles reposent certaines autorisations, en l'espèce une autorisation de renseignement étranger, afin de déterminer si ces conclusions sont raisonnables.

16. La jurisprudence du commissaire au renseignement établit que la norme de la décision raisonnable, qui s'applique aux contrôles judiciaires des mesures administratives, est celle qui s'applique en l'espèce.

17. Comme l'a déclaré la Cour suprême du Canada, lorsqu'elle effectue un contrôle selon la norme de la décision raisonnable, la cour de révision doit commencer son analyse à partir des motifs du décideur administratif (*Mason c Canada (Citoyenneté et Immigration)*, 2023 CSC 21 au para 79). Au paragraphe 99 de l'arrêt *Canada (Ministre de la Citoyenneté et de l'Immigration) c Vavilov*, 2019 CSC 65 [*Vavilov*], la Cour suprême du Canada a décrit de manière succincte ce qui constitue une décision raisonnable :

> La cour de révision doit s'assurer de bien comprendre le raisonnement suivi par le décideur afin de déterminer si la décision dans son ensemble est raisonnable. Elle doit donc se demander si la décision possède les caractéristiques d'une décision raisonnable, soit la justification, la transparence et l'intelligibilité, et si la décision est justifiée au regard des contraintes factuelles et juridiques pertinentes qui ont une incidence sur celle-ci.

18. Les contraintes factuelles et juridiques pertinentes peuvent inclure le régime législatif applicable, l'incidence de la décision et les principes d'interprétation des lois. De fait, pour

comprendre ce qui est raisonnable, il faut prendre en considération le contexte dans lequel la décision faisant l'objet du contrôle a été prise ainsi que le contexte dans lequel elle est examinée. Il faut donc comprendre le rôle du commissaire au renseignement, qui fait partie intégrante du régime législatif établi par la *Loi sur le CR* et la *Loi sur le CST*.

19. Un examen de la *Loi sur le CR* et de la *Loi sur le CST*, ainsi que des débats législatifs connexes, montre que le législateur a créé le rôle de commissaire au renseignement afin qu'il serve de mécanisme indépendant permettant d'assurer un juste équilibre entre les mesures prises par le gouvernement à des fins de sécurité nationale et le respect de la primauté du droit et des droits et libertés des Canadiens. J'estime que le législateur m'a attribué un rôle de gardien afin de maintenir cet équilibre. Au moment d'examiner les conclusions du ministre, je dois également examiner attentivement la question de savoir si le droit à la vie privée et les autres droits importants des Canadiens et des personnes se trouvant au Canada ont été considérés et soupesés de façon appropriée, et je dois veiller à ce que la primauté du droit ait été pleinement respectée.

20. Lorsque le commissaire au renseignement est convaincu (*satisfied* en anglais) que les conclusions en cause du ministre sont raisonnables, il « approuve » l'autorisation (art 20(1)a), *Loi sur le CR*). À l'inverse, lorsque ces conclusions sont déraisonnables, il « n'approuve pas » l'autorisation (art 20(1)b), *Loi sur le CR*).

IV. ANALYSE

21. Le 22 mars 2024, la chef du CST a présenté une demande écrite au ministre en vue d'obtenir une autorisation de cybersécurité visant des activités menées afin d'aider à protéger des infrastructures fédérales (la demande). La demande décrit les activités de cybersécurité que le CST souhaite entreprendre pour accéder à une infrastructure de l'information des systèmes des institutions fédérales ou acquérir de l'information qui provient ou passe par cette infrastructure, qui y est destinée ou y est stockée afin de protéger cette infrastructure contre tout méfait, toute utilisation non autorisée ou toute perturbation de son fonctionnement. Comme ces activités peuvent contrevenir aux lois canadiennes ou nuire à l'attente raisonnable en matière de protection de la vie privée d'un Canadien ou d'une personne se

trouvant au Canada, une autorisation délivrée par le ministre et l'approbation du commissaire au renseignement sont requises.

22. La demande décrit la nature et les objectifs des solutions de cybersécurité déployées par le CST dans les systèmes fédéraux. Cela comprend le déploiement de trois types de capteurs (les solutions de cybersécurité) à différents niveaux des systèmes fédéraux afin de recueillir des données brutes sur les clients (c.-à-d. des données non évaluées acquises en vertu d'une autorisation ou obtenues par la divulgation d'information par le client). Ces solutions comprennent : 1) les solutions au niveau de l'hôte – des capteurs sont installés sur des dispositifs de points terminaux physiques ou virtuels (p. ex. postes de travail, appareils mobiles et serveurs); 2) les solutions axées sur les réseaux – les capteurs sont installés sur le périmètre du réseau donnant ainsi au CST accès à tout le trafic du réseau et entraînant automatiquement la prise de mesures d'atténuation; 3) les solutions infonuagiques – elles offrent des capacités semblables aux deux solutions mentionnées ci-dessus, mais dans un environnement infonuagique.

23. Les données brutes du client sont alors […]. Le CST obtient le consentement des institutions fédérales avant de déployer ses capteurs dans leurs systèmes.

24. Les solutions de cybersécurité fournissent de multiples couches de défense à la lumière de l'information sur la menace et de l'analyse des activités anormales. De plus, la demande comprend des explications de la chef sur la manière dont le CST analysera, traitera et conservera l'information acquise et sur les mesures en place pour protéger la vie privée des Canadiens et des personnes se trouvant au Canada, dans les cas où le CST acquiert incidemment de l'information sur eux.

25. D'après les faits exposés dans la demande présentée par la chef du CST, et en général dans le dossier, le ministre a conclu, aux termes du paragraphe 33(2) de la *Loi sur le CST*, qu'il y a des motifs raisonnables de croire que l'autorisation est nécessaire et que les conditions énoncées aux paragraphes 34(1) et (2) sont remplies.

26. Par conséquent, la ministre a autorisé le CST à mener les activités décrites au paragraphe 42 de l'autorisation :

    a) accéder à un système fédéral et déployer, à la demande d'un client fédéral, des solutions au niveau de l'hôte, des solutions axées sur les réseaux et des solutions infonuagiques;
    b) acquérir toute information à l'aide des solutions mentionnées ci-dessus, y compris l'information ayant trait à un Canadien ou à une personne se trouvant au Canada qui provient ou passe par les systèmes fédéraux, qui y est destinée ou y est stockée;
    c) utiliser, analyser, conserver ou divulguer l'information acquise en vertu de cette autorisation afin de découvrir, d'isoler, de prévenir ou d'atténuer des dommages aux systèmes fédéraux;
    d) mettre en place des mesures d'atténuation, telles qu'elles sont décrites dans la demande, pour contrer les cybermenaces.

27. Les solutions de cybersécurité énoncées dans l'autorisation sont les mêmes que celles que j'ai approuvées dans l'autorisation ministérielle de l'an dernier. En somme, le fait que certaines des mêmes activités aient été approuvées dans le passé ne change pas les exigences établies par la loi qui doivent être satisfaites pour que le commissaire au renseignement puisse juger que les conclusions du ministre sont raisonnables. Le ministre doit disposer de la meilleure information disponible au moment de déterminer s'il doit autoriser des activités. Le dossier doit effectivement refléter que l'autorisation est nouvelle et distincte et doit comprendre les plus récentes activités opérationnelles du CST. Pour trancher la question du caractère raisonnable des conclusions du ministre, le commissaire au renseignement peut tenir compte de la façon dont le dossier traite des remarques formulées dans des décisions antérieures.

28. Par opposition au dossier reçu l'année dernière, je suis convaincu que le présent dossier reflète bien que l'autorisation est nouvelle et distincte. Je reconnais les efforts déployés par le CST pour tenir compte des remarques faites antérieurement dans le présent dossier, mais aussi d'autres questions sur la cybersécurité et le renseignement étranger. Le dossier tient compte des mises à jour importantes concernant les détails additionnels sur la nature, la fréquence et le volume de l'information conservée à l'égard d'un Canadien ou d'une personne se trouvant au Canada; des répercussions des vérifications à l'égard des logiciels malveillants et des précisions sur les mesures d'atténuation mises en œuvre; et des précisions

sur la manière dont les utilisateurs des systèmes électroniques d'information du gouvernement du Canada obtiennent le consentement.

29. Suivant l'article 14 de la *Loi sur le CR*, relativement à la délivrance d'une autorisation de renseignement étranger, je dois examiner si les conclusions du ministre, qui ont été formulées au titre des paragraphes 34(1) et 34(3) de la *Loi sur le CST* et sur lesquelles repose l'autorisation de renseignement étranger qu'il a délivrée en vertu du paragraphe 27(1) de cette loi, sont raisonnables.

A. Paragraphe 34(1) de la *Loi sur le CST* – Décider si les activités sont raisonnables et proportionnelles

i. Signification du caractère raisonnable et proportionnel

30. Pour délivrer une autorisation de renseignement étranger, le ministre doit conclure « qu'il y a des motifs raisonnables de croire que l'activité en cause (*any activity* en anglais) est raisonnable et proportionnelle compte tenu de la nature de l'objectif à atteindre et des activités » (art 34(1), *Loi sur le CST*).

31. Lorsqu'il examine si l'activité en cause est raisonnable et proportionnelle, le ministre doit mettre en pratique sa compréhension de ce en quoi consistent ces seuils. La question de savoir si une activité est raisonnable et proportionnelle dépend du contexte et le ministre peut tenir compte de nombreux facteurs pour prendre sa décision. Le commissaire au renseignement doit juger si les conclusions du ministre, qui comprennent sa compréhension de ce que les seuils emportent, sont « raisonnables », et applique pour ce faire la norme de la décision raisonnable, comme cela est expliqué précédemment.

ii. Examen de la conclusion du ministre selon laquelle les activités en cause sont raisonnables

32. Au paragraphe 13 de l'autorisation, le ministre a conclu qu'il avait des motifs raisonnables de croire que les activités étaient raisonnables compte tenu de l'objectif visant à protéger les systèmes fédéraux.

33. Pour remplir son mandat en matière de cybersécurité et d'assurance de l'information, le CST doit acquérir de l'information se trouvant sur les infrastructures électroniques des institutions fédérales au Canada. En délivrant l'autorisation, comme pour les autorisations de cybersécurité précédentes visant des activités menées dans des infrastructures non fédérales, le ministre a implicitement accepté que les activités de cybersécurité ne contreviennent pas aux dispositions législatives qui interdisent d'acquérir délibérément de l'information qui se rapporte à un Canadien ou à une personne se trouvant au Canada (art 22(1), 23(4) et (5), *Loi sur le CST*.) Comme il est indiqué dans la décision 2200-B-2023-06, cette position implique logiquement que toute information se rapportant à un Canadien ou à une personne se trouvant au Canada qui a été acquise dans le cadre de ces activités ne l'a pas été délibérément, mais incidemment. Il s'agit là d'une interprétation raisonnable, à mon avis.

34. Néanmoins, il est important de souligner que les systèmes fédéraux sont situés au Canada et que la grande majorité de l'information qui y est stockée, en raison de sa nature, se rapporte à des Canadiens et à des personnes se trouvant au Canada. De plus, l'information contenue dans les systèmes ne se limite pas aux renseignements personnels des employés des institutions fédérales, mais comprend également des renseignements personnels des membres du public canadien qui, par exemple, communiquent avec les institutions par courriel. Par conséquent, les activités de cybersécurité du CST mèneront nécessairement à l'acquisition d'information liée au Canada, et la mise en œuvre efficace de mesures, de sauvegarde et de protection de cette information est primordiale.

35. Le ministre avance deux arguments pour faire valoir que les activités autorisées sont raisonnables : la participation du CST à l'intervention en matière de cybersécurité est nécessaire, car les compromissions deviennent de plus en plus difficiles à détecter et à combattre, ce qui met en péril la posture générale des systèmes fédéraux en matière de cybersécurité; et les activités visées par l'autorisation demandée sont efficaces.

36. En ce qui concerne la première raison, le ministre explique, et le dossier montre, que les cybermenaces provenant de criminels expérimentés et d'acteurs parrainés par des États étrangers visant les institutions fédérales deviennent de plus en plus fréquentes et complexes.

Les auteurs de menace disposent de techniques efficaces et mettent à profit une multitude de points d'entrée et de méthodes pour infiltrer l'infrastructure de l'information au niveau de l'hôte, des réseaux ou du nuage. De plus, les systèmes fédéraux sont vastes et complexes et ont été créés et entretenus par diverses parties au fil des ans. Les pratiques en matière de sécurité de l'information diffèrent grandement dans chaque institution fédérale et sont donc davantage exposées aux cybermenaces. Grâce au grand volume d'information acquis à l'aide des solutions de cybersécurité et à une analyse approfondie des activités anormales, le CST est en mesure de détecter les menaces que les institutions fédérales ne pourraient pas identifier par elles-mêmes et de se défendre contre elles. Dans le cadre d'un écosystème de protection, l'information acquise au cours des activités du CST profite non seulement aux systèmes fédéraux, mais également aux systèmes non fédéraux recevant l'aide du CST.

37. Quant à l'efficacité des activités de CST, les outils avancés d'analyse des logiciels malveillants et les capacités automatisées de cybersécurité fournies par le CST permettent la mise en place de multiples couches de défense pour détecter et prévenir les intrusions. L'information acquise dans le cadre de ces activités aide le CST à découvrir, isoler, prévenir ou atténuer les dommages aux systèmes fédéraux.

38. Comme il est indiqué dans le rapport sur les résultats, qui fournit des détails sur l'efficacité des solutions de cybersécurité dans le cadre de l'autorisation de sécurité antérieure pour les infrastructures fédérales, le CST a détecté […] incidents attribuables à la malveillance dans les systèmes fédéraux. L'efficacité des solutions de cybersécurité est essentielle pour que le CST prévienne ou atténue les atteintes à l'intégrité. Comme l'indique la jurisprudence du commissaire au renseignement (décision 2200-B-2023-02), le CST peut non seulement accéder aux systèmes fédéraux et acquérir de l'information, mais il a également le pouvoir de prendre des mesures d'atténuation (art 23(3)a), *Loi sur le CST*).

39. En ce qui concerne les activités décrites au paragraphe 42 de l'autorisation, j'estime que le ministre avait raison de conclure que les activités sont raisonnables. Les conclusions démontrent qu'il existe un lien rationnel entre les activités précisées dans l'autorisation et l'objectif de protéger les systèmes fédéraux contre tout méfait, toute utilisation non autorisée ou toute perturbation de leur fonctionnement. D'après le dossier, ces activités précises

contribuent à la réalisation du mandat du CST en matière de cybersécurité et de l'assurance de l'information. Le ministre a compris et explique en quoi les activités décrites dans l'autorisation sont nécessaires pour aider à protéger les systèmes fédéraux.

iii. Examen de la conclusion du ministre selon laquelle les activités en cause sont proportionnelles

40. Le ministre a également conclu, au paragraphe 16 de l'autorisation, qu'il avait des motifs raisonnables de croire que les activités autorisées sont « proportionnelles compte tenu de la façon dont elles sont exercées ».

41. Encore une fois, je suis convaincu que les conclusions du ministre sur la proportionnalité sont raisonnables en ce qui concerne les activités autorisées décrites au paragraphe 42 de l'autorisation. Le ministre indique les raisons pour lesquelles les activités sont nécessaires et utiles, notamment pour l'acquisition d'informations permettant d'aider à protéger les systèmes fédéraux et à soutenir d'autres activités du CST. Il reconnaît que les activités peuvent mener à l'acquisition de grandes quantités de renseignements sur plusieurs plateformes afin de détecter les menaces. Toutefois, le ministre fait remarquer que le CST ne conserve qu'un très faible pourcentage de la quantité totale de données acquises initialement.

42. Le ministre présente les mesures et les contrôles énumérés ci-dessous pour démontrer que les activités sont proportionnelles :

a) les solutions de cybersécurité recueillent et utilisent les renseignements nécessaires afin de découvrir, d'isoler, de prévenir ou d'atténuer des dommages aux systèmes fédéraux;
b) l'information acquise est copiée et stockée par le CST, où les analystes en cybersécurité peuvent relever les activités malveillantes et rechercher rétroactivement les cas où les mêmes activités malveillantes sont menées ailleurs. Aucune information non évaluée n'est conservée plus longtemps que […] à compter de la date à laquelle elle a été acquise;

c) l'analyse et l'atténuation sont principalement effectuées par des processus automatisés qui limitent l'exposition des employés à l'information non évaluée et toute l'information est protégée conformément à la politique d'exploitation du CST;
d) les solutions de cybersécurité du CST acquièrent une vaste gamme d'information afin de mieux protéger les systèmes fédéraux, mais le CST conserve moins de 1 % de la quantité totale de données initialement acquise par les solutions de cybersécurité;
e) l'information acquise qui porte sur un Canadien ou une personne se trouvant au Canada ne sera utilisée, analysée ou conservée que si elle est jugée essentielle pour découvrir, isoler, prévenir ou atténuer les dommages aux systèmes fédéraux;
f) l'information acquise qui ne porte pas sur un Canadien ou une personne se trouvant au Canada ne sera conservée que lorsqu'elle est jugée essentielle pour découvrir, isoler, prévenir ou atténuer les dommages aux systèmes fédéraux;
g) chaque recherche effectuée sur l'information acquise, mais non évaluée, est vérifiable conformément à la section 11.3 de l'ensemble des politiques relatives à la mission de cybersécurité (EPM de cybersécurité) – l'ensemble des politiques qui s'appliquent aux activités de cybersécurité. Les journaux d'audit sont conservés pour un minimum de […] à des fins d'examen et de surveillance;
h) pour ce qui est de l'utilisation des contrôles de sécurité, l'accès à l'information acquise en vertu de la présente autorisation est limité aux employés qui ont besoin d'en avoir connaissance dans le cadre de leur travail. Avant d'accéder à de l'information non évaluée, les employés doivent réussir un examen annuel noté portant sur les exigences établies par les lois et les politiques qui s'appliquent au traitement de ce type d'information;
i) tous les outils de cybersécurité sont passés en revue pour veiller à ce qu'ils soient conformes aux lois et aux politiques;
j) les mêmes conditions s'appliquent à l'information utilisée par le CST pour découvrir, isoler, prévenir ou atténuer les dommages aux systèmes d'importance [systèmes non fédéraux].

43. Comme l'indiquent deux décisions relatives à l'autorisation de cybersécurité pour une entité non fédérale (décisions 2200-B-2023-05 et 2023-06), les mesures prévues aux alinéas a), b),

e), et f) n'appuient pas vraiment les conclusions du ministre selon lesquelles les activités sont proportionnelles, car elles constituent des conditions législatives distinctes qui doivent chacune être respectées au titre du paragraphe 34(3) de la *Loi sur le CST*. Le ministre ne peut satisfaire à une exigence prévue par la loi (les activités sont proportionnelles au titre du paragraphe 34(1)) en s'appuyant sur le respect d'exigences législatives distinctes (l'information ne sera acquise que si elle est nécessaire; l'information ne sera pas conservée plus longtemps que nécessaire; l'information ne sera conservée que si cela s'avère nécessaire; l'information liée au Canada ne sera conservée que si elle est essentielle au titre du paragraphe 34(3)).

44. Comme le montrent les autres mesures de la liste, le ministre se fonde en grande partie sur les mesures appliquées à l'information après son acquisition pour appuyer sa conclusion sur la proportionnalité. Cela soulève la question de savoir si le ministre a suffisamment tenu compte de la possibilité que les mesures puissent être appliquées avant l'acquisition de l'information pour décider si les activités de cybersécurité sont proportionnelles.

45. Une décision raisonnable en est une qui se justifie au regard des faits (*Vavilov*, para 126). Même lorsque la décision ne mentionne pas explicitement certains faits, la cour de révision doit être en mesure de suivre le raisonnement du décideur (*Vavilov*, para 102). En l'espèce, j'estime que je peux retracer le raisonnement suivi par le ministre pour s'appuyer sur les mesures à appliquer après l'acquisition de l'information dans son analyse sur la proportionnalité, plutôt que sur des mesures qui s'appliqueraient avant cette acquisition.

46. D'abord et avant tout, il reconnaît que pour mener efficacement des activités de cybersécurité, le CST doit obtenir une grande quantité d'information, notamment des fichiers, des courriels et des messages de clavardage à l'égard desquels les Canadiens et les personnes se trouvant au Canada ont une attente raisonnable en matière de protection de la vie privée. Les mesures à l'appui de ses conclusions relatives à la proportionnalité seront appliquées après l'acquisition de l'information, car cette dernière doit être acquise en premier lieu. Deuxièmement, l'accès à l'information acquise est limité aux employés désignés du CST qui sont formés pour traiter ce type d'information et l'utiliser selon le principe du « besoin de savoir » dans le cadre de leur travail. Le ministre était au courant des droits au

respect à la vie privée en cause et a présenté les mesures mises en place pour les protéger. Par conséquent, il a conclu que les activités proposées justifient toute atteinte potentielle aux droits des Canadiens en matière de vie privée.

47. Je suis convaincu que le ministre a effectué un exercice de mise en balance en tenant compte de l'objectif et de la nature des activités à l'égard desquels il a déterminé ce qu'il estime être des intérêts importants, à savoir l'acquisition d'information et la protection de la vie privée des Canadiens et des personnes se trouvant au Canada. Il explique également comment les activités avaient pour objectif l'atteinte d'un équilibre raisonnable entre elles. Je suis convaincu que les intérêts ont été considérés et que la mise en balance est raisonnable.

48. J'estime également que le ministre a tenu compte de l'incidence des activités sur la primauté du droit. Il explique qu'il existe une faible possibilité que des infractions autres que celles qui sont indiquées dans la demande soient commises, et que d'autres lois du Parlement peuvent être enfreintes, en fonction du contexte de l'activité qui est menée. Si le CST sait à l'avance que les activités entraîneront une infraction à une loi fédérale qui n'est pas mentionnée dans la demande, la chef en avisera le ministre et elle m'en informera par la suite. Le dossier relève les dispositions des différentes lois fédérales susceptibles d'être enfreintes et, comme l'indiquent les décisions précédentes en matière de cybersécurité, puisque le CST aura le consentement des institutions fédérales pour accéder à leurs systèmes, les possibles infractions sont en nombre limité et n'entraîneraient que peu de conséquences sur les Canadiens et les personnes se trouvant au Canada. Je suis convaincu qu'en cas de contravention à une loi fédérale, les conséquences négatives de cette violation seront limitées.

49. Enfin, les conclusions du ministre démontrent clairement sa compréhension des intérêts en matière de protection de la vie privée et des mesures en place pour les protéger. Si de l'information pouvant être liée aux droits des Canadiens en matière de vie privée est acquise et conservée, l'accès à cette information et son utilisation seront limités. En conséquence, je suis convaincu que les conclusions du ministre concernant le caractère proportionnel des activités sont raisonnables.

B. Paragraphe 34(3) de *la Loi sur le CST* – Les conditions nécessaires à la délivrance d'une autorisation

50. Lorsque le ministre estime que les activités sont raisonnables et proportionnelles au titre du paragraphe 34(1) de la *Loi sur le CST*, il peut délivrer une autorisation de cybersécurité visant à aider à protéger les systèmes fédéraux s'il conclut qu'il existe des motifs raisonnables de croire que les quatre conditions énoncées au paragraphe 34(3) de la *Loi sur le CST* sont remplies :

    a) l'information à acquérir au titre de l'autorisation ne sera pas conservée plus longtemps que ce qui est raisonnablement nécessaire;

    b) le consentement des personnes dont l'information peut être acquise ne peut raisonnablement être obtenu;

    c) l'information à acquérir est nécessaire pour découvrir, isoler, prévenir ou atténuer des dommages aux informations électroniques ou aux infrastructures de l'information des institutions fédérales;

    d) les mesures visées à l'article 24 de la *Loi sur le CST* permettront de veiller à ce que l'information acquise au titre de l'autorisation qui est identifiée comme se rapportant à un Canadien ou à une personne se trouvant au Canada soit utilisée, analysée ou conservée uniquement si elle est essentielle pour découvrir, isoler, prévenir ou atténuer des dommages aux informations électroniques ou aux infrastructures de l'information des institutions fédérales

        i. L'information à acquérir au titre de l'autorisation ne sera pas conservée plus longtemps que ce qui est raisonnablement nécessaire (alinéa 34(3)a))

51. Le ministre explique que l'information ne sera conservée que dans le cadre du mandat du CST touchant à la cybersécurité et à l'assurance de l'information. L'information est conservée conformément aux exigences définies dans les politiques du CST et elle est régie par un calendrier de conservation pour les différentes catégories d'information recueillie. Le ministre explique également que les exigences énoncées dans les politiques du CST sont conformes à la *Loi sur la protection des renseignements personnels*, LRC, 1985, c P-21 et à la *Loi sur la Bibliothèque et les Archives du Canada*, LC 2004, c 11.

52. La justification du ministre établit un lien entre les types d'information et leur période de conservation et explique pourquoi les différentes périodes de conservation sont nécessaires

pour des raisons de logistique. L'information acquise est initialement traitée par des processus automatisés pour établir si le CST devrait la conserver en raison de son caractère nécessaire ou essentiel à des fins de cybersécurité, mais le ministre explique que le CST doit également être en mesure de conserver l'information qui n'a pas été identifiée comme étant utile pour une période [...]. Une période d'évaluation de [...] est nécessaire pour donner le temps au CST d'analyser l'information dans le cas d'un cyberévénement et d'examiner son évolution au fil du temps.

53. Comme cela est expliqué dans le dossier, le fait de conserver l'information pendant une période de [...] permet au CST de comparer les nouvelles vulnérabilités découvertes par rapport à son information non évaluée et de déterminer si elles existent au sein des systèmes fédéraux. On trouve dans le dossier l'exemple d'une situation où la capacité du CST à « remonter le temps » a permis à ses analystes de repérer une menace et de prendre rapidement des mesures pour l'atténuer après avoir préalablement décelé une vulnérabilité dans les systèmes fédéraux touchés. La comparaison entre une atteinte à l'intégrité et des données non évaluées ou des activités malveillantes non détectées aide le CST à élaborer de meilleures mesures d'atténuation et des moyens de défense qui peuvent également être utilisés pour les systèmes fédéraux et non fédéraux.

54. L'information qui n'est pas évaluée sera automatiquement supprimée avant l'expiration de la période [...]. De plus, le programme de conformité interne du CST transmet des rappels trimestriels aux analystes de la cybersécurité afin que l'information qui n'est pas considérée comme nécessaire ou essentielle soit supprimée dans un délai de [...] après l'acquisition.

55. Le critère du caractère « nécessaire » s'applique à l'information qui ne se rapporte pas à un Canadien ou à une personne se trouvant au Canada; quant au critère du caractère « essentiel », il s'applique à l'information qui se rapporte à un Canadien ou à une personne se trouvant au Canada.

56. Comme il est écrit dans l'autorisation, l'information est jugée nécessaire pour découvrir, isoler, prévenir ou atténuer les dommages aux systèmes fédéraux lorsqu'elle est requise pour comprendre les activités cybernétiques malveillantes, [...], dans le but d'aider à protéger les

systèmes fédéraux. De par sa nature, cette information est intrinsèquement moins délicate que l'information jugée « essentielle », car elle ne concerne pas les Canadiens ou les personnes se trouvant au Canada. En effet, cela inclut [...]. Ce type d'information aide à développer des analyses en matière de détection et de prévention et renforce l'écosystème de la cyberdéfense. Par conséquent, elle peut conserver son utilité indéfiniment.

57. L'information sur les Canadiens et les personnes se trouvant au Canada est considérée comme essentielle si, sans elle, le CST n'était pas en mesure de découvrir, d'isoler, de prévenir ou d'atténuer des dommages aux systèmes fédéraux. Cela peut inclure [...]. L'information obtenue peut être de nature très délicate pour les Canadiens et la grande majorité de l'analyse est effectuée au moyen de processus automatisés, ce qui permet de signaler les comportements anormaux et de limiter l'exposition des employés au contenu des dossiers.

58. L'information qui a été jugée nécessaire ou essentielle pour découvrir, isoler, prévenir ou atténuer les dommages causés aux systèmes fédéraux peut être conservée « indéfiniment ou jusqu'à ce qu'elle ne soit plus utile à ces fins ». Cette information fera l'objet d'un suivi conformément à la section 11.2 de l'EMP de cybersécurité. De plus, chaque trimestre, les gestionnaires de l'exploitation doivent examiner l'information jugée essentielle pour déterminer si elle l'est toujours. L'information qui n'est plus essentielle doit être supprimée.

59. Compte tenu des restrictions importantes concernant l'accès à l'information non évaluée et des rappels trimestriels transmis aux analystes de la cybersécurité par l'intermédiaire du programme de conformité interne du CST pour évaluer l'information dans un délai de [...] après son acquisition, j'estime que la conclusion du ministre concernant la période d'évaluation de [...] est raisonnable.

60. Je suis également d'accord avec la conclusion du ministre selon laquelle l'information nécessaire ou essentielle pour découvrir, isoler, prévenir ou atténuer les dommages aux systèmes fédéraux peut être conservée jusqu'à ce qu'elle ne soit plus utile. La conservation de l'information pendant le temps nécessaire permet au CST de développer des cyberdéfenses et de suivre l'évolution rapide du savoir-faire des auteurs de menace qui

utilisent des logiciels malveillants. Cela permet une meilleure protection des systèmes fédéraux et non fédéraux.

ii. Le consentement des personnes dont l'information peut être acquise ne peut raisonnablement être obtenu (alinéa 34(3)b))

61. Avant de déployer ses solutions de cybersécurité, le CST obtient le consentement écrit des propriétaires des systèmes fédéraux qui lui autorise l'accès à leurs systèmes.

62. Les propriétaires de systèmes fédéraux doivent, conformément à la pratique courante du gouvernement, informer leurs utilisateurs – notamment les employés des institutions fédérales – que leurs appareils électroniques et leurs activités sur les réseaux sont surveillés à des fins de cybersécurité et d'assurance de l'information. Comme l'a expliqué le ministre, « en prenant connaissance de cet avis, les utilisateurs témoignent leur consentement au propriétaire du système fédéral auprès duquel le CST s'est engagé à fournir ces services de cybersécurité. »

63. Selon le ministre, il est parfois impossible d'obtenir le consentement des personnes dont les renseignements personnels ont pu être acquis par le CST dans le cadre d'activités de cybersécurité. En effet, le consentement des personnes qui communiquent avec des fonctionnaires fédéraux par courriel ou par l'intermédiaire d'une application de dialogue en ligne ne peut être raisonnablement obtenu.

64. J'estime que la conclusion du ministre à cet égard est raisonnable.

iii. L'information à acquérir est nécessaire pour découvrir, isoler, prévenir ou atténuer des dommages aux systèmes fédéraux (alinéa 34(3)c)))

65. Cette condition sous-tend les activités pour lesquelles l'autorisation est demandée. Comme il est impossible de prédire quelle information électronique contenue sur les systèmes fédéraux peut être utilisée de façon malveillante, le CST doit acquérir une vaste gamme d'information, y compris de l'information qui ne révèle pas l'existence d'une cybermenace. Ce faisant, le

CST peut acquérir incidemment de l'information qui nuit à l'attente raisonnable de protection en matière de vie privée d'un Canadien ou d'une personne se trouvant au Canada.

66. Suivant la jurisprudence du commissaire au renseignement, le Ministre n'est pas un expert technique et il peut se fier à l'évaluation de la chef selon laquelle cette acquisition est nécessaire pour découvrir, isoler, prévenir ou atténuer des dommages aux systèmes fédéraux au moment de tirer des conclusions. Le ministre a expliqué comment les auteurs de menace déguisent leurs activités et comportements malveillants afin de réduire la probabilité de détection, et il a fourni des exemples. Les informations acquises par l'entremise des solutions de cybersécurité sont utilisées pour [...]. Somme toute, les solutions de cybersécurité ne sont efficaces qu'en raison de l'acquisition de l'information.

67. La conclusion du ministre et le dossier n'indiquent pas si le CST peut atteindre les mêmes résultats en matière de cybersécurité grâce à des solutions de cybersécurité autres qui permettraient d'acquérir moins d'information se rapportant aux Canadiens. Si de telles solutions de cybersécurité étaient disponibles et réalisables sur le plan opérationnel, j'attendrais du CST qu'il fournisse cette information au ministre, car elles joueraient un rôle important dans sa décision de délivrer une autorisation, et elles auraient une incidence sur mon examen du caractère raisonnable.

68. Je suis tenu de procéder à mon examen sur la base de l'autorisation dont je suis saisi et de trancher la question de savoir si le contexte factuel justifie les conclusions du ministre sur cette question. Je suis convaincu que le ministre a expliqué pourquoi il a des motifs raisonnables de croire que l'acquisition d'information est nécessaire pour découvrir, isoler, prévenir ou atténuer des dommages aux systèmes fédéraux. En conséquence, je suis convaincu que les conclusions du ministre à cet effet sont raisonnables.

iv. Les mesures permettant de protéger la vie privée permettront de veiller à ce que l'information acquise au titre de l'autorisation qui est identifiée comme se rapportant à un Canadien ou à une personne se trouvant au Canada soit utilisée, analysée ou conservée uniquement si elle est essentielle pour découvrir, isoler, prévenir ou atténuer des dommages aux informations électroniques ou aux infrastructures de l'information des institutions fédérales (alinéa 34(3)d))

69. Le ministre conclut qu'il a des motifs raisonnables de croire que les mesures visées à l'article 24 de la *Loi sur le CST* permettront d'assurer que l'information acquise qui est identifiée comme se rapportant aux Canadiens ou aux personnes se trouvant au Canada sera utilisée, analysée ou conservée uniquement si elle est essentielle pour découvrir, isoler, prévenir ou atténuer des dommages aux systèmes fédéraux ou aux systèmes importants pour le gouvernement du Canada.

70. Les conclusions du ministre décrivent les mesures mises en place pour protéger les intérêts des Canadiens et des personnes se trouvant au Canada en matière de protection de la vie privée. Il explique que, suivant la *Loi sur le CST*, lorsque les activités du CST peuvent nécessiter l'acquisition d'information provenant de l'infrastructure mondiale de l'information (l'IMI) qui nuit à l'attente raisonnable de protection en matière de vie privée des Canadiens et des personnes se trouvant au Canada, le CST doit mener ses activités en vertu d'une autorisation ministérielle. À titre de précision, même si l'autorisation permet au CST d'accéder aux systèmes fédéraux – lesquels font partie de l'IMI – le paragraphe 42 de l'autorisation ne sollicite pas l'autorisation du CST pour acquérir de l'information auprès d'autres parties de l'IMI. J'analyserai cette question davantage dans mes remarques.

71. Le ministre précise que l'information se rapportant à un Canadien ou à une personne se trouvant au Canada ne peut être conservée que si elle est jugée essentielle. Le CST restreint l'accès à l'information non évaluée aux analystes qui travaillent dans le cadre de l'aspect cybersécurité et d'assurance de l'information de son mandat. De plus, toute l'information est restreinte à l'aide de contrôles d'accès particuliers. Tout d'abord, toutes les personnes doivent être des employés du CST, des détachés, des entrepreneurs, des employés intérimaires et du personnel nommé pour exercer les attributions du CST en vertu de la *Loi sur le CST*. L'information est fournie aux personnes concernées afin qu'elles puissent

accomplir leur travail, selon le principe du « besoin de savoir ». Deuxièmement, l'information qui n'a pas encore fait l'objet d'une évaluation de nécessité ou du caractère essentiel se limite également aux personnes ou aux catégories de personnes désignées dans l'autorisation qui ont besoin de savoir pour mener les activités précisées dans l'autorisation. Avant d'accéder à de l'information non évaluée, les employés du CST doivent recevoir une formation portant sur les exigences établies par les lois et les politiques qui s'appliquent au traitement de ce type d'information. Enfin, l'accès approprié à l'information est accordé à un nombre limité d'employés occupant des rôles de gouvernance et de responsabilité.

72. L'ensemble des politiques relatives à la mission de cybersécurité prévoit les mesures à prendre par le CST pour la conservation, l'utilisation et la divulgation d'information concernant les Canadiens et les personnes se trouvant au Canada. Selon la section 8.2.2, les analystes du CST effectuent une « analyse du caractère essentiel » avant que l'information acquise soit conservée et ils consignent les justifications appuyant le caractère essentiel. La réponse à la question de savoir si l'information est essentielle peut être obtenue à l'issue d'un processus manuel ou automatisé. Selon le tableau de conservation et suppression, les gestionnaires de l'exploitation doivent examiner l'information conservée sur une base trimestrielle et déterminer si elle est toujours nécessaire. L'information qui n'est plus essentielle doit être supprimée. Conformément au dossier, le tableau sera incorporé dans une prochaine version de l'EMP. Enfin, le CST dispose également un programme de conformité qui veille à ce que ses activités soient conformes à la norme EMP de cybersécurité ainsi qu'aux conditions de l'autorisation en vertu de laquelle elles sont menées.

73. Comme il est indiqué à l'article 24 de l'EMP, des mesures sont en place pour protéger la vie privée des Canadiens et des personnes se trouvant au Canada lorsque des renseignements qui les concernent sont divulgués à d'autres ministères ou partenaires. Par exemple, les renseignements personnels peuvent être supprimés afin d'éviter de dévoiler l'identité d'une personne. De plus, l'information non supprimée ne peut être divulguée que si le destinataire (ou la catégorie de destinataire) a été désigné par arrêté ministériel (art 45, *Loi sur le CST*), et que la divulgation est essentielle aux affaires internationales, à la défense, à la sécurité ou à la cybersécurité, conformément à l'article 43 de la *Loi sur le CST*. Je suis d'avis que les conclusions du ministre et le dossier tireraient profit d'explications supplémentaires sur

l'utilisation de mesures préventives lors de la communication d'information nominative sur un Canadien.

74. Compte tenu de ce qui précède, je suis convaincu que les conclusions du ministre sont raisonnables : le CST peut compter sur des mesures appropriées qui lui permettent de respecter ses obligations légales et politiques en matière de protection de la vie privée des Canadiens et des personnes se trouvant au Canada.

V. REMARQUES

75. Je voudrais formuler quatre remarques supplémentaires pour aider à l'examen et à la rédaction d'autorisations ministérielles futures. Ces remarques ne modifient pas ma décision concernant le caractère raisonnable des conclusions du ministre.

A. […]

76. Dans la décision de l'année dernière concernant la cybersécurité des infrastructures fédérales, j'ai fait une remarque au sujet de […]. En résumé, le commissaire au renseignement précédent n'avait pas approuvé d'activité en particulier […] et dans l'affaire dont j'étais saisi, le CST ne cherchait plus à obtenir d'autorisation pour l'activité en question, car elle n'avait pas à être approuvée par le ministre, même si elle était menée par le CST. J'ai exprimé une réserve à l'égard du manque d'explications en l'espèce sur les raisons pour lesquelles le CST avait abandonné sa demande d'autorisation concernant une activité qu'il avait néanmoins décidé de mener. Dans la décision 2200-B-2023-05 relative à une autorisation de cybersécurité pour les infrastructures non fédérales, j'ai souligné que ma préoccupation demeurait entière et que je m'attendais à ce que le CST fournisse une réponse satisfaisante dans le contexte d'une future demande d'autorisation de cybersécurité.

77. Le CST a fourni une réponse dans le dossier dont je suis saisi; cette réponse comprend de l'information qui vise à justifier sa décision selon laquelle il peut mener l'activité sans autorisation. Plus particulièrement, le dossier comprend une note d'information de la chef à l'intention du ministre qui explique le processus entrepris par le CST à la suite de la décision du commissaire au renseignement de l'époque en juin 2022 pour déterminer qu'une

autorisation n'était pas nécessaire, ainsi que deux brefs avis juridiques appuyant cette position.

78. Le processus du CST consistait à [...], obtenue par divulgation ou ingérée d'une autre manière par le CST aux fins de l'article 17 de la *Loi sur le CST*. Le but de cet exercice était de déterminer quelles sources constituaient [...]. D'après les avis juridiques, le CST a conclu que [...].

79. Le CST a identifié [...]. Le CST a ensuite jugé que l'information acquise jusqu'à présent [...] ne risque pas de nuire à une attente raisonnable en matière de protection de la vie privée, et la manière dont le CST demande l'information [...] ne risque pas de nuire à l'attente raisonnable de protection en matière de vie privée d'un Canadien ou d'une personne se trouvant au Canada. Le CST explique également que dans l'éventualité peu vraisemblable où une telle information serait recueillie, elle serait identifiée et supprimée, et elle serait portée à l'attention de l'équipe de conformité interne.

80. Comme il est indiqué dans la section Analyse de la présente décision, l'autorisation n'inclut pas [...] comme activité nécessitant l'approbation du commissaire au renseignement. En ce sens, cela ne relève pas de ma compétence en l'espèce. Le CST a répondu à ma demande visant à savoir pourquoi il n'avait plus besoin d'obtenir une autorisation ministérielle pour [...]. La CST a expliqué que l'information qu'il [...] à des fins de cybersécurité ne nécessite pas d'autorisation ministérielle.

81. Je tiens toutefois à rappeler que, lorsque le CST se prononce sur la question de savoir s'il peut mener une activité sans autorisation ministérielle, la *Loi sur le CST* indique clairement que la préoccupation première consiste à éviter que de l'information à l'égard de laquelle les Canadiens ont une attente raisonnable de protection en matière de vie privée ne soit recueillie. Ainsi, le fait de déterminer que l'information n'était pas [...] n'est pas nécessairement suffisant. L'information accessible au public, au sens de l'article 2 de la *Loi sur le CST*, ne peut pas inclure l'information à l'égard de laquelle les Canadiens et les personnes se trouvant au Canada ont une attente raisonnable de protection en matière de vie privée. Par conséquent, bien que le paragraphe 23(4) de la *Loi sur le CST* permette au CST

d'acquérir incidemment de l'information se rapportant à un Canadien ou à une personne se trouvant au Canada dans le cadre d'activités visées par une autorisation de cybersécurité, l'information accessible au public acquise pour l'application de l'article 17 de la *Loi sur le CST* ne peut contenir d'information liée au Canada acquise incidemment. En effet, conformément au paragraphe 23(4), le pouvoir d'acquérir incidemment de l'information liée au Canada est limité aux activités menées au titre d'une autorisation.

82. Je comprends que l'autorisation pour cette activité a été initialement demandée « par excès de prudence », en particulier parce qu'il y a une incompatibilité entre l'article 17 et le paragraphe 22(4) d'une part, et l'article 27 d'autre part, de la *Loi sur le CST*. Le CST souhaite mener ses activités légalement et il est raisonnable de faire preuve de prudence lorsque la nécessité d'une autorisation est incertaine. Néanmoins, les analyses requises doivent être effectuées avant de demander une autorisation ministérielle. Lorsque des activités sont menées sans autorisation ministérielle, les mesures appropriées doivent être mises en place pour empêcher l'acquisition incidente d'information qui nuit à l'attente raisonnable de protection en matière de vie privée d'un Canadien ou d'une personne se trouvant au Canada. Le fait de signaler cette acquisition à l'équipe de conformité interne après les faits n'est pas suffisant.

83. Je souligne également que je ne suis pas en désaccord avec l'évaluation de la chef selon laquelle il y a une incongruité dans la *Loi sur le CST* et qu'une modification permettrait de clarifier les activités du CST dans ce domaine.

B. Terminologie utilisée dans les avis destinés aux utilisateurs pour obtenir leur consentement

84. Le document ne précise pas la terminologie utilisée dans les avis aux utilisateurs des systèmes fédéraux sur lesquels le ministre s'est appuyé pour démontrer que les utilisateurs des systèmes fédéraux avaient consenti à ce que leurs renseignements personnels soient acquis à des fins de cybersécurité. J'estime qu'il est important de faire preuve de transparence envers tous les utilisateurs du système ainsi qu'envers ceux qui communiquent avec eux. Par conséquent, l'avis aux utilisateurs doit indiquer clairement que l'information contenue ou partagée sur les appareils et les réseaux du gouvernement fédéral, y compris les

renseignements personnels, peut être acquise incidemment et peut être utilisée, analysée, conservée et divulguée à des fins de cybersécurité. Cela comprend les communications privées à l'égard desquelles l'auteur a une attente raisonnable de protection en matière de vie privée. Cet énoncé peut sembler inquiétant, mais il est important que les utilisateurs comprennent le type de renseignements personnels qui peuvent être conservés ou divulgués et les mesures qui ont été mises en place pour protéger leur vie privée. Par exemple, même si les courriels peuvent être acquis par l'entremise des solutions de cybersécurité, le CST s'intéresse d'abord aux comportements anormaux liés aux courriels plutôt qu'à leur contenu. De plus, avant de partager de l'information liée au Canada, le CST doit conclure que la divulgation est nécessaire pour aider à protéger les systèmes fédéraux (art 44(1)a), *Loi sur le CST*) et à respecter ses obligations légales et politiques visant à protéger la vie privée des Canadiens.

85. Par conséquent, j'espère que le CST veille à ce que les propriétaires des systèmes fédéraux utilisent dans leurs avis des termes qui informent clairement leurs utilisateurs de la portée étendue des activités de cybersécurité, qui pourraient inclure l'acquisition de renseignements personnels.

86. Bien que j'aie jugé raisonnables les conclusions du ministre selon lesquelles il serait trop difficile d'obtenir le consentement des personnes dont les renseignements personnels peuvent être acquis par le CST dans le cadre de ses activités de cybersécurité, j'encourage le CST à réfléchir à des façons d'aviser les utilisateurs externes.

C. Résultats – résultats et rapports envoyés hors du CST

87. Le rapport sur les résultats présente certains détails, y compris des données empiriques, sur les résultats de l'autorisation délivrée par le ministre que j'ai approuvée en 2023 – jusqu'au moment où la demande de la chef a été préparée. Il permet de mieux comprendre les incidents observés attribuables à la malveillance. Le rapport indique que le CST a publié […] rapports sur la cyberdéfense fondés sur les activités malveillantes et les vulnérabilités identifiées par ses solutions de cybersécurité. La grande majorité des rapports sur la cyberdéfense, […] contenaient de l'information liée au Canada, comme […] canadien.

Comme c'est la première fois que le CST fournit le nombre de rapports de cyberdéfense publiés ou qui contiennent de l'information liée au Canada, je ne peux faire de comparaisons avec les années précédentes. Toutefois, le rapport indique que, pendant la période d'autorisation, le CST a détecté [...] incidents attribuables à la malveillance dans les systèmes fédéraux. Dans le rapport des résultats inclus dans l'autorisation de l'an dernier, le CST a indiqué qu'il avait détecté [...] incidents attribuables à la malveillance. J'estime que si le volume ou la nature des menaces détectées varient d'une année à l'autre, il serait utile d'inclure une explication dans le dossier à l'intention du ministre et de la mienne indiquant que cet élément doit être considéré dans nos décisions respectives.

88. Le rapport indique que le CST a communiqué les rapports aux destinataires désignés lorsque cela était nécessaire pour aider à protéger les systèmes fédéraux ou non fédéraux importants (art 44 et 45, *Loi sur le CST*). Toutefois, il n'y a aucune information concernant le volume ou les destinataires des rapports divulgués. J'ai soulevé une question similaire dans la décision que j'ai rendue cette année concernant les renseignements étrangers (décision 2200-B-2024-01). Le rapport des résultats dans ce dossier contient un graphique indiquant quels ministères ont consulté les rapports, mais ne renferme rien sur la question de savoir si ces rapports avaient été communiqués à des partenaires internationaux. À cet égard, je suis d'avis que le ministre et moi bénéficierions de l'inclusion d'information plus détaillée sur la communication de rapports (particulièrement s'ils sont communiqués à des partenaires internationaux) et sur le traitement de l'information liée au Canada lorsque les rapports sont communiqués.

D. Rapport de fin d'autorisation – communications entre un avocat et son client

89. La législation prévoit que quatre-vingt-dix jours après la fin de la période d'autorisation, le CST doit fournir un rapport sur le résultat des activités menées au titre de l'autorisation ministérielle au ministre et au commissaire au renseignement (para 52(2), *Loi sur le CST*).

90. Au cours de l'examen de cette question, le Bureau a demandé au CST de fournir une copie du rapport suivant l'expiration de l'autorisation qui avait été envoyé au ministre après la période d'autorisation de 2022, lequel ne m'avait pas encore été remis en raison, semble-t-il,

d'un oubli du CST. Je reconnais que le ministre ne disposait pas du rapport au moment où l'autorisation ministérielle a été délivrée (art 23, *Loi sur le CST*). Néanmoins, je considère que ce rapport est utile pour les besoins de mon examen, car il fournit un contenu contextuel applicable à la question dont je suis saisi et, par conséquent, je formule les commentaires suivants.

91. Dans le rapport suivant la fin de l'autorisation, le CST indique qu'il a acquis incidemment des communications entre un avocat et son client en 2023. Je souligne que c'est la première fois que le CST rapporte l'acquisition incidente de communications entre un avocat et son client dans le cadre d'une autorisation de cybersécurité. D'après le rapport, le CST a consulté l'équipe interne responsable de la politique interne et de la conformité après avoir pris conscience de la nature des communications; les communications ont été immédiatement supprimées et elles n'ont pas été conservées, utilisées ou analysées. Je souligne que cette acquisition incidente de communication n'a pas été décrite dans le rapport des résultats ni incluse dans le dossier qui m'a été soumis cette année ou dans celui dont je disposais l'année dernière. J'estime que cette information devrait être incluse dans le dossier pour que le ministre et moi-même puissions en prendre connaissance.

92. J'ai insisté dans les décisions précédentes sur l'importance du secret professionnel de l'avocat, et j'ai souligné que, lorsqu'il doit être levé, il doit l'être de la manière la plus minime possible (décisions 2200-B-2022-05 et 2200-B-2023-01). Je reconnais que l'acquisition incidente de communications a eu lieu au cours de la période d'autorisation de 2022 et que depuis, le CST a détaillé le processus interne à suivre lors de l'acquisition incidente de communications entre un avocat et son client, notamment pour préciser que l'accès aux communications durant l'évaluation doit être limité. D'après le bref processus général décrit dans le rapport suivant la fin de l'autorisation – qui indique que l'équipe responsable de la politique interne et de la conformité a été mobilisée – il est impossible d'affirmer avec certitude que le processus établi (en place à ce moment-là) a été suivi. Le ministre délivre des autorisations et le commissaire au renseignement les approuve en reconnaissant que les processus internes du CST permettent de gérer le secret professionnel de l'avocat de manière appropriée et en s'attendant à ce qu'ils soient respectés. Les rapports

suivant la fin de l'autorisation doivent indiquer clairement si ces processus ont été suivis ou non.

VI. CONCLUSIONS

93. D'après mon examen du dossier, je suis convaincu que les conclusions tirées par le ministre en application des paragraphes 34(1) et (3) de la *Loi sur le CST* à l'égard des activités et des catégories d'activités énumérées au paragraphe 42 de l'autorisation sont raisonnables.

94. J'approuve donc, en vertu de l'alinéa 20(1)a) de la *Loi sur le CR*, l'autorisation de cybersécurité pour des activités visant à protéger des infrastructures fédérales délivrée par le ministre le 18 avril 2024.

95. Comme le ministre l'a indiqué, et en vertu du paragraphe 36(1) de la *Loi sur le CST*, cette autorisation expire un an après la date de mon approbation.

96. Conformément à l'article 21 de la *Loi sur le CR*, une copie de la présente décision sera remise à l'Office de surveillance des activités en matière de sécurité nationale et de renseignement afin de l'aider à accomplir son mandat au titre des alinéas 8(1)a) à c) de la *Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement*, LC 2019, c 13, art 2.

Le 14 mai 2024

(Original signé)

L'honorable Simon Noël, c.r.
Commissaire au renseignement