Dossier : 2200-B-2024-05

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

MOTIFS DE LA DÉCISION RENDUE LE [...]

AFFAIRE INTÉRESSANT UNE AUTORISATION DE CYBERSÉCURITÉ POUR DES ACTIVITÉS DANS DES INFRASTRUCTURES NON FÉDÉRALES EN VERTU DU PARAGRAPHE 27(2) DE LA *LOI SUR LE CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS* ET DE L'ARTICLE 14 DE LA *LOI SUR LE COMMISSAIRE AU RENSEIGNEMENT*

[...]

Canada

TABLE DES MATIÈRES

I. APERÇU

1. Le [...], j'ai rendu une décision approuvant une autorisation de cybersécurité pour des activités dans des infrastructures non fédérales (autorisation), en précisant que je motiverais cette décision à une date ultérieure. Le ministre de la Défense nationale (le ministre) a délivré l'autorisation le [...]. D'après mon examen du dossier, j'étais convaincu que les conclusions du ministre, formulées en vertu des paragraphes 34(1) et (3) de la *Loi sur le Centre de la sécurité des télécommunications*, LC 2019, c 13, art 76 (*Loi sur le CST*) et sur la base desquels l'autorisation a été délivrée, étaient raisonnables.

2. Compte tenu du contexte dans lequel l'autorisation a été délivrée, j'étais d'avis qu'il était dans l'intérêt public de rendre ma décision rapidement et que les motifs de ma décision ne devait pas retarder la mise en œuvre des solutions de cybersécurité par le CST sur les infrastructures non fédérales. J'ai donc rendu ma décision, dont une copie est jointe à l'annexe A. Ci-après se trouve les motifs de cette décision.

II. CONTEXTE

3. 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 (art 15(1), *Loi sur le CST*). Dans le cadre de son mandat, il mène des activités de cyberprotection pour défendre les systèmes, les appareils et les réseaux électroniques ainsi que l'information qu'ils contiennent contre les cybermenaces criminelles et étatiques. Le CST fournit également des avis et des conseils pour renforcer la posture de cybersécurité de ces systèmes.

4. Pour mener efficacement ses activités de cyberprotection, le CST peut devoir contrevenir à certaines lois canadiennes. De plus, lorsqu'il mène des activités de cybersécurité pour protéger les systèmes électroniques, 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 de Canadiens ou de personnes se trouvant au Canada.

5. 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. Conformément à 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.

6. Le CST peut obtenir une autorisation du ministre qui lui permet d'accéder à de l'information électronique et à des infrastructures de l'information appartenant à une institution fédérale – systèmes fédéraux (art 27(1), *Loi sur le CST*) – ou d'une entité non fédérale désignée comme étant d'importance pour le gouvernement du Canada – systèmes non fédéraux (art 27(2), *Loi sur le CST*) – comme des entités dans les secteurs de la santé, de l'énergie et des télécommunications.

7. La *Loi sur le CST* décrit le processus que le CST doit suivre pour obtenir une autorisation de cybersécurité. Lorsque l'autorisation porte sur un système non fédéral, le propriétaire ou l'opérateur de ce système doit amorcer le processus en demandant au CST, dans une demande écrite, de mener des activités de cybersécurité pour protéger le système et l'information électronique qu'il contient (art 33(3), *Loi sur le CST*). La chef du CST doit ensuite présente une demande écrite au ministre en expliquant les facteurs qui lui permettraient de conclure qu'il existe des motifs raisonnables de croire que l'autorisation est nécessaire (art 33(2), *Loi sur le CST*). Les paragraphes 34(1) et (3) de la *Loi sur le CST* établissent les conditions dans lesquelles le ministre peut délivrer une autorisation de cybersécurité. L'autorisation ministérielle est valide lorsqu'elle est approuvée par le commissaire au renseignement (art 28(1), *Loi sur le CST*). Ce n'est qu'à ce moment que le CST peut mener les activités énoncées dans l'autorisation.

8. Conformément au paragraphe 27(2) de la *Loi sur le CST*, le ministre peut autoriser le CST à acquérir de l'information qui provient d'un système non fédéral, passe par ce système, y est destinée ou y est stockée afin d'aider à le protéger, dans les cas visés à l'alinéa 184(2)e) du *Code criminel*, LRC 1985, c C-46, cette infrastructure contre tout méfait, toute utilisation non autorisée ou toute perturbation de leur fonctionnement. L'alinéa 184(2)e) s'applique

généralement aux personnes qui gèrent la qualité du service d'un système informatique ou sa protection.

9. Même si une autorisation de cybersécurité est délivrée, la *Loi sur le CST* impose des limites aux activités du CST. Les activités du CST ne peuvent viser un Canadien ou une personne se trouve au Canada ou porter atteinte à la *Charte canadienne des droits et libertés* (art 22(1), *Loi sur le CST*). Toutefois, au cours d'activités menées au titre d'une autorisation, le CST peut légalement acquérir incidemment de l'information qui se rapporte à un Canadien ou à une personne se trouvant au Canada (art 23(4), *Loi sur le CST*). « Incidemment » s'entend de la manière dont l'information est acquise dans le cas où elle n'était pas délibérément recherchée (art 23(5), *Loi sur le CST*).

10. Lorsque le CST acquiert des renseignements personnels liés à des Canadiens ou à des personnes au Canada, des mesures politiques et législatives doivent être appliquées pour l'utilisation, l'analyse et la conservation de ces renseignements. De fait, le CST est tenu d'avoir des mesures en place pour protéger la vie privée des Canadiens et des personnes se trouvant au Canada en ce qui a trait à l'utilisation, à l'analyse, à la conservation et à la divulgation (art 24, *Loi sur le CST*).

11. 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;
    b) La note d'information de la chef du CST à l'intention du ministre;
    c) La demande de la chef du CST, qui contenait 11 annexes, dont les suivantes :
        i. les lettres de demande des entités non fédérales;
        ii. deux arrêtés ministériels;
        iii. le tableau de conservation et suppression;
        iv. l'ensemble des politiques sur la mission (EPM) en matière de cybersécurité, approuvé le 28 février 2022;
    d) Le document d'information – aperçu des activités;

III. NORME DE CONTRÔLE

12. Selon l'article 12 de la Loi sur le CR, le commissaire au renseignement procède à un examen quasi judiciaire des conclusions sur lesquelles repose une autorisation ministérielle afin de déterminer si ces conclusions sont raisonnables.

13. La jurisprudence du commissaire au renseignement établit que la norme de la décision raisonnable, qui s'applique aux contrôles judiciaires des mesures administratives, est la même qui s'applique à mon examen.

14. Comme l'a affirmé la Cour suprême du Canada, lorsqu'elle procède à un contrôle judiciaire de la décision raisonnable, une 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, 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.

15. 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 est donc nécessaire de comprendre le rôle du commissaire au renseignement, qui fait partie intégrante du régime législatif institué par la *Loi sur le CR* et la *Loi sur le CST*.

16. 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 du 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 ainsi que les droits et libertés des Canadiens. J'estime que le législateur m'a attribué un rôle de gardien afin de maintenir cet équilibre. Dans mon examen des conclusions du ministre, je dois soigneusement déterminer si les intérêts importants des Canadiens et des personnes se trouvant au Canada, notamment en matière de vie privée, ont été dûment pris en compte et pondérés, et je dois m'assurer que la primauté du droit est pleinement respectée.

17. 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

18. Suivant l'article 14 de la Loi sur le CR, 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 qu'il a délivrée en vertu du paragraphe 27(2) de cette loi, sont raisonnables.

19. La chef a adressé au ministre une demande écrite pour obtenir une autorisation de cybersécurité (demande) afin de pouvoir mener des activités aidant à protéger les systèmes des entités non fédérales en question.

20. Les entités non fédérales sont d'importance pour le gouvernement du Canada, aux termes de l'*Arrêté ministériel désignant l'information électronique et les infrastructures de l'information d'importance pour le gouvernement du Canada*, qui a été émis le 25 août 2020.

21. La demande décrit la nature et les objectifs des solutions de cybersécurité qui seront déployées par le CST. Elles comprennent : […] et […]. Comme l'exige la loi, chaque entité non fédérale a demandé l'aide du CST par écrit.

22. Une description des entités non fédérales, le contexte dans lequel elles ont demandé le soutien du CST et les activités décrites dans l'autorisation se trouvent dans l'annexe

classifiée de la présente décision (annexe B). J'inclus ces informations dans une annexe classifiée pour deux raisons. Premièrement, cela empêchera qu'une partie importante de la présente décision soit caviardée, ce qui facilitera la lecture de sa version publique. Deuxièmement, cela permettra de s'assurer que la nature des faits dont j'ai été saisi, qui autrement ne seraient accessibles que dans le dossier, est incluse dans la décision.

23. D'après les frais présentés dans la demande soumise par la chef du CST le [...], le ministre a conclu, avec des motifs raisonnables, que l'autorisation est nécessaire et que les conditions des paragraphes 34(1) et (3) de la *Loi sur le CST* ont été remplies.

24. Le ministre reconnaît également que sans l'autorisation, les activités dont il est question dans le paragraphe 72 pourraient être contraires à d'autres lois fédérales ou nuire à l'attente raisonnable en matière de protection de la vie privée de Canadiens ou de personnes se trouvant au Canada.

25. Par conséquent, le ministre a délivré une autorisation d'un an.

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

i. Signification du caractère raisonnable et proportionnel

26. 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*).

27. Le ministre doit parvenir à sa conclusion en se fondant sur sa compréhension de ce qu'impliquent des seuils raisonnables et proportionnels. 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

28. Le ministre a conclu au paragraphe 42 de l'autorisation qu'il avait des motifs raisonnables de croire que les activités autorisées dans l'autorisation sont raisonnables étant donné l'objectif d'aider à protéger les systèmes des entités non fédérales et de potentiellement protégé les systèmes fédéraux et d'autres systèmes d'importance contre les méfaits, l'utilisation non autorisée et la perturbation.

29. Comme dans les autorisations de cybersécurité antérieures, le ministre reconnaît que toute information liée à des Canadiens ou à des personnes se trouvant au Canada acquise au cours des activités n'est pas délibérément recherchée, mais incidemment acquise – et ne contrevient donc pas à l'interdiction, établie dans la loi, de chercher délibérément de l'information qui visent, ou de mener des activités qui visent, des Canadiens ou des personnes se trouvant au Canada (art 22(1), *Loi sur le CST*). Le paragraphe 23(3) de la *Loi sur le CST* précise que malgré l'interdiction de mener des activités qui visent des Canadiens ou des personnes se trouvant au Canada, le CST peut mener des activités de cybersécurité pour protéger les systèmes et atténuer les dommages. Par conséquent, en ce qui concerne l'interdiction, les activités de cybersécurité doivent viser des cybermenaces et non des Canadiens. Je suis convaincu que les activités de cybersécurité décrites dans l'autorisation respectent cette exigence de la loi.

30. Le ministre explique que les activités de cybersécurité décrites dans l'autorisation peuvent mener à la collecte et à la possible conservation d'information à l'égard de laquelle des Canadiens ou des personnes se trouvant au Canada ont une attente raisonnable en matière de respect de la vie privée. Étant donné le contexte dans lequel l'autorisation a été délivrée et la description de l'information que le CST doit acquérir pour mener efficacement ses activités, je suis d'avis que la probabilité que le CST recueille ce genre d'information est presque certaine. En effet, le dossier indique que le CST « doit » acquérir […].

31. Malgré cela, le ministre justifie le caractère raisonnable des activités en se fondant sur la posture de cybersécurité actuelle des entités non fédérales, le rôle qu'elles jouent dans la vie

des Canadiens et des personnes se trouvant au Canada, et le fait que les activités pour lesquelles l'autorisation est demandée sont efficaces.

32. De fait, le dossier décrit de manière très détaillée les compromissions et les potentielles compromissions des systèmes appartenant à des entités non fédérales – de l'information que j'ai incluse dans l'annexe B. Le ministre explique qu'il est de plus en plus difficile de détecter les cybercompromissions et qu'elles peuvent avoir de graves effets sur les entités non fédérales, entraînant la perte d'information ou de fonctionnalité d'un système. D'après l'information fournie par la chef, le ministre conclut que l'état actuel de la posture de cybersécurité des entités non fédérales n'est pas suffisant pour détecter et contrer les méthodes et les capacités sophistiquées employées par des auteurs de menaces avancés et persistants.

33. Selon le ministre, les systèmes des entités non fédérales doivent être sécurisés en raison du rôle important qu'elles jouent dans la vie de Canadiens et de personnes se trouvant au Canada. J'estime que la description du rôle joué par les entités non fédérales soutient la conclusion du ministre selon laquelle les activités décrites dans l'autorisation sont raisonnables.

34. Afin d'améliorer la cybersécurité, le ministre explique que les connaissances et les cybersolutions du CST permettent de répondre aux menaces inconnues des fournisseurs commerciaux de services de cybersécurité. Les cybermenaces peuvent être difficiles à détecter et les compromissions peuvent rapidement entraîner la perte d'information ou de fonctionnalité d'un système. Étant donné le contexte dans lequel l'autorisation a été délivrée, le […] du CST soutien aussi la conclusion du ministre selon laquelle les activités sont efficaces et raisonnables.

35. Les activités du CST aident les entités non fédérales à identifier les indicateurs de compromis […], à éliminer la présence des auteurs de menaces identifiés et à renforcer la posture de cybersécurité pour assurer une protection contre les futures menaces […]. De plus, les activités permettraient au CST de repérer, d'isoler et de mieux comprendre les cyberactivités malveillantes et d'autres indicateurs de compromission afin de conseiller les entités non

fédérales sur des moyens de les prévenir ou de les atténuer dans les systèmes. De fait, les activités permettent au CST de recommander des mesures d'atténuation ou de prendre des mesures d'atténuation, avec le consentement des entités non fédérales.

36. Je suis d'avis que les conclusions du ministre montrent qu'il a tenu compte et était convaincu du lien entre les besoins actuels des entités non fédérales et les cyberactivités proposées. Il y a un lien rationnel évident entre les activités de cybersécurité proposées par le CST et leur objectif d'aider à protéger les systèmes non fédéraux. Le ministre se fonde sur le rôle important joué par les entités non fédérales qui, à mon avis, soutient sa conclusion. Étant donné la nature de l'objectif et l'information dans le dossier concernant la nature des activités, j'estime que la conclusion du ministre selon laquelle les activités sont raisonnables est raisonnable.

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

37. Le ministre a également conclu, au paragraphe 45 de l'autorisation, qu'il avait des motifs raisonnables de croire que les activités autorisées sont [traduction] « proportionnelles compte tenu de la façon dont elles sont exercées ».

38. Je suis convaincu que les conclusions du ministre sur la proportionnalité sont raisonnables en ce qui concerne les activités autorisées décrites au paragraphe 72 de l'autorisation. Il reconnaît que les cyberactivités proposées peuvent mener à l'acquisition de grands volumes d'information afin de déceler les cybermenaces. Bien qu'il puisse y avoir des droits en matière de vie privée à l'égard d'une partie de l'information, le ministre explique que le CST est intéressé par tous les comportements anormaux touchant l'information, et non par le contenu.

39. Le ministre présente des mesures et des contrôles pour démontrer que les activités sont proportionnelles. Je constate que les mesures correspondent à celles qui ont été incluses dans l'autorisation ayant fait l'objet de la décision 2200-B-2024-02 (autorisation de cybersécurité pour des activités visant à aider à protéger des infrastructures fédérales). Dans cette décision, j'ai fait remarquer que le ministre ne peut pas satisfaire à une exigence de la loi – les activités

sont proportionnelles (art 34(1), *Loi sur le CST*) – en se fondant sur la satisfaction d'exigences séparées établies au paragraphe 34(3) de la *Loi sur le CST* (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 c'est nécessaire; l'information liée à des Canadiens ne sera conservée que si elle est essentielle).

40. En réponse à ma remarque, le ministre précise que les mesures et les contrôles internes sont divisés en deux catégories, « les exigences de la loi sur lesquelles le CST se fonde pour déterminer ses mesures et contrôles internes » et les mesures et contrôles supplémentaires qui dépassent les exigences de la loi. D'après les conclusions du ministre, je ne vois pas clairement quelle est la différence entre les exigences de la loi utilisées par le CST pour déterminer ses mesures internes et le simple fait d'utiliser les exigences de la loi comme mesures internes.

41. Quoi qu'il en soit, le ministre énonce les six mesures et contrôles internes appliqués par le CST :

    a) le CST conserve moins de 1 % de toutes les données initialement acquises au moyen de solutions de cybersécurité;
    b) 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;
    c) chaque fouille effectuée dans l'information acquise non évaluée est auditable pour assurer la conformité avec l'EPM;
    d) 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;
    e) toutes les technologies de cybersécurité sont passées en revue pour veiller à ce qu'elles soient conformes aux lois et aux politiques;

f) les mêmes conditions s'appliquent à l'information utilisée par le CST pour découvrir, isoler, prévenir ou atténuer les dommages aux systèmes fédéraux et autres systèmes d'importance.

42. Le ministre se fie largement aux mesures appliquées à l'information après son acquisition pour étayer sa conclusion au sujet de la proportionnalité. Je peux comprendre la justification du ministre pour se fonder sur ces mesures. Il reconnaît que le CST doit d'abord acquérir une grande quantité d'information, comme […], à l'égard de laquelle des Canadiens et des personnes se trouvant au Canada peuvent, selon lui, avoir une attente raisonnable en matière de respect de la vie privée. Les mesures qui soutiennent ses conclusions relatives à la proportionnalité seront appliquées après l'acquisition de l'information. De plus, l'accès à l'information 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. 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.

43. Le ministre était conscient des droits en matière de vie privée en jeu – même si ses conclusions auraient pu être plus précises quant à la probabilité qu'ils puissent être enfreints et à l'importance des éventuelles atteintes – et a décrit les mesures en place pour les protéger. Il conclut que les activités proposées justifient toute atteinte potentielle aux droits des Canadiens en matière de vie privée. Il explique également comment les activités avaient pour objectif l'atteinte d'un équilibre raisonnable entre elles. Je suis convaincu que les intérêts des Canadiens et des personnes se trouvant au Canada ont été pris en considération et que la mise en balance effectuée était raisonnable.

44. En ce qui concerne la règle de droit, le ministre 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 fédérales peuvent être enfreintes, en fonction du contexte de l'activité qui est menée. Le ministre et moi serons avisés si le CST contrevient à une loi fédérale qui n'est pas indiquée dans la demande. Puisque les entités non fédérales ont donné son consentement pour que le CST accède à ses systèmes, je suis d'avis que les infractions potentielles sont limitées et que leur incidence sur les Canadiens et les personnes au Canada est aussi limitée.

En cas de contravention à une loi fédérale, les conséquences négatives de cette violation seront limitées.

45. Les conclusions du ministre démontrent sa compréhension des intérêts en matière de protection de la vie privée et des mesures en place pour les protéger. Compte tenu de ces intérêts, il a conclu que les activités sont tout de même proportionnelles. J'estime que ses conclusions sont justifiées et intelligibles. 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

46. 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 pour aider à protéger des systèmes non fédéraux s'il conclut qu'il y a des motifs raisonnables de croire que les trois conditions suivantes, énoncées au paragraphe 34(3) *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) l'information à acquérir est nécessaire pour découvrir, isoler, prévenir ou atténuer des dommages aux systèmes non fédéraux;

c) les mesures en place pour s'assurer que l'information acquise au titre de l'autorisation qui est identifiée comme se rapportant à des Canadiens ou à des 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 non fédéraux.

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

47. L'information est conservée conformément aux exigences définies dans les politiques du CST et régies par un calendrier de conservation. 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.

48. Comme il est impossible pour le CST de déterminer quelle information sera utile pour découvrir des activités malveillantes, il acquiert une grande quantité d'information. Le ministre explique que le CST traite cette information surtout avec des moyens automatisés. Le processus peut permettre de déterminer qu'une partie de l'information est « nécessaire » ou « essentielle ». Toute autre information est considérée comme de l'information non évaluée, même si elle est passée par le processus automatisé.

49. La période de conservation pour l'information non évaluée est […]. Le ministre explique qu'il y a souvent une période entre le moment où la compromission débute et celui où elle est découverte. Par conséquent, l'efficacité des activités du CST dépend de la capacité à recouper et à analyser de l'information de multiples sources déjà acquise, y compris les indicateurs de compromissions découverts. La période de conservation […] permet au CST de remonter aux origines d'un événement ou d'examiner son évolution au fil du temps. 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 être utilisés non seulement pour les systèmes non fédéraux, mais aussi pour les systèmes fédéraux.

50. Après la période […], l'information non évaluée sera automatiquement supprimée, à moins qu'elle soit jugée « nécessaire » ou « essentielle » pour aider à protéger […] ou les systèmes fédéraux et les systèmes désignés comme étant d'importance. L'article 10.2 de l'EPM indique que l'accès à l'information non évaluée ([…]) doit être strictement contrôlé et limité aux personnes autorisées à mener ou à soutenir des activités de cybersécurité. La liste du personnel ayant un accès approuvé à l'information non évaluée est surveillée aux fins de reddition de comptes. L'information non évaluée ne peut pas être divulguée à l'extérieur du CST. En outre, la chef affirme dans la demande que chaque entité non fédérale dans ce cas-ci connaît l'utilisation de cette information et l'accepte.

51. 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. L'information est jugée « nécessaire » quand elle est requise pour

comprendre la cyberactivité malveillante, […], dans le but d'aider à protéger des systèmes non fédéraux. Par sa nature, cette information ne contient pas d'information liée à des Canadiens ou à des personnes se trouvant au Canada et est donc moins sensible que l'information jugée « essentielle ». Le but est d'aider à réaliser des analyses de détection et de prévention et à renforcer davantage l'écosystème de cyberdéfense.

52. L'information sur les Canadiens et les personnes se trouvant au Canada est considérée comme « essentielle » si, sans elle, le CST ne serait pas en mesure de découvrir, d'isoler, de prévenir ou d'atténuer des dommages aux systèmes non fédéraux. Cela peut inclure […]. L'information acquise peut être hautement sensible pour les Canadiens, et la plupart des analyses sont faites suivant des processus automatisés qui détectent les comportements anormaux et limitent l'exposition des employés au contenu des fichiers.

53. 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 ». Le suivi de cette information sera assuré en conformité avec l'article 11.2 de l'EPM, et les gestionnaires de l'exploitation devront examiner cette information sur une base trimestrielle pour vérifier si elle demeure essentielle. L'information qui n'est plus essentielle doit être supprimée.

54. Je suis d'avis que la conservation de l'information pour la durée requise permet au CST de concevoir les outils de cyberdéfense requis pour suivre l'évolution du savoir-faire des auteurs de menaces utilisant des logiciels malveillants. Cela permet une meilleure protection des systèmes non fédéraux et des systèmes fédéraux.

55. Étant donné les importantes restrictions sur l'accès à l'information non évaluée, l'exemple fourni et les examens trimestriels servant à confirmer que la conservation de l'information liée à des Canadiens demeure « essentielle », j'estime que la conclusion du ministre concernant la période d'évaluation […] est raisonnable. 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 non fédéraux peut être conservée jusqu'à ce qu'elle ne soit plus utile.

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

56. Les solutions de cybersécurité du CST ne s'appliquent qu'à l'acquisition d'information. Par conséquent, le CST accorde un vaste accès aux systèmes des entités non fédérales pour surveiller les activités malveillantes et acquérir un éventail d'information, y compris de l'information qui ne révèle pas l'existence d'une cybermenace. Ce faisant, il peut – et le fera presque certainement vu que les entités non fédérales sont situées au Canada – acquérir incidemment de l'information qui nuit à l'attente raisonnable en matière de protection de la vie privée de Canadiens ou de personnes se trouvant au Canada.

57. La jurisprudence du commissaire au renseignement reconnaît que le ministre n'est pas un expert technique. Toutefois, il est raisonnable, quand il formule des conclusions, de se fier à la détermination de la chef selon laquelle l'acquisition d'information est nécessaire pour découvrir, isoler, prévenir ou atténuer des dommages aux systèmes non fédéraux.

58. Le ministre explique que les auteurs de menaces déguisent délibérément leurs activités malveillantes. Il n'est pas possible pour le CST de prédire [...]. Par conséquent, afin d'atténuer efficacement les cybermenaces sophistiquées décrites dans la présente affaire et de prévenir les cybermenaces potentielles, le CST doit acquérir un large éventail d'information qui peut ensuite être évaluée pour repérer les activités malveillantes. L'information comprend [...].

59. Rien dans le dossier ne donne à entendre que le CST peut atteindre les mêmes résultats de cybersécurité en employant des solutions de cybersécurité différentes qui permettent d'acquérir moins d'information, tout particulièrement de l'information se rapportant à des Canadiens. Les conclusions du ministre contiennent des exemples de la façon dont l'information acquise au titre de cette autorisation peut aussi être utilisée par le CST pour appuyer des activités au titre d'autres autorisations de cybersécurité et sous d'autres volets de son mandat. Avant que l'information liée à des Canadiens ou à des personnes se trouvant au Canada puisse être utilisée, elle doit être évaluée pour déterminer si elle est essentielle pour découvrir, isoler, prévenir ou atténuer des dommages aux systèmes non fédéraux et aux

systèmes fédéraux. L'information qui ne répond pas au critère du caractère essentiel sera supprimée. Toute autre utilisation, analyse, conservation et divulgation d'information acquise au titre de l'autorisation est assujettie aux restrictions et aux conditions établies dans les politiques du CST.

60. Pour ces motifs, je suis convaincu que les conclusions du ministre sont raisonnables et qu'il a des motifs raisonnables de croire que l'acquisition d'information est nécessaire pour découvrir, isoler, prévenir ou atténuer des dommages aux systèmes.

iii. Les mesures de protection à la vie privée permettront de veiller à ce que l'information acquise au titre de l'autorisation qui est identifiée comme se rapportant à des Canadiens ou à des personnes se trouvant au Canada soit utilisée, analysée ou conservée uniquement si elle est essentielle pour découvrir, isoler, prévenir ou atténuer des dommages aux systèmes non fédéraux (art 34(3)d))

61. L'article 24 de la *Loi sur le CST* exige que le CST ait des mesures en place pour protéger la vie privée des Canadiens et des personnes se trouvant au Canada en ce qui a trait à l'utilisation, à l'analyse, à la conservation et à la divulgation d'information qui se rapporte à eux et qui a été acquise dans la réalisation des volets de son mandat touchant la cybersécurité et l'assurance de l'information. Au paragraphe 62 de l'autorisation, le ministre conclut qu'il a des motifs raisonnables de croire que les mesures dont il est question à l'article 24 ont été satisfaites.

62. Le ministre répète que l'information qui se rapporte à un Canadien ou à une personne se trouvant au Canada ne peut être conservée que si elle est évaluée comme étant essentielle, à savoir que le CST juge que sans elle, il serait incapable de découvrir, d'isoler, de prévenir ou d'atténuer des dommages aux systèmes d'entités non fédérales. Comme il est indiqué à la section 8.2.2 de l'EPM, le critère du caractère essentiel est évalué par des employés du CST accrédités et formés, à l'aide de processus manuels ou automatisés. Les employés doivent consigner les raisons pour lesquelles ils estiment que l'information est essentielle. Cette façon de procéder limite l'accès au contenu de l'information qui est très sensible pour les Canadiens et l'exposition à l'information non évaluée. À mon avis, ces mesures contribuent à

la conformité à l'obligation législative établie à l'article 24 de la *Loi sur le CST* et soutiennent les conclusions du ministre.

63. Les conclusions du ministre et le dossier expliquent comment l'information relative à des Canadiens ou à des personnes se trouvant au Canada peut être divulguée, ce qui correspond à l'obligation énoncée à l'article 44 de la *Loi sur le CST*. L'information est communiquée uniquement aux personnes ou aux catégories de personnes désignées en vertu de l'*Arrêté ministériel désignant des destinataires de renseignements canadiens d'identification acquis, utilisés et analysés en vertu de l'aspect de cybersécurité et de l'assurance de l'information du mandat du CST* émis le 13 juin 2023 en vertu de l'article 45 de la *Loi sur le CST*. Ces destinataires comprennent les propriétaires et les administrateurs d'un système ou d'un réseau informatique utilisé par le gouvernement du Canada ou une entité non fédérale, ainsi que les personnes et les catégories de personnes au sein d'entités étrangères avec lesquelles le CST a conclu des ententes. Afin de recevoir de l'information divulguée par le CST qui se rapporte à des Canadiens ou à des personnes au Canada, l'information doit être nécessaire pour aider à protéger des systèmes non fédéraux ou fédéraux.

64. Comme il est indiqué à la section 24 de l'EPM, 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. Par exemple, les renseignements personnels peuvent être supprimés afin d'éviter de dévoiler l'identité d'une personne. L'EPM établit également les niveaux d'approbation de la divulgation requis qui accompagnent les différents types d'information. Ces approbations doivent être documentées.

65. Je note que dans leur lettre de demande au CST, les entités non fédérales ont demandé que toute l'information personnelle ou confidentielle qui peut être recueillie et conservée soit masquée avant la divulgation. De plus, toute l'information qui n'est pas pertinente pour le mandat du CST doit être supprimée en conformité avec le calendrier de conservation du CST. Je comprends donc que toute divulgation d'information acquise au titre de l'autorisation devra d'abord respecter cette directive.

66. L'EPM énonce les politiques pour contrôler et protéger l'information concernant des Canadiens ou des personnes se trouvant au Canada qui est acquise au titre d'une autorisation de cybersécurité. Les employés du CST doivent documenter les motifs de la conservation, de l'utilisation et la divulgation de l'information liée à des Canadiens ou à des personnes se trouvant au Canada. À mon avis, lorsqu'elles sont suivies, ces mesures constituent un moyen efficace pour le CST de respecter l'exigence législative de protéger suffisamment cette information.

67. Je suis donc convaincu que la conclusion du ministre est raisonnable et qu'il a des motifs raisonnables de croire que l'information concernant des Canadiens ou des personnes se trouvant au Canada ne sera utilisée, analysée ou conservée que si elle est essentielle pour découvrir, isoler, prévenir ou atténuer des dommages aux systèmes des entités non fédérales.

V. REMARQUE

68. J'aimerais faire les remarques suivantes qui ne changent rien à mes conclusions concernant le caractère raisonnable des conclusions du ministre.

A. Consentement de toutes les personnes dont l'information peut être acquise

69. Afin de déployer des solutions de cybersécurité dans des systèmes non fédéraux, la *Loi sur le CST* exige que le CST obtienne une demande écrite – le consentement – du propriétaire ou de l'opérateur de ces systèmes. En comparaison, dans le cas des activités de cybersécurité dans les systèmes fédéraux, le ministre peut conclure qu'il existe des motifs raisonnables de croire que « le consentement des personnes dont l'information peut être acquise ne peut raisonnablement être obtenu » (art 34(3)b), *Loi sur le CST*).

70. Sur le plan conceptuel, l'information qui peut être acquise par le CST lorsqu'il fournit des services à une entité non fédérale « appartient » à cette entité non fédérale. Afin de délivrer une autorisation de cybersécurité, le ministre n'est pas tenu de déterminer si l'entité non fédérale a le pouvoir légal d'acquérir ou de communiquer l'information que le CST pourrait ultimement acquérir au moyen de ses solutions de cybersécurité, ce qui pourrait inclure des

éléments de consentement. Je ne dis pas que les entités non fédérales ici – ou en général – ne détiennent pas ce pouvoir légal. Je rappelle plutôt que les activités de cybersécurité soulèvent des enjeux complexes en ce qui a trait à la collecte et à l'utilisation d'information possiblement personnelle aux fins de cybersécurité et à l'obtention du consentement pour le faire. Étant donné l'importance accrue de la cybersécurité pour tous les Canadiens, ces enjeux devraient rester des enjeux centraux pour toutes les entités responsables de protéger l'information sensible.

VI. CONCLUSIONS

71. Comme il est indiqué dans la décision du [...] (annexe A), j'ai approuvé l'autorisation de cybersécurité pour des activités dans des infrastructures non fédérales, qui expire un an après la date de mon approbation.

72. Conformément à l'article 21 de la Loi sur le CR, une copie de ma décision et de sa motivation 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.

[...]

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