~~TRÈS SECRET//SI//LIMITED/RAC~~

Dossier : CST-2025-01

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 SUR 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
II. CONTEXTE 1
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 6
i. Examen des conclusions du ministre selon lesquelles les activités en cause sont raisonnables 6
ii. Examen des conclusions du ministre selon lesquelles les activités en cause sont proportionnelles 9
B. Paragraphe 34(3) de la *Loi sur le CST* – les conditions nécessaires à la délivrance d'une autorisation 11
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)) 11
ii. L'information à acquérir est nécessaire pour découvrir, isoler, prévenir ou atténuer des dommages aux systèmes non fédéraux (alinéa 34(3)c))) 14
iii. Les mesures visant à protéger la vie privée permettront d'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 (alinéa 34(3)d)) 15
V. REMARQUES 18
A. Contenu de la lettre de demande du propriétaire du système 18
B. Masquage des renseignements personnels et exclusifs avant la communication 20
C. Modification des dispositions relatives aux examens trimestriels 21
VI. CONCLUSIONS 23
ANNEXE A – Décision du CR rendue le [...]
ANNEXE B – Description de l'entité non fédérale et des activités

I. APERÇU

1. Le [...], j'ai rendu une décision approuvant une autorisation de cybersécurité pour des activités sur des infrastructures non fédérales (autorisation) pour une entité non fédérale – [...] – conformément à la *Loi sur le commissaire au renseignement*, LC 2019, c 13, art 50 (*Loi sur le CR*). Une copie de cette décision est jointe à l'annexe A.

2. L'autorisation a été délivrée le [...] par le ministre de la Défense nationale (le ministre) en vertu du paragraphe 27(2) de la *Loi sur le Centre de la sécurité des télécommunications*, LC 2019, c 13, art 76 (*Loi sur le CST*). Compte tenu du contexte de l'autorisation, j'ai accepté la demande du ministre d'examiner rapidement l'autorisation. À mon avis, le délai de trois jours entre la signature du ministre et la réception de l'autorisation par mon bureau n'a pas amoindri le caractère urgent de l'autorisation. D'après mon examen du dossier, je suis convaincu que les conclusions que le ministre a tirées en vertu des paragraphes 34(1) et (3) de la *Loi sur le CST* et sur lesquels s'appuie l'autorisation délivrée sont raisonnables. Afin d'éviter tout retard dans la capacité du Centre de la sécurité des télécommunications (CST) à fournir un soutien en matière de cybersécurité à l'entité non fédérale, le jour même où j'ai reçu l'autorisation et les documents connexes à examiner, j'ai rendu ma décision avec l'ensemble des motifs à suivre. Voici mes motifs.

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 électroniques, les appareils, les réseaux et l'information qu'ils contiennent contre les cybermenaces criminelles et parrainées par des États. Le CST fournit également des avis et des conseils pour renforcer la posture de cybersécurité de ces systèmes.

4. Afin de 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 portent atteinte à l'attente raisonnable en matière de protection de la vie privée des Canadiens ou des personnes se trouvant au Canada.

5. Avant d'entreprendre des activités pouvant avoir ces effets, le CST doit obtenir une autorisation délivrée par le ministre et approuvée par le commissaire au renseignement. Pour approuver les activités ou les catégories d'activités précisées dans l'autorisation, le commissaire au renseignement doit être convaincu que les conclusions du ministre – essentiellement les motifs justifiant la délivrance de l'autorisation – sont raisonnables (art 14, *Loi sur le CR*).

6. Une autorisation ministérielle permet au CST d'accéder à l'information électronique et aux infrastructures d'information appartenant soit à une institution fédérale – systèmes fédéraux (art 27(1), *Loi sur le CST*), soit à une entité non fédérale désignée comme étant d'importance pour le gouvernement fédéral – systèmes non fédéraux (art 27(2), *Loi sur le CST*), comme des entités œuvrant dans les secteurs de la santé, de l'énergie et des télécommunications. Le ministre peut autoriser le CST à acquérir de l'information qui provient ou passe par le système non fédéral, qui lui est destiné ou y est stocké afin d'aider à protéger cette infrastructure contre tout méfait, toute utilisation non autorisée ou toute perturbation de son fonctionnement.

7. Si l'autorisation vise un système non fédéral, le propriétaire ou l'opérateur du système doit demander par écrit au CST de mener des activités de cybersécurité pour protéger le système et ses informations électroniques (art 33(3), *Loi sur le CST*). La chef du CST doit ensuite présenter au ministre une demande écrite exposant les faits 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*).

8. Les paragraphes 34(1) et (3) de la *Loi sur le CST* précisent les autres conditions légales pour que le ministre puisse délivrer une autorisation de cybersécurité. L'autorisation est valide au moment où le commissaire au renseignement l'approuve (art 28(1), *Loi sur le CST*). Ce n'est

qu'à ce moment-là que le CST peut mener les activités autorisées précisées dans l'autorisation.

9. Malgré toute autorisation de cybersécurité, la *Loi sur le CST* impose des limites aux activités du CST. Le CST doit s'abstenir de mener quelque activité que ce soit visant un Canadien ou une personne se trouvant au Canada ou de contrevenir à la *Charte canadienne des droits et libertés* (art 22(1), *Loi sur le CST*). Toutefois, lorsqu'il mène des activités au titre d'une autorisation, le CST est autorisé à acquérir incidemment de l'information se rapportant à un Canadien ou à une personne se trouvant au Canada (art 23(4), *Loi sur le CST*). Le mot « incidemment » signifie que l'information acquise n'a pas été délibérément recherchée (art 23(5), *Loi sur le CST*).

10. Lorsque le CST acquiert des renseignements personnels se rapportant à un Canadien ou à une personne se trouvant au Canada, il doit suivre des mesures strictes prévues par la loi et les politiques à l'égard de telles informations. En effet, le CST est tenu de mettre en place des mesures visant à protéger la vie privée des Canadiens et des personnes se trouvant au Canada dans l'utilisation, l'analyse, la conservation et la divulgation de l'information qui se rapporte à eux (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 toute l'information dont il disposait pour accorder l'autorisation en cause. Voici les documents qui composent le dossier :

    a) la lettre du ministre adressée au commissaire au renseignement;
    b) l'autorisation;
    c) la note d'information de la chef du CST adressée au ministre;
    d) la demande de la chef, qui comprend neuf annexes, dont les suivantes :
        i. lettre de demande de l'entité non fédérale;
        ii. deux arrêtés ministériels;
        iii. tableau de conservation et suppression;
        iv. l'ensemble des politiques sur la mission en matière de cybersécurité (EPM), approuvé le 28 février 2022;

e) 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 des conclusions sur lesquelles repose une autorisation ministérielle afin de déterminer si ces conclusions sont raisonnables.

13. La jurisprudence applicable au commissaire au renseignement établit que la norme de la décision raisonnable, qui s'applique au contrôle judiciaire d'une mesure administrative, est la même que celle qui s'applique à mon examen.

14. Comme l'a indiqué la Cour suprême du Canada, lorsqu'elle procède au contrôle d'une décision 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.

15. Les contraintes factuelles et juridiques pertinentes peuvent comprendre 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 est nécessaire de tenir compte du 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 établi par la *Loi sur le CR* et la *Loi sur le CST*.

16. L'examen de ces lois et des débats législatifs connexes montrent que le législateur a créé la fonction de commissaire au renseignement en tant que mécanisme indépendant permettant d'assurer un juste équilibre entre les mesures prises par le gouvernement à des fins de sécurité nationale, le respect de la primauté du droit ainsi que des 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 droits en matière de vie privée et d'autres intérêts importants des Canadiens et des personnes se trouvant au Canada ont été dûment pris en compte et pondérés. Je dois aussi 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*). Si, au contraire, les conclusions sont jugées déraisonnables, il « n'approuve pas l'autorisation » (art 20(1)b), *Loi sur le CR*).

IV. ANALYSE

18. La chef a présenté au ministre une demande écrite d'autorisation de cybersécurité à l'égard de l'entité non fédérale (la demande). Cette demande comprend aussi la lettre de demande écrite de l'entité non fédérale pour le soutien du CST afin de mener des activités de cybersécurité.

19. Comme l'exige le paragraphe 21(1) de la *Loi sur le CST*, je suis convaincu que les systèmes de l'entité non fédérale appartiennent à une catégorie d'infrastructures de l'information qui sont importantes pour le gouvernement fédéral, comme il est désigné dans l'*Arrêté ministériel désignant l'information électronique et les infrastructures de l'information d'importance pour le gouvernement du Canada*, pris le 25 août 2020 – en particulier à titre de [...]

20. La demande décrit les solutions de cybersécurité qui seront déployées par le CST. Il s'agit des solutions suivantes : [...] et [...]

21. Une description de l'entité non fédérale, le contexte dans lequel elle a demandé le soutien du CST, ainsi que les activités exposées dans l'autorisation, se trouvent à l'annexe classifiée de la présente décision (annexe B). J'ai placé ces informations dans une annexe classifiée pour deux raisons. Premièrement, cela empêchera qu'une partie importante du texte de la présente décision soit caviardé, 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.

22. Le ministre a reconnu que, sans l'autorisation, les activités de cybersécurité exposées au paragraphe 76 de l'autorisation pourraient contrevenir à d'autres lois fédérales ou porter atteinte à une attente raisonnable en matière de protection de la vie privée de Canadiens ou de personne se trouvant au Canada. Compte tenu des faits exposés dans la demande que la chef a présentée, le ministre a conclu pour des motifs raisonnables que l'autorisation est nécessaire et que les conditions énoncées aux paragraphes 34(1) et (3) de la *Loi sur le CST* sont remplies. Par conséquent, le ministre a délivré une autorisation d'un an.

23. Je dois maintenant vérifier si les conclusions du ministre sur lesquelles repose l'autorisation délivrée sont raisonnables.

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

i. Examen des conclusions du ministre selon lesquelles les activités en cause sont raisonnables

24. Pour délivrer une autorisation de cybersécurité, 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*).

25. Le ministre a conclu, au paragraphe 34 de l'autorisation, qu'il y avait de tels motifs étant donné l'objectif d'aider à protéger les systèmes de l'entité non fédérale, et éventuellement les

systèmes fédéraux et d'autres systèmes d'importance contre tout méfait, toute utilisation non autorisée ou toute perturbation de leur fonctionnement.

26. 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, pour respecter l'interdiction, les activités de cybersécurité doivent viser les cybermenaces et ne pas viser des Canadiens. Je suis convaincu que les activités de cybersécurité exposées dans l'autorisation respectent cette exigence légale.

27. Le ministre explique que les activités de cybersécurité exposées dans l'autorisation présentent un risque que le CST puisse acquérir de l'information à l'égard de laquelle les Canadiens ou les personnes se trouvant au Canada ont une attente raisonnable en matière de protection de la vie privée. Étant donné que les solutions de cybersécurité acquièrent [...], je suis d'avis que le CST recueillera presque assurément de telles informations, ce qui met en évidence la nécessité de la présente autorisation.

28. Pour justifier le caractère raisonnable des activités, le ministre s'appuie sur trois motifs : 1) l'efficacité des activités pour lesquelles l'autorisation est demandée; 2) la nécessité du soutien du CST étant donné [...]; et 3) la menace pour les systèmes de l'entité non fédérale que représentent les auteurs de cybermenaces.

29. Premièrement, les activités exposées dans l'autorisation sont efficaces et complètent les autres activités de cybersécurité de l'entité non fédérale. Le ministre explique que la sophistication des cybermenaces les rend difficiles à découvrir. En s'appuyant sur l'information fournie par la chef, le ministre conclut que la posture de cybersécurité de l'entité non fédérale n'est pas suffisante pour identifier et contrer les moyens sophistiqués déployés par des auteurs de menaces avancés et persistants.

30. Les solutions de cybersécurité du CST ajoutent une couche de défense distincte et supplémentaire pour détecter des compromissions possibles. Le ministre explique que les connaissances et les cybersolutions du CST permettent de détecter et de réagir aux menaces

inconnues des fournisseurs commerciaux de cybersécurité. Compte tenu du contexte dans lequel l'autorisation a été délivrée, le CST [...] appuie également la conclusion du ministre selon laquelle les activités sont efficaces et raisonnables.

31. Je suis d'accord avec le ministre que les activités exposées dans l'autorisation permettent au CST de conseiller l'entité non fédérale et de mieux protéger ses systèmes. En effet, dans le cadre des activités, le CST pourrait recommander des mesures d'atténuation et les mener avec le consentement de l'entité non fédérale. Je suis également d'accord avec le ministre pour dire que le soutien du CST est encore plus pressant compte tenu de [...] de l'entité non fédérale.

32. Le deuxième motif exposé par le ministre pour lequel les activités du CST sont raisonnables est le rôle essentiel que jouent les systèmes de l'entité non fédérale [...] Ce rôle consiste effectivement à [...]. [...], l'entité non fédérale [...], l'entité non fédérale constitue une cible attrayante pour les auteurs de cybermenaces. [...]

33. Le troisième motif qui appuie la conclusion du ministre selon laquelle les activités sont raisonnables est le contexte actuel des cybermenaces. Une autorisation de cybersécurité a pour objet d'aider à protéger les systèmes et l'information de l'entité non fédérale (art 27(2), *Loi sur le CST*). Pour protéger les systèmes, il n'est pas nécessaire que des cybercompromissions soient présentes. Lorsque des activités de cybersécurité sont menées à des fins préventives ou proactives, le ministre doit démontrer qu'il existe un fondement factuel pour demander l'aide du CST (décision CST-2024-07, para 84). Comme il est indiqué dans ma décision de [...], le ministre a délivré l'autorisation de façon proactive; il n'y a pas de compromission ou de menace particulière pour l'entité non fédérale. Néanmoins, le dossier décrit en détail les auteurs de cybermenaces existants et contient de l'information sur la probabilité que les systèmes de l'entité non fédérale soient la cible de cyberactivités malveillantes – de l'information que j'ai ajoutée à l'annexe B.

34. Le ministre n'affirme pas avec certitude que l'entité non fédérale sera la cible d'auteurs de cybermenaces. La justification du ministre repose plutôt sur le fait que la cybermenace pour l'entité non fédérale existe en tant que corrélation directe avec le rôle essentiel qu'elle joue.

En effet, le CST estime que chaque province et territoire au Canada a probablement été ciblé par des auteurs de cybermenaces afin de recueillir du renseignement et que [...]. En même temps, le CST évalue que dans les circonstances actuelles, l'entité non fédérale est [...]

35. Je trouve que la justification du ministre est convaincante, que la nature de l'entité non fédérale en fait une cible probable pour les auteurs de cybermenaces. Je suis convaincu que le ministre a établi un fondement factuel suffisant de la menace pour les systèmes de l'entité non fédérale. Je trouve raisonnables les conclusions du ministre selon lesquelles les activités exposées dans l'autorisation sont raisonnables.

ii. Examen des conclusions du ministre selon lesquelles les activités en cause sont proportionnelles

36. Le ministre a également conclu, au paragraphe 34 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 menées ».

37. Je suis convaincu que les conclusions du ministre à cet égard sont raisonnables. Le ministre reconnaît que les activités de cybersécurité proposées peuvent mener à l'acquisition de grands volumes d'information pour découvrir des cybermenaces. Bien que certaines informations puissent porter atteinte aux droits en matière de vie privée, le ministre affirme que le CST s'intéresse aux comportements anormaux concernant l'information et non à son contenu.

38. Pour démontrer que les activités sont proportionnelles, le ministre expose sept mesures et contrôles internes appliqués par le CST pour assurer la protection de l'information qu'il acquiert :

a) aucune information non évaluée n'est conservée plus longtemps que [...] à compter de la date à laquelle elle a été acquise;
b) le CST conserve moins de 1 % de toutes les données qui ont initialement été acquises dans le cadre d'activités de cybersécurité;

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) chaque recherche effectuée sur l'information non évaluée acquise est vérifiable conformément à l'EPM;
e) l'accès à l'information acquise au titre 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;
f) tous les outils de cybersécurité sont passés en revue pour veiller à ce qu'ils soient conformes aux lois et aux politiques;
g) les mêmes conditions s'appliquent à l'information utilisée par le CST pour découvrir, isoler, prévenir ou atténuer les dommages aux systèmes fédéraux et à d'autres systèmes d'importance.

39. Je peux suivre le raisonnement du ministre lorsqu'il s'est appuyé sur ces mesures. Il conclut que les activités proposées justifient toute atteinte possible aux droits en matière de vie privée des Canadiens. Il décrit également comment les activités cherchent à atteindre un équilibre raisonnable entre l'atteinte éventuelle et les droits en matière de vie privée. Je suis convaincu que les droits des Canadiens et des personnes se trouvant au Canada ont été pris en compte et que la mise en balance est raisonnable.

40. L'exercice de mise en balance du ministre est également évident lorsqu'il expose les lois fédérales qui pourraient être enfreintes. Le ministre mentionne que leur nombre est limité, parce que le CST mènerait ses activités uniquement sur les systèmes pour lesquels il a reçu le consentement exprès du propriétaire. De plus, les activités doivent respecter la portée de celles décrites dans la demande de la chef et se limiter à l'acquisition de l'information pour protéger les systèmes non fédéraux et les systèmes fédéraux. Enfin, en cas de contravention à une loi fédérale qui ne figure pas dans la demande, la chef en informera le ministre et le commissaire au renseignement.

41. Les conclusions du ministre démontrent sa compréhension des droits en matière de vie privée et des mesures en place pour les protéger. 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

42. 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 les 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 permettront d'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 (alinéa 34(3)a))

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

44. Comme il n'est pas possible pour le CST de déterminer quelle information sera utile pour identifier les activités malveillantes, il acquiert un grand volume d'information des systèmes de l'entité non fédérale. Le ministre explique que le CST traite cette information, principalement par des méthodes automatisées. Ce processus permet de déterminer que certaines informations sont « nécessaires » ou « essentielles ». Toute autre information est jugée comme étant de l'information non évaluée, même si elle a été assujettie au processus automatisé. La période maximale de conservation de l'information non évaluée est de [...].

45. Le ministre explique que l'efficacité des activités du CST dépend de sa capacité à analyser plusieurs sources d'information acquise et à faire des recoupements, y compris les indicateurs de compromission trouvés. La période de conservation [...] de l'information permet au CST de remonter aux origines d'un événement ou d'examiner son évolution au fil du temps. La comparaison entre une compromission et des données non évaluées aide le CST à élaborer de meilleures mesures d'atténuation et des cyberinterventions qui peuvent être utilisées non seulement pour les systèmes non fédéraux, mais aussi pour les autres systèmes désignés comme étant d'importance et les systèmes fédéraux.

46. Après la période [...], l'information non évaluée sera automatiquement supprimée, à moins qu'elle soit jugée « nécessaire » ou « essentielle » pour aider à protéger le système non fédéral ou les systèmes fédéraux et d'autres systèmes désignés comme étant d'importance. La chef indique dans la demande que l'entité non fédérale comprend et accepte cette utilisation de l'information. La section 10.2 de l'EPM précise 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 transmise à d'autres organismes que le CST.

47. Le ministre a précisé que même si l'information non évaluée pourrait être conservée par le CST jusqu'à [...] du moment de l'acquisition, l'information est en réalité conservée jusqu'à un maximum de [...]. Cela signifie que si les scripts de conservation automatisés quotidiens ne fonctionnent pas correctement, les analystes en sont alertés et peuvent les rétablir avant [...] l'échéance de conservation de l'évaluation. Le ministre souligne également le

programme de conformité interne du CST qui a un processus établi pour intervenir en cas d'incident. Cette approche à couches multiples permet au CST de maintenir un écosystème solide de mesures de protection de la vie privée.

48. Comme il est indiqué au dossier, le critère du caractère « nécessaire » s'applique à l'information qui ne se rapporte pas à des Canadiens ou à des personnes se trouvant au Canada; quant au critère du caractère « essentiel », il s'applique à l'information qui se rapporte à des Canadiens ou à des personnes se trouvant au Canada. L'information est jugée « nécessaire » lorsqu'elle est requise pour comprendre la cyberactivité malveillante, [...], dans le but d'aider à protéger les systèmes non fédéraux. De par sa nature, cette information ne contient aucune information se rapportant à des Canadiens ou à des personnes se trouvant au Canada. Le but est d'aider à réaliser des analyses de détection et de prévention et à renforcer l'écosystème de cyberdéfense.

49. L'information se rapportant à des Canadiens et à des personnes se trouvant au Canada est considérée comme « essentielle » si, sans elle, le CST ne peut pas découvrir, isoler, prévenir ou atténuer des dommages aux systèmes non fédéraux. Cette information peut comprendre [...]. L'information acquise peut être hautement sensible pour des 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.

50. L'information qui a été jugée nécessaire ou essentielle pour découvrir, isoler, prévenir ou atténuer les dommages 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'EPM, et on rappelle aux gestionnaires de l'exploitation chaque trimestre d'examiner l'information reconnue et conservée se rapportant à des Canadiens ou à des personnes se trouvant au Canada afin de vérifier si elle est toujours essentielle. J'analyserai davantage cette question dans mes remarques.

51. Je suis d'avis que la conservation de l'information pour la durée nécessaire permet au CST de mettre au point les cyberinterventions nécessaires pour suivre l'évolution du savoir-faire

des auteurs de menaces utilisant des logiciels malveillants. Cela permet une meilleure protection des systèmes non fédéraux ainsi que des systèmes fédéraux.

52. Compte tenu des multiples couches de contrôles internes pour protéger la vie privée et de l'accès limité à l'information non évaluée, je trouve la conclusion du ministre concernant [...] période d'évaluation raisonnable. Je suis également d'accord avec le ministre lorsqu'il conclut que 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.

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

53. Le CST ne peut pas prédire [...]. Par conséquent, pour surveiller efficacement les systèmes de l'entité non fédérale et atténuer toute cybermenace éventuelle, le CST doit acquérir un large éventail d'informations. Ces informations sont ensuite évaluées afin de détecter des activités malveillantes. L'information comprend [...]. Comme les systèmes non fédéraux sont situés au Canada, le CST acquerra probablement incidemment de l'information portant atteinte à l'attente raisonnable en matière de protection de la vie privée des Canadiens et des personnes se trouvant au Canada.

54. Le ministre explique que même si les plateformes commerciales de cybersécurité sont actuellement utilisées par l'entité non fédérale, les solutions de cybersécurité du CST sont nécessaires pour offrir une meilleure protection, compte tenu de l'existence d'auteurs de menace sophistiqués et persistants. Le CST ne peut pas obtenir les mêmes résultats en utilisant différentes solutions de cybersécurité qui permettent d'obtenir moins d'information, en particulier de l'information se rapportant à des Canadiens.

55. 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 en vertu d'autres autorisations de cybersécurité et sous d'autres volets de son mandat. Avant que de l'information se rapportant à des Canadiens ou à des personnes se trouvant au Canada puisse être utilisée, elle doit avoir été évaluée comme étant essentielle à des fins de cybersécurité. L'utilisation, l'analyse, la conservation et la divulgation de toute information

acquise en vertu de l'autorisation sont assujetties aux restrictions et conditions énoncées dans l'EPM.

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

iii. Les mesures visant à protéger la vie privée permettront d'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 (alinéa 34(3)d))

57. L'article 24 de la *Loi sur le CST* exige que le CST veille à ce que des mesures pour protéger la vie privée des Canadiens et des personnes se trouvant au Canada soient en place en ce qui a trait à l'utilisation, à l'analyse, à la conservation et à la divulgation de l'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 67 de l'autorisation, le ministre conclut qu'il a des motifs raisonnables de croire que les mesures requises à l'article 24 sont en place.

58. Le ministre réaffirme que l'information qui se rapporte à des Canadiens ou à des personnes 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 de l'entité non fédérale. 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 fournir des justifications lorsqu'ils croient que de 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 au respect de l'obligation prévue à l'article 24 de la *Loi sur le CST* et appuient les conclusions du ministre.

59. Dans la décision CST-2024-05 relative à d'autres entités non fédérales, j'ai fait remarquer que l'information que le CST peut acquérir lorsqu'il fournit des services à une entité non fédérale « appartient » à cette entité. L'information pour laquelle il existe une attente raisonnable en matière de protection de la vie privée se trouvant dans le système d'une entité non fédérale pourrait finir par être conservée à des fins de cybersécurité par le CST, un organisme du gouvernement fédéral. Bien que la *Loi sur le CST* ne l'exige pas explicitement, le ministre devrait être en mesure de comprendre facilement que l'entité non fédérale a la juridiction initiale de recueillir l'information, et qu'il existe un fondement juridique pour partager l'information avec le CST. En réponse à cette remarque, la chef confirme dans une note d'information adressée au ministre ainsi que dans la demande que le CST a reçue, une confirmation verbale selon laquelle l'entité non fédérale a le pouvoir légal requis de recueillir et d'utiliser de l'information se rapportant à des Canadiens ou à des personnes se trouvant au Canada à des fins de cybersécurité. Pour les autorisations à venir, le CST s'efforce d'obtenir la confirmation par écrit. J'ajoute qu'il serait utile pour cette confirmation d'ajouter un aperçu de toutes les mesures prises par l'entité non fédérale pour aviser les utilisateurs de ses systèmes que leurs informations peuvent être recueillies et utilisées à des fins de cybersécurité et obtenir leur consentement.

60. En plus de conclure que l'information se rapportant à des Canadiens ne sera utilisée, conservée et analysée que si elle satisfait au critère du caractère essentiel, les conclusions du ministre et le dossier expliquent également comment l'information se rapportant aux Canadiens ou aux personnes se trouvant au Canada peut être communiquée. L'explication reflète l'obligation prévue à l'article 44 de la *Loi sur le CST*, à savoir que cette communication doit être nécessaire pour aider à protéger le système non fédéral, les systèmes fédéraux ou d'autres systèmes désignés comme étant d'importance. L'information est seulement communiquée aux personnes ou aux catégories de personnes énoncées dans l'*Arrêté ministériel désignant les destinataires de l'information qui se rapporte à un Canadien ou à une personne se trouvant au Canada qui a été acquise, utilisée ou analysée dans le cadre des volets du mandat du CST touchant la cybersécurité et l'assurance de l'information*, pris le 13 juin 2023 en vertu de l'article 45 de la *Loi sur le CST*. Ces destinataires comprennent les propriétaires ou les administrateurs de systèmes informatiques

ou de réseaux utilisés par le gouvernement fédéral ou une entité non fédérale, ainsi que les personnes et les catégories de personnes autorisées au sein d'entités étrangères avec lesquelles le CST a conclu des ententes.

61. 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 de l'information se rapportant à eux est communiquée. Par exemple, les renseignements personnels peuvent être supprimés afin d'éviter de dévoiler l'identité d'une personne. L'EPM décrit les niveaux d'approbation requis pour communiquer l'information selon les différentes catégories d'information. Ces approbations doivent être consignées.

62. Je constate que dans sa lettre de demande au CST, l'entité non fédérale a demandé que tous les renseignements exclusifs et tous les renseignements personnels qui pourraient être recueillis et conservés soient masqués avant la communication. Je soulève certaines inquiétudes dans mes remarques concernant cette question.

63. L'EPM établit des politiques complexes visant à contrôler et à protéger l'information se rapportant à des Canadiens et à des personnes se trouvant au Canada qui est acquise en vertu d'une autorisation de cybersécurité. Les employés du CST doivent consigner les justifications pour la conservation, l'utilisation et la communication de l'information se rapportant à des Canadiens et à des personnes se trouvant au Canada. À mon avis, lorsqu'elles sont suivies, ces mesures permettent au CST de respecter efficacement l'exigence prévue par la loi de protéger suffisamment cette information.

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

V. REMARQUES

65. J'aimerais faire les trois remarques suivantes, qui ne modifient pas mes conclusions concernant le caractère raisonnable des conclusions du ministre.

A. Contenu de la lettre de demande du propriétaire du système

66. Pour déployer des solutions de cybersécurité sur des systèmes non fédéraux, le CST doit obtenir la demande écrite du propriétaire ou de l'opérateur de ces systèmes. La demande doit accompagner la demande présentée au ministre (art 33(3), *Loi sur le CST*) et, par conséquent, fait partie de la trame factuelle soumise au décideur (*Vavilov*, para 94 et 126). En effet, dans l'autorisation, le ministre affirme que ses conclusions reposent non seulement sur « les faits et les observations exposés dans la demande », mais aussi « sur la demande écrite du propriétaire du système ».

67. La *Loi sur le CST* ne réglemente pas le contenu d'une lettre de demande. Toutefois, l'EPM – Cybersécurité prévoit que les lettres de demande doivent utiliser un modèle rédigé par la Direction des services juridiques du CST (section 18.1.1). À l'exception de quelques modifications mineures – et d'un ajout notable que j'aborde dans ma troisième remarque – la lettre au dossier reflète celles qui ont été reçues dans les autorisations de cybersécurité antérieures.

68. Bien qu'un modèle de lettre de l'entité non fédérale puisse satisfaire à l'obligation prévue par la loi, je fais la remarque suivante à prendre en considération dans le but d'améliorer la lettre et, par conséquent, l'information dont dispose le ministre au moment de décider si une autorisation peut être délivrée.

69. Le modèle de lettre n'explique pas pourquoi l'entité non fédérale demande le soutien du CST. Il présente plutôt une demande générale et comprend plusieurs énoncés selon lesquels l'entité non fédérale reconnaît et accepte que les solutions de cybersécurité du CST seront déployées sur ses systèmes. Le modèle de lettre constitue effectivement le consentement de l'entité non fédérale. En effet, l'EPM indique que l'objectif de la lettre est de saisir clairement le consentement du client pour que le CST puisse accéder à son infrastructure et

acquérir de l'information (section 18.1.1). Je conviens qu'il est important que le ministre soit au courant du consentement de l'entité non fédérale.

70. Le fondement factuel du soutien du CST doit donc être fourni dans la demande de la chef au ministre. En ce qui concerne les autorisations de cybersécurité relatives aux entités non fédérales, je suis convaincu que le ministre a compris pourquoi le soutien du CST était nécessaire, comme l'exige le paragraphe 33(2) de la *Loi sur le CST*. En effet, dans le dossier dont je suis saisi, une note d'information de la chef adressée au ministre précise que l'entité non fédérale avait exprimé des inquiétudes concernant l'existence de vulnérabilités inconnues dans ses systèmes, puisque ses produits commerciaux de cybersécurité ne sont pas en mesure de procéder à une analyse des vulnérabilités.

71. Néanmoins, étant donné que le ministre se fie à la lettre de demande pour permettre au CST d'accéder aux systèmes de l'entité non fédérale, je crois que le dossier dont il est saisi tirerait avantage d'une lettre qui fournit, à tout le moins, un aperçu général des raisons pour lesquelles l'entité non fédérale demande le soutien du CST. Je reconnais qu'il peut y avoir des situations où l'entité non fédérale pourrait ne pas être en mesure de fournir beaucoup d'information sur une cybermenace ou une compromission dans la lettre. Dans certains cas, le CST peut également avoir accès à d'autres informations qu'il ne peut pas communiquer à l'entité non fédérale et, le cas échéant, il doit continuer de fournir cette information au ministre.

72. Le fait d'ajouter des précisions supplémentaires dans la lettre de demande permet de formuler plus clairement les objectifs à atteindre et de veiller à ce que le consentement de la partie qui fait la demande soit pleinement éclairé. Cela pourrait également ajouter de l'importance aux situations dans lesquelles il pourrait être urgent que le ministre délivre une autorisation et que le commissaire au renseignement procède à son examen dans un délai plus court.

B. Masquage des renseignements personnels et exclusifs avant la communication

73. Dans ma décision rendue le [...] dans cette affaire, j'ai constaté que dans sa lettre de demande adressée au CST, l'entité non fédérale a demandé que tous ses renseignements exclusifs et personnels soient masqués avant qu'ils ne soient communiqués. La lettre de demande comprend également une attestation de la part de l'entité non fédérale selon laquelle l'information contenue ou communiquée dans les systèmes de l'entité non fédérale, « y compris les renseignements personnels et les communications privées, peuvent être acquise incidemment et utilisée, analysée, conservée ou divulguée par le CST/CCC [Centre canadien pour la cybersécurité] à des fins de cybersécurité » (soulignement ajouté). Une telle attestation n'a été ajoutée dans aucune des lettres de demande antérieures d'une entité non fédérale.

74. Je suis d'avis qu'il manque de clarté dans la lettre quant à savoir si l'entité non fédérale comprend bien les mesures de protection de la vie privée du CST. D'une part, l'entité non fédérale demande le masquage avant la communication de l'information, tandis que, d'autre part, le CST peut communiquer des renseignements personnels – et selon l'EPM, la communication d'information se rapportant à des Canadiens est autorisée sous certaines conditions.

75. Le manque de clarté est également évident dans l'autorisation. Au paragraphe 66 de l'autorisation, le ministre affirme ce qui suit : « L'utilisation, l'analyse, la conservation ou la divulgation d'informations acquises en vertu d'une autorisation de cybersécurité demeure assujettie à des restrictions relatives à l'information conservée à des fins de cybersécurité, y compris les conditions imposées par les clients ou les entités qui font la divulgation » (soulignement ajouté). L'EPM prévoit également que « l'utilisation, le traitement et la manipulation internes de cette information sont également assujettis à toutes les restrictions relatives à l'information conservée à des fins de cybersécurité, y compris les conditions imposées par les clients ou les entités qui font la divulgation » (section 26.2 de l'EPM) (soulignement ajouté). Si la demande de masquage de l'entité non fédérale constitue une « condition du client », je comprends que cette information dans l'autorisation signifie que le

CST ne pourrait pas communiquer des renseignements personnels ou des renseignements exclusifs de l'entité non fédérale sans que cette information soit masquée au préalable.

76. Toutefois, au paragraphe 71 de l'autorisation, le ministre indique que le CST peut communiquer de l'information à l'extérieur du CST qui pourrait avoir été tirée de l'information acquise, utilisée et analysée dans le cadre des activités menées en vertu de l'autorisation. Bien que le même paragraphe précise que la communication doit être nécessaire et faite uniquement aux personnes désignées dans l'arrêté ministériel approprié pris en vertu de l'article 45 de la *Loi sur le CST*, il n'y a aucune mention concernant la suppression ou le masquage de l'information avant la communication. En effet, en vertu de la *Loi sur le CST* et de l'arrêté ministériel du 13 juin 2023, de l'information se rapportant à des Canadiens peut être divulguée.

77. Je ne suis pas au courant des discussions qui ont eu lieu entre le CST et l'entité non fédérale, et il peut être clair pour les deux parties de quelle façon les renseignements personnels et exclusifs recueillis en vertu de l'autorisation peuvent être divulgués. Cependant, si je me fonde uniquement sur l'information au dossier, le manque de clarté crée un risque de mauvaise interprétation qui pourrait avoir une incidence sur le consentement de l'entité non fédérale. À l'avenir, les dossiers devraient être plus clairs sur la façon dont une demande de masquage de la part d'une entité non fédérale est appliquée et préciser si cette façon de faire respecte les politiques du CST relatives à la communication d'information se rapportant à des Canadiens. De plus, si le CST croit qu'il y a effectivement un risque que sa compréhension diffère de celle de l'entité non fédérale en ce qui concerne la communication de renseignements personnels et exclusifs, il serait utile que le CST clarifie cette question avec l'entité non fédérale.

C. Modification des dispositions relatives aux examens trimestriels

78. Ma dernière remarque concerne l'examen de l'information conservée se rapportant à des Canadiens et à des personnes se trouvant au Canada afin de déterminer si elle est toujours essentielle. Le libellé employé pour décrire le processus de détermination a changé dans les autorisations récentes sans que le changement soit apporté dans les dossiers connexes. Je suis

d'avis qu'à l'avenir, les autorisations pourraient bénéficier d'une clarification supplémentaire.

79. Dans la décision CST-2023-02, mes remarques portaient sur le sujet des critères de conservation de l'information « jusqu'à ce que l'information ne soit plus utile » (para 89 et 90). J'ai remarqué que le dossier ne contenait rien quant aux procédures en place pour examiner l'utilisation de l'information et la suppression de l'information qui n'est plus utile, y compris la fréquence des examens périodiques.

80. En réponse, dans la demande d'autorisation suivante (décision CST-2023-05), le dossier indiquait que « [s]ur une base trimestrielle, les gestionnaires de l'exploitation doivent examiner l'[information se rapportant à un Canada à ou une personne au Canada] (IRC) reconnue et conservée afin de déterminer si elle est toujours essentielle. L'information qui n'est plus essentielle doit être supprimée » (soulignement ajouté). De plus, la demande précise que cette exigence doit être ajoutée dans la prochaine version de l'EPM.

81. Depuis la décision CST-2024-07, y compris dans la présente affaire dont je suis saisi, les dossiers connexes ne mentionnent plus que les gestionnaires de l'exploitation « doivent examiner » l'IRC reconnue et conservée pour déterminer si elle est essentielle. On leur rappelle plutôt d'examiner cette information. De plus, le dossier ne fait plus référence à l'ajout de l'exigence d'examen dans une prochaine version de l'EPM.

82. Je ne sais pas si le changement dans le libellé employé dans le dossier reflète un changement réel dans la pratique. Aux fins de mon examen, il est important que l'information présentée au ministre reflète avec exactitude la façon dont le CST mène ses activités et que la politique du CST soit claire pour ses employés. Je remarque que le ministre et moi avons compté sur le fait que des examens de détermination sont effectués pour tirer chacun nos conclusions afin de délivrer des autorisations et de les approuver. J'attends avec intérêt un prochain dossier qui apportera plus de clarté sur cette question.

VI. CONCLUSIONS

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

84. Conformément à l'article 21 de la *Loi sur le CR*, une copie de ma décision et des présents motifs 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 prévu aux 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.

[...]

(Original signé)

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