National Security and Intelligence Review Agency

Office de surveillance des activités en matière de sécurité nationale et de renseignement

NON CLASSIFIÉ (version caviardée)

Examen de l'OSSNR 08-501-02

Le 8 janvier 2020

L'honorable Harjit Sajjan
Ministre de la Défense nationale
101, promenade du Colonel-By
Ottawa (Ontario), KIA 012

Objet : Examen des incidents liés à la vie privée et des erreurs de procédure autosignalés par le Centre de la sécurité des télécommunications

Monsieur le Ministre,

Par la présente, je vous soumets notre rapport d'examen des incidents liés à la vie privée et des erreurs de procédure autosignalés par le Centre de la sécurité des télécommunications (CST) dans le Dossier relatif aux incidents liés à la vie privée (DIVP). L'examen a été réalisé en vertu de l'alinéa 8(1)a) de la *Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement,* et le rapport vous est remis conformément à l'article 34 de cette même loi.

L'examen du DIVP est le tout premier examen du CST réalisé par l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR) depuis l'entrée en vigueur de la *Loi sur l'OSSNR*, en 2019. Compte tenu des circonstances uniques entourant la création récente de l'OSSNR et des divers problèmes de logistique et de procédure associés à cette transition, nous sommes reconnaissants au CST de nous avoir aidés à accomplir notre travail dans un délai convenable. Avant la conclusion de l'examen, les fonctionnaires du CST ont eu l'occasion de vérifier l'exactitude des faits.

L'OSSNR entend s'inspirer de son examen pour travailler avec le CST, dans le but de mieux comprendre et connaître sa mission et ses difficultés.

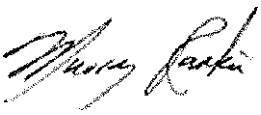
Les fonctionnaires de l'OSSNR travailleront avec le CST au caviardage du rapport définitif destiné au public. Nous espérons achever le processus de caviardage en huit semaines ou moins et entendons discuter de certains aspects de l'examen avec le Commissariat à la protection de la vie privée.

P.O. Box / C.P. 2430, Station / Succursale D
Ottawa, Canada K1P 5W5

Tel.: 1-833-890-0293 Fax: 613-907-4445

Comme je l'ai signalé dans ma lettre du 19 décembre 2019, je serai heureux de vous rencontrer pour discuter de cet examen et vous informer de façon plus générale du rôle de l'OSSNR.

Veuillez agréer, Monsieur le Ministre, mes salutations les plus sincères.



Murray Rankin,

Président, Office de surveillance des activités en matière de sécurité nationale et de renseignement

c.c. Shelly Bruce, chef du Centre de la sécurité des télécommunications

National Security and Intelligence Review Agency

Office de surveillance des activités en matière de sécurité nationale et de renseignement

NON CLASSIFIÉ

EXAMEN DES INCIDENTS LIÉS À LA VIE PRIVÉE ET DES ERREURS DE PROCÉDURE AUTOSIGNALÉS PAR LE CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS

(EXAMEN DE L'OSSNR 08-501-2)

P.O. Box / C.P. 2430, Station / Succursale D
Ottawa, Canada K1P 5W5
Tel.: 1-833-890-0293 Fax: 613-907-4445

I SOMMAIRE

1. Le Centre de la sécurité des télécommunications (CST) estime qu'il y a atteinte à la vie privée lorsque les renseignements personnels d'un Canadien ou d'une personne se trouvant au Canada sont exposés à un risque d'une manière non prévue à ses politiques ou contraire à celles-ci. Les atteintes à la vie privée sont inévitables en raison de la nature des activités du CST. L'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR) ne s'attend donc pas à ce que les activités du CST n'en génèrent aucune.

2. Dans le Dossier relatif aux incidents liés à la vie privée (DIVP), le CST signale et documente tous les incidents liés à la vie privée connus. L'OSSNR a examiné un échantillon d'incidents signalés dans le DIVP entre le 1er juillet 2018 et le 31 juillet 2019. Elle a consulté des dossiers électroniques, des fichiers, des pièces de correspondance et d'autres documents, tels que des politiques, procédures et conseils juridiques se rapportant aux incidents échantillonnés. En outre, son personnel a procédé à une vérification indépendante en comparant les renseignements obtenus du CST à ceux inscrits dans les systèmes du CST.

3. À la lumière des dossiers fournis par le CST et d'une vérification indépendante des incidents liés à la vie privée examinés, l'OSSNR estime que les mesures de conformité prises par le CST étaient opportunes et conformes aux politiques. Cependant, l'OSSNR a fait les cinq constatations suivantes assorties de recommandations, dans le but d'améliorer la documentation, l'évaluation et l'atténuation des incidents liés à la vie privée au CST :

- Le CST a choisi une approche à niveaux multiples pour renforcer ses mesures de protection des renseignements personnels. Il n'utilise toutefois pas le DIVP ou une compilation similaire d'incidents liés à la vie privée pour prévenir la répétition d'incidents systémiques ou pour relever les lacunes des politiques ou pratiques existantes. L'OSSNR lui recommande donc d'examiner la totalité des incidents liés à la vie privée, dans l'optique de cerner les tendances systémiques ou les lacunes des politiques ou pratiques susceptibles de réduire la fréquence des incidents.

- L'atténuation, la documentation et le signalement des incidents liés à la vie privée manquent de régularité et ne cadrent pas toujours avec les objectifs de transparence et de reddition de comptes de la politique interne du CST. Par ailleurs, les incidents ne sont pas systématiquement évalués dans le but d'en déterminer l'effet sur le caractère licite ou sur les renseignements personnels des Canadiens. L'OSSNR recommande au CST d'adopter une méthode uniforme d'évaluation et de documentation de tous les incidents liés à la vie privée.

- Certaines mesures d'atténuation prises après la découverte d'un incident consistent à supprimer les renseignements ayant un intérêt en matière de vie privée. Le CST ne vérifie pas l'usage réservé aux renseignements avant leur suppression, ni s'ils existent dans un format qui échappe à son contrôle. L'OSSNR recommande au CST de toujours vérifier l'utilisation faite des renseignements avant leur suppression, afin de déterminer si d'autres mesures d'atténuation s'imposent.

- En outre, l'évaluation du CST pour déterminer si un incident porte une atteinte importante à la vie privée est limitée. Conformément à la *Directive sur les pratiques relatives à la protection de la vie privée* du Secrétariat du Conseil du Trésor du Canada, le CST doit signaler les atteintes importantes à la vie privée. L'OSSNR recommande au CST de normaliser sa politique d'évaluation des incidents en vue de déterminer s'il y a atteinte importante à la vie privée.

- Enfin, la politique par laquelle le CST accorde

pour la divulgation par inadvertance du nom d'un Canadien ou d'une personne se trouvant au Canada dans des rapports de SIGINT, n'est pas une mesure d'atténuation convenable de l'effet sur la vie privée et du risque qui en découlent. L'OSSNR recommande au CST de cesser cette pratique ou d'obtenir un avis juridique concernant ce mécanisme d'atténuation.

4. Le présent examen ne comporte aucune analyse permettant de cerner les tendances ou les lacunes systémiques, éléments sur lesquels ont porté les examens antérieurs du DIVP réalisés par le Bureau du commissaire du Centre de la sécurité des télécommunications. Toutefois, les prochains examens de l'OSSNR en feront une priorité.

5. De plus, conformément à l'article 15.1 de la *Loi sur l'OSSNR*, l'OSSNR entend travailler avec le Commissariat à la protection de la vie privée, afin d'établir le processus de signalement des futurs incidents liés à la vie privée au CST.

II INSTRUMENTS HABILITANTS

6. Le présent examen a été réalisé sous l'autorité de l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR), conformément aux alinéas 8(1)a) et b), ainsi qu'aux articles 9 et 11, de la *Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement.*

III INTRODUCTION

7. Le Centre de la sécurité des télécommunications (CST) signale et documente toutes les atteintes à la vie privée associées à ses activités, ou à celles de ses organismes secondaires[1] ou partenaires nationaux, si les renseignements personnels d'un Canadien ou d'une personne se trouvant au Canada sont exposés à un risque d'une manière non prévue à ses politiques ou contraires à celles-ci. C'est ce qu'on appelle un incident lié à la vie privée[2]. Les incidents sont enregistrés dans un des trois dossiers secondaires, selon le lieu de l'incident et le préjudice qu'il risque de causer :

- **Dossier relatif aux incidents liés à la vie privée (DIVP) :** Le DIVP répertorie les incidents pour lesquels le CST a traité les renseignements personnels d'un Canadien (particulier ou entreprise) ou d'une personne se trouvant au Canada d'une manière contraire à la politique ou non prévue par celle-ci. Ce type de mauvaise gestion est qualifié d'« incident lié à la vie privée »[3].
- **Dossier relatif aux incidents liés aux organismes secondaires (DIA) :** Le DIA est un dossier des atteintes à la vie privée ou à la conformité qui mettent en cause un Canadien ou une personne se trouvant au Canada, et qui sont attribuables à un organisme secondaire ou à un partenaire national. Ces incidents peuvent être signalés par des partenaires ou par le CST, et sont aussi qualifiés d'« incidents liés à la vie privée »[4].

[1] Par organismes secondaires, on entend les organismes nationaux de cryptologie de l'Australie (Australian Signals Directorate), de la Grande-Bretagne (Government Communications Headquarters), de la Nouvelle-Zélande (Government Communications Security Bureau) et des États-Unis (National Security Agency). Le CST travaille avec eux dans le but de donner suite à des priorités mutuelles relatives à la communication de renseignements de sécurité et d'atteindre des objectifs communs.
[2] *Ensemble de politiques relatives à la mission,* partie A, section 33.4, et partie B, section 27.2.
[3] Communication de renseignements, *Procédure normale d'exploitation 4 : Gestion des incidents liés à la vie privée,* section 3.1.
[4] Communication de renseignements, *Procédure normale d'exploitation 4 : Gestion des incidents liés à la vie privée,* section 4.1.

- **Dossier des erreurs de procédure mineures (DEPM) :** Le DEPM répertorie les incidents liés à la conformité des activités, lorsque le CST traite inadéquatement les renseignements d'un Canadien ou d'une personne se trouvant au Canada, sans toutefois les disséminer à d'autres. Il s'agit d'une erreur de procédure[5].

8. Ces trois dossiers secondaires réunis forment le DIVP. Celui-ci sert à colliger les dossiers d'incidents autosignalés qui peuvent porter atteinte à la vie privée, malgré les mesures de protection en place. Il représente donc une partie des efforts déployés par le CST pour protéger les renseignements personnels des Canadiens. Il importe de reconnaître que le CST signale lui-même ces incidents. Il dit utiliser le DIVP pour démontrer sa conformité à ses politiques opérationnelles et aux exigences juridiques, et pour prévenir d'autres incidents[6].

9. L'OSSNR sait que les atteintes à la vie privée sont inévitables, étant donné la nature des activités du CST et l'infrastructure mondiale de l'information. À titre d'exemple,

l'OSSNR ne s'attend pas à ce que les activités du CST ne produisent aucune atteinte à la vie privée ni aucune erreur de procédure.

10. Le Bureau du commissaire du Centre de la sécurité des télécommunications (BCCST), auparavant l'organisme externe d'examen du CST, procédait à un examen annuel des incidents signalés dans le DIVP. Cette année, l'examen du DIVP est le tout premier examen du CST qu'effectue l'OSSNR depuis l'entrée en vigueur de la *Loi sur l'OSSNR*.

11. Compte tenu des circonstances uniques entourant la création récente de l'OSSNR et des nombreux problèmes de logistique et de procédure causés par cette transition, le présent examen n'aurait pas été possible sans l'aide du personnel du CST. L'OSSNR a dû se familiariser avec le cadre opérationnel et les activités uniques et complexes du CST, et du même coup réaliser l'examen. En s'appuyant sur ces premières notions, l'OSSNR travaillera avec le CST afin d'obtenir d'autres séances d'information technique qui lui permettront d'approfondir ses solides connaissances de base de la mission et des difficultés du CST.

IV CONTEXTE

12. Au CST, le signalement des incidents liés à la vie privée, l'atténuation de leurs effets et la consignation des incidents dans le DIVP sont des responsabilités partagées (voir le diagramme du processus à l'Annexe F). Selon le mandat sous lequel ils se produisent, les incidents sont gérés par deux équipes de la conformité différentes. est responsable des incidents liés à la vie privée qui s'inscrivent dans le mandat lié au renseignement étranger. Le s'occupe des incidents qui relèvent du mandat de cyberdéfense[7].

13. Généralement, dès qu'un incident se produit, les analystes le signalent à leur équipe respective de la conformité au moyen d'un formulaire Web; toutefois, certains incidents sont relevés à l'issue d'examens internes et d'activités de conformité. Après la découverte d'un incident lié à la vie privée, le documentent, l'atténuent et le surveillent en observant leurs politiques respectives[8].

14. Si, une fois l'incident géré et les activités de suivi terminées, un intérêt en matière de vie privée concerne un Canadien ou une personne se trouvant au Canada (intérêt dans l'optique de la protection de la vie privée au Canada), les détails de l'incident sont

[5] Communication de renseignements, *Procédure normale d'exploitation 4 : Gestion des incidents liés à la vie privée,* section 5.1.
[6] Communication de renseignements, *Procédure normale d'exploitation 4 : Gestion des incidents liés à la vie privée,* section 3.1.
[7] Communication de renseignements, « Dossier relatif aux incidents liés à la vie privée », présentation du 19 août 2019 à l'OSSNR.
[8] Réponse du CST à la DDR-6, questions 20 et 21, reçue le 16 octobre 2019 par l'OSSNR.

communiqués au groupe aux fins de leur inscription dans le DIVP[9]. informe des incidents dès qu'ils se produisent, tandis que signale les incidents sur une base trimestrielle. Une fois informé d'un incident à inscrire dans le DIVP, l'évalue afin de déterminer s'il porte une atteinte importante à la vie privée[10].

15. L'organisme secondaire responsable d'un incident communique directement avec , qui, entre autres choses, lui demande de prendre les mesures nécessaires pour atténuer l'atteinte à la vie privée du Canadien ou de la personne se trouvant au Canada.

16. Au cours de la période de référence, un nombre total combiné de 123 incidents ont été signalés dans le DIVP, le DIA et le DEPM. Dans le DIVP et le DEPM, incidents étaient attribuables au CST. De ce nombre, incidents s'inscrivaient dans le mandat lié au renseignement étranger du CST, dans son mandat de cyberdéfense, et dans son mandat d'assistance[11].

17. incidents dans le DIA, étaient attribuables à un partenaire national. communique les incidents dans le DIA. Les autres incidents liés à la vie privée découlaient des activités des organismes secondaires.
incidents

18. Les incidents peuvent être classés par type, et ce type dicte bien souvent les mesures d'atténuation correspondantes que prendrait le CST (l'Annexe C fournit une explication). Les incidents communs qui découlent des activités du mandat lié au renseignement étranger, comme les incidents de ciblage, de divulgation de nom, de et de recherche, sont visés par des politiques, procédures d'exploitation et outils de travail qui exposent la façon d'en atténuer les effets. D'autres types d'incident dont la portée et les conséquences varient sont moins comparables les uns aux autres, comme ceux touchant la manipulation et la conservation des données. Il n'existe aucune mesure d'atténuation normalisée pour ces types d'incident.

19. Voici les incidents qui figuraient dans le DIVP pendant la période de référence, par type d'incident (l'Annexe C décrit les types d'incident) et dossier secondaire :

	Collecte	Manipulation et conservation des données		Appellation	Recherche	Communication	Ciblage	Ciblage et divulgation de nom	Total
DIVP									
DIA									
DEPM									

20. Selon l'examen du DIVP réalisé par le BCCST pour la période du 1er juillet 2017 au 30 juin 2018, le CST avait relevé 44 incidents liés à la vie privée à inscrire dans le DIVP, 31 incidents dans le DIA, et 11 erreurs dans le DEPM. Même si le nombre d'entrées dans le

[9] Réponse du CST à la DDR-6, questions 20 et 21, reçue le 16 octobre 2019 par l'OSSNR. Sachez qu'un incident peut être considéré comme étant lié à la conformité, soit une activité contraire aux politiques mais ne comportant aucun aspect lié à la vie privée des Canadiens.
[10] Réponse du CST à la DDR-6, question 21, reçue le 16 octobre 2019 par l'OSSNR.
[11] Dans le DIVP, incidents consignés se sont produits dans le cadre du mandat d'assistance, partie C, du CST. Après clarification par l'OSSNR, l'incident a été associé par erreur au mandat C. Réponse du CST à la DDR-6, question 1, reçue le 29 octobre 2019 par l'OSSNR.

DIA et le DEPM est sensiblement le même que l'an dernier, celui du DIVP est à la hausse. En raison de la réception tardive des DIVP des quatre années précédentes[12], l'OSSNR n'a pas pu évaluer les tendances des incidents liés à la vie privée aux fins du présent examen.

V CONSTATATIONS ET RECOMMANDATIONS

Utilisations du DIVP au CST

21. Comme on peut le lire à la section 33.4, partie A (mandat lié au renseignement étranger), de son *Ensemble de politiques relatives à la mission* (EPM)[13], le CST doit signaler et consigner les incidents liés à la vie privée, afin de :

- se conformer aux politiques et aux lois;
- empêcher d'autres incidents similaires de se produire;
- cerner les lacunes des politiques ou pratiques actuelles.

22. De même, selon la section 27.2, partie B (mandat de cyberdéfense) de l'EPM, il incombe au CST de signaler et de consigner les incidents liés à la vie privée afin de :

- corriger ou atténuer le préjudice que pourrait subir une personne ou une entité;
- se conformer aux obligations légales en matière de reddition de comptes;
- empêcher d'autres incidents similaires de se produire;
- cerner toute possibilité de clarification dans les politiques ou pratiques existantes.

23. L'OSSNR croyait que le CST se servait des incidents signalés et documentés dans le DIVP pour prévenir des incidents similaires et relever les lacunes des politiques ou pratiques existantes. Cependant, elle a constaté que le CST ne les utilise pas pour prévenir la répétition d'incidents systémiques, cerner les lacunes des politiques ou pratiques existantes et réduire la fréquence des atteintes à la vie privée. Nous doutons de l'utilité du signalement et de la documentation des incidents liés à la vie privée, car le CST prend peu de mesures stratégiques ou utilise peu ces incidents pour réduire les éventuels effets de ses activités sur les intérêts des Canadiens en matière de vie privée.

24. Le CST applique des méthodes d'atténuation à certains types d'incident commun, de façon à éviter que la même situation de fait engendrant un incident ne se reproduise. Pour les incidents de ciblage, par exemple, un analyste protège le Canadien et les sélecteurs qui le concernent, de sorte qu'il ne soit pas ciblé de nouveau, prévenant ainsi un autre incident fondé sur les mêmes sélecteurs.

25. Constatation nº 1 : Lorsqu'une politique impose des mesures de conformité à des incidents liés à la vie privée, le CST utilise ces mesures de façon opportune et conforme à la politique.

26. L'OSSNR n'a rien trouvé qui puisse démontrer que le CST emprunte une approche stratégique ou globale pour réduire la fréquence totale des atteintes à la vie privée. Pendant la période de référence, n'a fait aucune recommandation à la haute direction qui soit fondée sur les lacunes relevées dans les politiques ou pratiques actuelles, à la suite d'un incident lié à la vie privée ou d'une erreur de procédure[14].

[12] Initialement sollicités dans la DDR-1 transmise au CST le 22 août 2019, et reçus par l'OSSNR les 15 et 24 octobre 2019.
[13] L'*Ensemble de politiques relatives à la mission* est le cadre stratégique du CST qui guide toutes les activités opérationnelles.
[14] Réponse du CST à la DDR-3, question 6, reçue le 4 octobre 2019 par l'OSSNR.

27. Pendant la période de référence, l'absence de modification apportée aux politiques et aux pratiques à la suite d'incidents liés à la vie privée soulève des questions, car ces incidents ont connu une hausse de 81 % depuis l'année précédente[15]. Au moyen d'une étude ou d'un examen, l'OSSNR se penchera sur l'augmentation des incidents liés à la vie privée.

28. Dans le cadre de conformité globale du CST, s'imposent pour maintenir un cadre annuel de conformité ou un plan annuel de réalisation des examens internes, et pour surveiller la conformité des activités aux politiques et procédures du CST. Les résultats des activités de conformité sont communiqués à la haute direction deux fois l'an, au moyen des rapports de conformité, lesquels font aussi état des incidents liés à la vie privée. Les examens réguliers de la conformité peuvent aussi étayer les recommandations adressées à la direction et aux équipes responsables des politiques.

29. L'OSSNR reconnaît que les cadres et activités internes de conformité jouent un rôle important dans l'application des politiques et mesures de protection des renseignements personnels du CST. Les efforts de conformité du CST sont alimentés par une expertise technique et une connaissance intime des activités. Cependant, l'OSSNR a constaté que les initiatives internes de conformité du CST se fondent sur les actuels cadres d'examen de la conformité, lesquels sont le produit des politiques et procédures en place.

30. Compte tenu des cadres de conformité annuels et des rapports dont disposait l'OSSNR au moment de l'examen[16], il a été difficile de cerner les mesures que prend le CST pour réduire les incidents systémiques liés à la vie privée du programme SIGINT. Les rapports sur les incidents liés à la vie privée semblent se concentrer sur leur nombre, et ils fournissent rarement une analyse détaillée de leur cause ou encore des recommandations visant à en réduire la fréquence. Les cadres d'examen de la conformité misent plutôt sur l'examen des activités, afin de veiller à ce que les mesures de protection des renseignements personnels sont en place et fonctionnent.

31. **Constatation nº 2 : Malgré son approche à niveaux multiples qui renforce les mesures de protection de la vie privée, le CST ne se sert pas du DIVP, ni d'aucun autre recueil similaire d'incidents liés à la vie privée, pour éviter de répéter des incidents systémiques ou pour relever les lacunes des politiques ou pratiques actuelles susceptibles de réduire la fréquence des incidents liés à la vie privée.**

Recommandation nº 1 : Le CST devrait examiner tous les incidents liés à la vie privée, dans l'optique de cerner les tendances systémiques ou les lacunes des politiques ou pratiques actuelles.

[15] Au total, 80 incidents étaient inscrits dans le DIVP entre le 1er juillet 2018 et le 31 juillet 2019, comparativement à 44 entre le 1er juillet 2017 et le 30 juin 2018.

[16] En ce qui concerne la DDR-1, l'OSSNR n'a été en mesure de consulter que le rapport de conformité annuel de SIGINT de 2017 et que les rapports semestriels de janvier à juin 2018, et de juillet à décembre 2018 de , puisque le rapport du premier semestre de 2019 n'était pas accessible au moment de l'examen. L'OSSNR a reçu les rapports de conformité interne de pour les périodes du 1er avril 2018 au 30 septembre 2018, et du 1er octobre 2018 au 31 mars 2019. Les autres rapports semestriels de la période de référence n'étaient pas disponibles au moment de l'examen.

32. Comme nous l'avons déjà indiqué, l'OSSNR comprend que la nature et le volume des activités du CST rendent inévitables les atteintes à la vie privée. Elle ne s'attend pas à ce que ces activités ne génèrent aucun incident lié à la vie privée ni aucune erreur de procédure. Cependant, le signalement et la documentation des incidents liés à la vie privée devraient servir d'outils pour les réduire de manière similaire. À l'heure actuelle, le cadre de conformité et de signalement ne semble pas assorti de plans stratégiques en vue de réduire les incidents liés à la vie privée qui se rapportent aux activités de SIGINT.

Évaluation et documentation des incidents liés à la vie privée

33. Le DIVP se veut un document sommaire qui n'expose pas tous les détails d'un incident donné. Pour son examen, l'OSSNR s'attendait à trouver tous les renseignements essentiels relatifs aux incidents dans les documents justificatifs, quel qu'en soit le format, notamment le formulaire Web de signalement ou les courriels échangés.

34. Après examen du DIVP et de tous les documents justificatifs, l'OSSNR a conclu que, dans le cadre du processus de gestion des incidents, le CST ne fait pas une analyse systématique approfondie des lois régissant l'incident et ses effets sur la vie privée, comme l'EPM l'y oblige.

35. L'EPM est un ensemble de principes stratégiques qui découlent du cadre juridique du CST, lequel est formé de la *Loi sur la défense nationale*, de la *Loi sur la protection des renseignements personnels,* des autorisations ministérielles, des instructions du ministre et de toute autre loi canadienne pertinente. L'EPM exige du CST qu'il atténue et documente les atteintes à la vie privée afin d'en informer la direction et de rendre des comptes. Les parties A et B de l'EPM présentent également la transparence et la reddition de comptes comme de vastes principes stratégiques qui régissent la conduite légitime des activités du CST[17]. Avant d'inclure un incident dans le DIVP, l'évalue, le documente et l'atténue en fonction de ses propres politiques. Cependant, l'OSSNR a constaté que l'approche d'évaluation et de documentation des incidents diffère entre et rend incohérente la manière dont le CST s'acquitte de ses obligations de transparence et de reddition de comptes.

36. Pour , la section 27.2.1, partie B de l'EPM, exige que chaque incident lié à la vie privée fasse l'objet d'un rapport, notamment pour évaluer :

- ce qui relie l'incident à la vie privée, dont les politiques ou les lois enfreintes;
- les mesures correctives et de prévention recommandées en vue d'éviter d'autres incidents de nature similaire;
- l'intérêt touché en matière de protection des renseignements personnels.

[17] Le vaste principe stratégique qui englobe la transparence et la reddition de comptes régit la conduite légitime des activités du CST relevant du mandat lié au renseignement étranger et du mandat de cyberdéfense, conformément à l'*Ensemble de politiques relatives à la mission* du CST. En vertu du mandat lié au renseignement étranger, les activités sont soumises à un examen interne et externe, et tous les dossiers connexes de décisions sont consignés et documentés pour en faciliter l'examen (EPM, partie A, section 2.5). Quant au mandat de cyberdéfense, les activités font l'objet d'un examen interne et externe, et doivent être assorties de documents facilitant le processus d'examen (EPM, partie B, section 2.5).

37. Les rapports renferment également une *Évaluation des facteurs relatifs à la vie privée* qui s'inspire d'un instrument d'évaluation de l'incidence, lequel favorise une analyse constante de la portée et de la gravité d'un incident lié à la conformité ou à la vie privée[18]. Ce calcul se fonde sur le risque pour la confidentialité, l'intégrité et la disponibilité des données. L'OSSNR a reçu un rapport pour chaque incident lié à la vie privée relevant de les rapports d'incident lié à la vie privée exposent clairement et en détail la façon dont a fait un suivi de chaque incident. De plus, les rapports démontrent que l'effet sur la protection de la vie privée de chaque incident compris dans l'échantillon de l'OSSNR a été évalué.

38. Les rapports ne justifient pas tous la méthode d'évaluation des incidents utilisée, ni ne précisent comment le risque pour la confidentialité, l'intégrité et la disponibilité des données est évalué à la lumière des circonstances de l'incident. L'OSSNR suggère que continue son examen de routine des effets de chaque incident sur la protection de la vie privée, et aille même jusqu'à veiller à ce que tous les rapports justifient les conclusions tirées de l'évaluation des répercussions.

39. En revanche, ne produit pas de rapport similaire sur chaque incident lié à la vie privée. À l'heure actuelle, le CST n'est pas tenu en vertu de ses politiques d'analyser systématiquement les effets de chaque incident sur la vie privée. La section 33.4.1, partie A de l'EPM, n'exige qu'une analyse des effets des cas complexes sur la vie privée. Par ailleurs, selon le guide de gestion des incidents de , une évaluation de l'effet sur la vie privée n'est réalisée que si l'incident est porté à l'attention de la haute direction.

40. L'OSSNR estime qu'à défaut de produire un rapport pour chaque incident lié à la vie privée, les pratiques de documentation et de signalement de ne reflètent pas les principes stratégiques de transparence et de reddition de comptes. Une politique qui reporte l'analyse des effets d'un incident sur la vie privée et ne tient pas compte des manquements aux instruments de politique n'affiche pas le degré requis de responsabilisation et de transparence.

41. L'information inscrite dans le DIVP et les documents justificatifs ne précise pas si l'effet de l'incident sur la vie privée est pris en compte. De même, elle n'indique pas de qui relève l'activité ni les manquements aux instruments de politique. Pendant la période de référence, les effets sur la vie privée d'un seul incident associé au SIGINT ont clairement été évalués, lorsqu'il a été présenté à la haute direction dans un rapport trimestriel sur le DIVP[19]. L'OSSNR qualifie d'inadéquate la pratique se limitant à n'évaluer que les effets sur la vie privée des incidents signalés à la haute direction, car elle permet une analyse faible ou inexistante des effets de tels incidents sur les renseignements personnels des Canadiens.

42. En outre, la méthode et les critères utilisés pour établir les effets sur la vie privée du seul incident associé au programme SIGINT signalé à la haute direction ne sont pas clairs. Pour cet incident, rapports renfermant ont été distribués incorrectement, si bien que personnes non autorisées ont consulté ces rapports. Pour déterminer les effets de l'incident sur la vie privée, on s'est demandé si l'incident risquait de causer un dommage ou un préjudice grave, critère qui sert à l'analyse d'une atteinte importante à la vie privée. Cette

[18] Réponse du CST à la DDR-6, question 13, reçue le 28 octobre 2019 par l'OSSNR.

[19] Incident réponse du CST à la DDR-4, question 6, reçue le 16 octobre 2019 par l'OSSNR. À titre d'information, cet élément a été signalé différemment étant donné qu'il a été relevé, examiné et atténué par , car il comportait une erreur de mise en œuvre technique d'un accord du Groupe des cinq, visant à limiter le dévoilement de certains rapports hiérarchiques. Par conséquent, cet incident a été traité différemment, puisqu'il a été décelé et géré par un secteur extérieur au programme .

analyse n'évoquait aucune autre obligation conférée au CST par l'EPM relativement à la protection des renseignements personnels, par la *Loi sur la protection des renseignements personnels* en ce qui a trait à l'utilisation et à la divulgation des renseignements personnels, par la *Loi sur la défense nationale* ou par toute autre exigence prévue aux autorisations ministérielles. Puisque l'OSSNR n'a trouvé aucun document indiquant que la Direction des services juridiques du CST est consultée lorsqu'un incident lié à la vie privée se produit, l'absence de directive ne lui permet pas d'établir la fréquence de cette pratique.

43. Par ailleurs, la documentation versée aux dossiers du CST semble indiquer que tout préjudice est limité, puisque les personnes qui ont accédé aux renseignements possèdent une cote de sécurité de niveau TRÈS SECRET, sont formées à l'utilisation de RENSEIGNEMENTS SPÉCIAUX et ont consulté le rapport . L'éventail et le nombre de personnes qui n'auraient pas dû consulter le rapport sont clairement des facteurs à prendre en considération. Même si la possession de la cote de sécurité requise pour accéder au rapport n'élimine pas tous les effets sur la vie privée, le CST ne s'est pas penché sur l'utilisation qui peut avoir été faite de ces renseignements. De plus, invoquer la cote de sécurité comme facteur atténuant dans l'évaluation de l'atteinte à la vie privée ne tient pas compte du « besoin de savoir » à la base de tous les rapports de SIGINT.

44. Faute d'indiquer les manquements aux instruments politiques ou juridiques et d'évaluer l'effet des incidents sur la vie privée, la responsabilité est incomplète et les normes de reddition de comptes et de transparence ne sont pas respectées. Lorsqu'aucun document n'appuie l'évaluation d'un incident, par exemple, il semble que le CST conclue tout simplement à son faible effet sur la vie privée. La portée de l'effet d'un incident n'étant pas rigoureusement évaluée, des incidents similaires risquent de se reproduire et les lacunes des politiques ou pratiques existantes pourraient passer sous le radar.

45. L'absence de rapports d'incident de SIGINT a fait en sorte que l'OSSNR a eu du mal à repérer les mesures d'atténuation et à en faire le suivi, surtout lorsque l'OSSNR a demandé au CST de lui produire des documents à l'appui. L'OSSNR a constaté que pour les incidents relevant de , les documents justificatifs étaient rares, irréguliers et parfois incomplets[20]. Il était donc difficile de comprendre l'exposé et le contexte d'un incident associé au SIGINT, qu'on y trouve une analyse de l'incident ou que des mesures d'atténuation aient été prises. Une présentation homogène du rapport d'incident produirait un compte rendu plus complet et fournirait à l'OSSNR et à la direction du CST assez d'information pour évaluer l'incident.

46. **Constatation n° 3 : L'approche irrégulière qu'emprunte le CST pour évaluer et consigner les incidents liés à la vie privée ne permet pas l'atteinte des objectifs de transparence et de reddition de compte de l'autosignalement de ces incidents.**

[20] À titre d'exemple, dans les cas de ou de ciblage pour lesquels des données doivent être éliminées, les documents justificatifs ne contiennent pas toujours une confirmation par courriel de l'élimination des données. Pour d'autres incidents, les pièces de correspondance évoquées ne figuraient pas dans les documents justificatifs. Voir la DDR-6, question 16 : Veuillez confirmer… qu'il y a eu nettoyage ou suppression pour les incidents suivants.

Recommandation nº 2 : devrait émuler la méthode de signalement des incidents liés à la vie privée de , de sorte que chaque incident comportant un intérêt en matière de protection de la vie privée au Canada fasse l'objet d'un examen.

47. L'OSSNR suggère que pour chaque incident lié à la vie privée, les rapports devraient :

- indiquer sous quel programme ou autorité l'activité a été réalisée;
- préciser les instruments de politique ou habilitants qui ont été enfreints;
- évaluer et consigner les effets de l'incident sur la vie privée.

48. dispose déjà d'outils pour encadrer l'adoption d'une telle exigence. Un incident survenu pendant la période de référence comportait un rapport d'incident , lequel exposait en détail l'incident, sa cause, les mesures d'atténuation, les recommandations de mise et la nécessité, le cas échéant, de porter l'incident à l'attention de la direction[21]. De plus, le questionnaire d'entrevue auprès des intervenants[22] de renferme des renseignements utiles et essentiels qui sont actuellement absents du DIVP ou des documents à l'appui, comme une série de questions en vue de déterminer si les renseignements personnels des Canadiens ont été compromis. Ces outils pourraient servir à la collecte de données et à la documentation d'un incident, et ainsi favoriser une compréhension et une évaluation exhaustives.

Mesures d'atténuation des incidents lié à la vie privée

49. L'OSSNR a constaté que les mesures d'atténuation de se limitent à mettre fin au préjudice éventuel après la découverte d'un incident. Pour certains types d'incident, comme ceux pour lesquels le CST a toujours contrôlé l'information, des mesures tournées vers l'avenir suffisent à limiter le préjudice. Quant aux incidents où de l'information sur l'identité de Canadiens (IIC) a été divulguée à tort, où la création de produits en matière de SIGINT a entraîné le ciblage par inadvertance d'un Canadien, et où les produits en matière de SIGINT ont propagé par inadvertance de l'IIC non supprimée, le CST annule ou supprime l'information. Habituellement, le CST annule ou supprime l'information sans chercher à savoir si elle a été utilisée.

50. Même s'il est pratique courante pour de demander les registres de consultation des rapports annulés à la suite d'une atteinte à la vie privée, ne détermine pas systématiquement qui pourrait avoir consulté un rapport avant son annulation. Le CST est en mesure de vérifier les registres de consultation pour déterminer qui a eu accès à des renseignements ayant un intérêt en matière de vie privée par l'entremise de . Pour certains incidents, a vérifié l'identité des personnes qui ont consulté les rapports avant leur annulation, afin de déterminer l'ampleur de la consultation[23]. Cet exercice ne s'est toutefois pas répété chaque fois qu'un rapport fournissait par inadvertance de l'IIC non supprimée. C'est là un problème, car il faut parfois connaître le nombre de personnes ayant

[21] Incident
[22] Ce questionnaire figure dans le guide de gestion des incidents , et il a été conçu afin que documente tous les détails d'un incident porté à l'attention de la haute direction.
[23] À titre d'exemple, lorsque avant son annulation.

consulté un rapport pour saisir la portée de l'atteinte à la vie privée d'une personne. De plus, le CST ne vérifie généralement pas si des renseignements ayant un intérêt dans l'optique de la protection de la vie privée au Canada pourraient exister dans un autre format, comme une copie imprimée du rapport.

51. Lorsqu'un produit de SIGINT comportant un intérêt dans l'optique de la protection de la vie privée au Canada est divulgué par inadvertance par , le rapport de SIGINT est annulé ou republié comme mesure d'atténuation, de sorte que toute l'IIC soit correctement supprimée. Le rapport annulé est automatiquement rayé des systèmes, prévenant ainsi d'autres utilisations des renseignements. Le superviseur de l'auteur du rapport est ensuite responsable de vérifier que l'information a été retirée de tous les fonds de renseignements. Tous les utilisateurs sont avisés de l'annulation ou de la correction d'un rapport du CST ou d'un organisme secondaire qu'ils ont consulté, et ils reçoivent pour directive de détruire les copies de ce rapport et les renseignements qui en découlent. Le rapport annulé ne peut plus être utilisé ou disséminé, car il n'y a plus de rapport auquel se reporter sur [24].

52. L'OSSNR estime que l'annulation d'un produit de SIGINT ne suffit pas à atténuer le préjudice éventuel attribuable à l'inclusion, par inadvertance, des renseignements personnels des Canadiens dans un rapport. Même si l'annulation du rapport limite dès lors le préjudice éventuel, les renseignements comportant un intérêt dans l'optique de la protection de la vie privée au Canada ont tout de même servi avant l'annulation. À titre d'exemple, la politique du CST autorise les clients des services de SIGINT à utiliser les données de SIGINT pour effectuer des recherches et orienter la collecte de renseignements au sein de leur ministère. Au moyen d'une demande d'intervention[25] ou de nettoyage[26], les clients des services de SIGINT peuvent aussi demander au CST la permission d'utiliser l'information à d'autres fins.

53. Cependant, le CST ne vérifie pas si un rapport qui contient de l'information relative à la protection de la vie privée au Canada a fait l'objet d'une demande d'intervention ou de nettoyage, et il ne communique pas avec les clients ayant consulté ce rapport pour savoir s'ils l'auraient utilisé pour orienter la collecte de renseignements[27]. Les demandes d'intervention et de nettoyage pourraient indiquer s'il y a eu utilisation des renseignements recueillis ou communiqués par inadvertance qui comportent un intérêt dans l'optique de la protection de la vie privée au Canada, auquel cas les risques de préjudice s'en trouveraient accrus. Les effets de l'incident lié à la vie privée et le préjudice éventuel ne sont pas évalués à fond, puisque le CST ne cherche pas à savoir qui a accédé aux renseignements et l'utilisation qui en a été faite.

54. L'OSSNR signale que pour tous les incidents liés à la vie privée qui ont fait l'objet d'un rapport, le CST devrait systématiquement vérifier le registre de consultation et l'existence de demandes de nettoyage ou d'intervention. Si de telles demandes ont été déposées, le CST devrait effectuer un suivi auprès de l'organisme demandeur, afin de s'assurer que l'atteinte à la vie privée du particulier est correctement évaluée et atténuée en conséquence. Si le CST arrive à confirmer la consultation du rapport, mais qu'aucune demande d'intervention ou de nettoyage n'a été présentée, il devrait évaluer le risque dans le but de déterminer s'il doit communiquer

[24] Réponse du CST à la DDR-6, question 20(4), reçue le 16 octobre 2019 par l'OSSNR.
[25] Une intervention s'entend de toute mesure ou décision d'agir qui se fonde sur des renseignements de SIGINT.
[26] Le nettoyage consiste à réviser ou à autrement distinguer les RS, de manière à protéger les sources, méthodes et techniques ou autres aspects sensibles des données, et à fournir une couverture plausible. Le but du nettoyage est de permettre une dissémination plus étendue des renseignements à l'extérieur des réseaux de RS.
[27] Réponse du CST à la DDR-8, question 2(b), reçue le 18 octobre 2019 par l'OSSNR.

avec les personnes ayant consulté le rapport, afin de leur demander si les renseignements ont été utilisés et si la personne concernée a subi un préjudice. L'évaluation des risques devrait tenir compte du type de renseignements divulgués par inadvertance, des personnes qui les ont consultés et de tout autre renseignement pertinent.

55. Il arrive que des renseignements comportant un intérêt en matière de protection de la vie privée au Canada existent ou puissent exister à l'extérieur des réseaux de SIGINT, et que leur annulation est impossible. À titre d'exemple, un incident lié à la vie privée concernait CST a annulé le rapport, le rendant ainsi automatiquement inaccessible . Cependant, le rapport peut avoir été copié sur support papier ou électronique avant son annulation. L'avis d'annulation des rapports transmis aux utilisateurs évoque cette possibilité, et il les charge d'éliminer toutes les copies imprimées et électroniques du rapport annulé[28]. Pour cet incident, le CST n'a pas communiqué avec pour s'assurer que le rapport incorrectement disséminé avait été éliminé de tous leurs systèmes, et non seulement des dépôts de rapports[29].

56. Il se peut que les renseignements comportant un intérêt dans l'optique de la protection de la vie privée au Canada perdurent à l'extérieur de , et que l'annulation du rapport ne les élimine pas entièrement. incidents liés à la vie privée pour lesquels un produit touchant la protection de la vie privée au Canada a été créé et diffusé par l'entremise de [30], le CST aurait dû examiner l'identité des personnes ayant consulté le rapport et vérifier si une demande d'intervention ou de nettoyage avait été déposée. Ces renseignements indiqueraient la portée de l'éventuelle atteinte à la vie privée et, au besoin, les mesures correctives à prendre autres que la simple annulation d'un rapport.

57. Quant à certains incidents inscrits dans le DIVP, même s'il savait qui avait consulté les renseignements touchant la protection de la vie privée au Canada, le CST n'a effectué aucun suivi auprès de ces personnes. Il maintient que l'annulation des rapports sur fournit les protections nécessaires en empêchant toute autre divulgation des renseignements et toute autre activité visant l'entité en question. n'a pas toujours vérifié auprès des utilisateurs non autorisés que les renseignements n'avaient pas été utilisés ou conservés, ou n'étaient plus disséminés. Pour les incidents , le CST n'a pas été en mesure de confirmer ou de démontrer qu'un tiers avait supprimé les renseignements comportant un intérêt dans l'optique de la protection de la vie privée au Canada[31]. Au moment de procéder au présent examen, la portée de l'utilisation ou de la conservation de ces renseignements demeure incertaine.

58. Pour incidents différents, le temps écoulé entre le moment où l'incident s'est produit et sa découverte a servi à justifier l'absence de vérification des effets de l'incident ou d'atténuation complète du préjudice éventuel[32]. Le CST voit le passage du temps comme un facteur à considérer dans le choix de la méthode la plus efficace pour atténuer une atteinte à la vie privée[33].

---

[28] Réponse du CST à la DDR-6, question 2(d), reçue le 28 octobre 2019 par l'OSSNR.
[29] Réponse du CST à la DDR-6, question 2(c), reçue le 28 octobre 2019 par l'OSSNR.
[30] Incidents
[31] Incidents réponse du CST à la DDR-6, question 16, reçue le 30 octobre 2019 par l'OSSNR.
[32] Incidents
[33] Réponse du CST à la DDR-6, question 7(a), reçue le 28 octobre 2019 par l'OSSNR. , de l'IIC a été envoyée par erreur à , qui ne l'a pas retirée. Puisque l'IIC a été divulguée au moins six mois avant la découverte de , il a été décidé que toute utilisation de l'information (sujette à des mises en garde) aurait déjà été faite. L'OSSNR constate que le CST n'a pas

59. Le CST devrait atténuer les effets d'un incident dont il est responsable. Il n'y a aucun lien entre le passage du temps et la probabilité réduite que les renseignements aient été conservés ou plus tard utilisés. Par conséquent, le temps qui s'écoule entre l'incident et sa découverte n'éteint pas l'obligation du CST de vérifier si les renseignements touchant la protection de la vie privée ont été utilisés ou conservés.

60. Pour atteintes à la vie privée qui s'inscrivent dans le mandat de cyberdéfense[34], le CST sait qui a accédé à l'information comportant un intérêt dans l'optique de la protection de la vie privée au Canada, mais présume que le temps écoulé rend le souvenir de ces données peu fiable. données renfermant de l'IIC ont été copiées sur une plate-forme interne accessible à tout le personnel du CST. À l'aide des registres d'utilisateurs du programme, a vérifié qui avait accédé à l'information sans disposer des autorisations nécessaires. n'a pas communiqué avec ces personnes pour s'assurer que l'information n'avait pas été utilisée ni conservée. Étant donné le temps qui s'est écoulé entre la découverte de l'incident et la date du dernier accès à l'information, estime que les personnes ne se souviendraient sans doute plus de l'incident, et que leur déclaration, à savoir s'ils avaient utilisé ou enregistré les données, manquerait de fiabilité[35].

61. L'OSSNR désapprouve l'explication que donne le CST de son défaut de vérifier si les renseignements comportant un intérêt pour la protection de la vie privée au Canada ont été utilisés ou conservés, en cas d'écart entre le moment où l'incident se produit et sa découverte. L'hypothèse voulant que les réponses des personnes seraient peu fiables ne dégage pas le CST de son obligation de s'enquérir de cette possibilité. De même, l'hypothèse ne tient pas compte de l'aspect préoccupant de la conservation, par ces personnes, de renseignements comportant un intérêt pour la protection de la vie privée au Canada.

62. **Constatation n° 4 : Les mesures d'atténuation que le CST applique à certains incidents liés à la vie privée après leur découverte se limitent à la suppression de renseignements touchant la protection de la vie privée, sans que soit vérifiée l'utilisation ou l'extraction des renseignements avant leur suppression.**

Recommandation n° 3 : Le CST devrait toujours examiner l'utilisation qui pourrait avoir été faite des renseignements comportant un intérêt dans l'optique de la protection de la vie privée au Canada, afin de déterminer si les circonstances d'une atteinte particulière à la vie privée justifient d'autres mesures d'atténuation.

Évaluation réalisée par le CST pour déterminer si un incident porte une atteinte importante à la vie privée

reconsidéré cette décision de ne pas agir après l'Examen annuel des divulgations d'information sur l'identité de Canadiens réalisé en 2017-2018 par le BCCST. Le 25 juillet 2019, le CST a demandé le retrait de renseignements divulgués par erreur, ce que confirme le 30 juillet 2019.

[34] Incidents

[35] Réponse du CST à la DDR-3, question 38, reçue le 15 octobre 2019 par l'OSSNR. Réponse du CST à la DDR-6, questions 8 et 12, reçue le 30 octobre 2019 par l'OSSNR.

63. Conformément à la *Directive sur les pratiques relatives à la protection de la vie privée* du Secrétariat du Conseil du Trésor du Canada (SCT), le CST doit signaler toute atteinte importante à la vie privée. Selon le CST, une entente conclue en 2016 autorise une structure de rapport divisée qui consiste à signaler au BCCST toute atteinte à la vie privée associée à des activités opérationnelles sensibles, et au Commissariat à la protection de la vie privée (CPVP) toute atteinte importante à la vie privée[36]. L'OSSNR étudiera les solutions de suivi auprès du CPVP que prévoit l'entente prise en 2016 avec le BCCST.

64. Les lignes directrices du SCT signalent qu'il y a atteinte importante à la vie privée si :

- l'atteinte concerne des renseignements personnels sensibles;
- on peut raisonnablement penser que l'atteinte causera un préjudice ou un dommage grave à la personne ou touche un grand nombre de personnes[37].

65. Au cours de la période de référence, le CST n'a signalé aucune atteinte importante à la vie privée[38]. À ce jour, par ailleurs, le CST n'a qualifié d'importante aucune atteinte à la vie privée[39].

66. Selon le CST, les atteintes importantes à la vie privée sont déterminées en fonction des directives du SCT[40]. Le groupe est responsable de déterminer si un incident lié à la vie privée porte une atteinte importante à la vie privée, une fois l'incident communiqué à pour la saisie des données dans le DIVP. Après chaque incident lié à la vie privée au CST, l'éventualité d'une atteinte importante à la vie privée doit être évaluée[41].

67. On note cependant des comptes rendus contradictoires quant à la façon dont le CST applique les lignes directrices du SCT à l'évaluation d'un incident. Dans une réponse à une DDR envoyée le 16 octobre 2019 à l'OSSNR, le CST explique que pour appliquer les lignes directrices du SCT à un incident, détermine si l'incident soulève des renseignements personnels sensibles[42]. évalue ensuite si la personne concernée a subi un grave préjudice; le CST estime toutefois qu'un préjudice grave est très peu probable en raison des voies classifiées qu'emprunte chaque incident[43].

68. La version provisoire de la *Procédure normale d'exploitation 4 : Gestion des incidents liés à la vie privée* (PNE) du CST décrit le processus que doit emprunter l'analyste pour évaluer un incident et déterminer s'il y a atteinte importante à la vie privée. Cette PNE reste une version provisoire, mais on nous a expliqué que les procédures qui y sont décrites sont représentatives de la gestion du DIVP pendant la période de référence[44]. Comme le veut la section 3.4 de la PNE, lorsqu'un incident lié à la vie privée est signalé, l'analyste évalue la présence de renseignements personnels sensibles. S'il en relève, il vérifie les bases de données pour déterminer si une demande d'intervention a été traitée à l'égard de ces

[36] Lettre du 27 janvier 2016 envoyée par le secrétaire du Conseil du Trésor à la chef du Centre de la sécurité des télécommunications.
[37] Voir www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/privacy/breach-managementimaterial-privacy-breaches.html.
[38] Réponse du CST à la DDR-3 question 1, reçue le 4 octobre 2019 par l'OSSNR.
[39] Réponse du CST à la DDR-6 question 22.1, reçue le 16 octobre 2019 par l'OSSNR.
[40] Réponse du CST à la DDR-3 question 1, reçue le 4 octobre 2019 par l'OSSNR.
[41] Réponse du CST à la DDR-6 question 21(1), reçue le 16 octobre 2019 par l'OSSNR.
[42] Réponse du CST à la DDR-6, question 21(1), reçue le 16 octobre 2019 par l'OSSNR.
[43] Réponse du CST à la DDR-6, question 21(1), reçue le 16 octobre 2019 par l'OSSNR.
[44] Courriel du CST à un chercheur de l'OSSNR, 23 septembre 2019.

renseignements sensibles. Dans l'affirmative, l'analyste évalue si la personne concernée a subi un grave préjudice. Cette méthode diffère de celle analysée plus tôt, puisque la PNE exige que l'utilisation faite des renseignements sensibles soit établie. De plus, le processus de la PNE ne présume pas de l'improbabilité d'une atteinte grave.

69. Si le CST utilise un de ces processus pour déterminer si un incident porte une atteinte importante à la vie privée, il est difficile de savoir lequel. La seule documentation et la seule évaluation que l'OSSNR a pu trouver se résumaient à une colonne du DIVP dans laquelle on indiquait par oui ou par non si l'incident portait une atteinte importante à la vie privée. L'OSSNR n'a trouvé aucune analyse qui porte sur le caractère sensible des renseignements ou qui vérifie l'existence d'un préjudice important à l'égard de la personne concernée. De même, l'OSSNR n'a relevé aucun document ni aucune preuve voulant que les analystes ont évalué l'existence de demandes d'intervention pour les incidents en question. incidents liés à la vie privée inscrits dans le DIVP[45], il aurait été utile de vérifier si une demande d'intervention avait été traitée, afin de voir s'il y avait atteinte importante à la vie privée.

70. L'OSSNR estime que l'évaluation du dommage ou du préjudice grave ne devrait pas se fonder sur le traitement d'une demande d'intervention. Les demandes d'intervention exigent des renseignements de SIGINT, et les incidents non assortis de produit de SIGINT – comme les incidents relevant du mandat de cyberdéfense – échappent donc à une telle analyse. Les incidents non associés à des produits de SIGINT peuvent renfermer des renseignements personnels susceptibles de causer un dommage ou préjudice grave à la personne concernée. Faute de se pencher sur l'utilisation de tous les renseignements personnels sensibles à l'extérieur des voies de SIGINT, le CST ne peut évaluer avec exactitude la présence d'un préjudice grave. Pour établir avec précision s'il y a atteinte importante à la vie privée, l'analyse du dommage ou préjudice grave subi par la personne ne devrait pas reposer uniquement sur les demandes d'intervention.

71. **Constatation n° 5 : L'évaluation du CST ne suffit pas à déterminer si un incident porte une atteinte importante à la vie privée.**

Recommandation n° 4 : Le CST devrait normaliser la politique d'évaluation qui permet d'établir si un incident lié à la vie privée porte une atteinte importante à la vie privée. De plus, une fois les renseignements personnels sensibles analysés, le CST devrait élaborer des méthodes d'analyse afin de déterminer s'il y a eu dommage ou préjudice grave, sans s'appuyer uniquement sur le traitement d'une demande d'intervention.

comme méthode d'atténuation

72. Conformément à l'EPM
comme mesure d'atténuation ou une personne se trouvant au Canada, est défini à l'alinéa 33.4.1(d) de l'EPM :

[45] Incidents :

> [Trad.] est autorisé lorsque la correction, l'annulation ou la re-publication d'un rapport risque d'attirer une attention indésirable sur le Canadien ou la personne se trouvant au Canada qui est nommée par inadvertance. Les approbations éliminent le besoin de corriger, d'annuler ou de réutiliser des rapports dans lesquels un Canadien ou une personne se trouvant au Canada est nommée par inadvertance… ne s'applique pas aux rapports subséquents. Aucun rapport subséquent non supprimé.

73. Si un Canadien ou une personne se trouvant au Canada est nommée par inadvertance dans un rapport de SIGINT, le CST parle d'un « incident de divulgation de nom ». L'ancienne *Loi sur la défense nationale* et l'actuelle *Loi sur le Centre de la sécurité des télécommunications* autorisent dans certaines circonstances la divulgation du nom d'un Canadien ou d'une personne se trouvant au Canada[46], mais l'incident de divulgation de nom ne correspond pas à ces circonstances particulières. Le CST n'a pas été en mesure de préciser le fondement juridique ou l'autorité, autre que sa politique interne, ayant justifié l'utilisation comme technique d'atténuation des incidents liés à la vie privée[47].

74. Au cours de la période de référence, et comme mesure d'atténuation incidents inscrits dans le DIA, le CST a autorisé à nommer un Canadien dans [48].

75. La pratique du CST qui consiste à a été mise au point pour gérer les cas de divulgation par inadvertance et sans autorisation des noms de Canadiens ou de personnes se trouvant au Canada dans . Le CST considère le processus de comme une mesure d'atténuation puisque, à son avis, attirerait une attention indésirable sur la personne nommée. Bien que valable, cette considération stratégique ne suffit pas à autoriser la divulgation du nom d'un Canadien ou d'une personne se trouvant au Canada dans un rapport de SIGINT. La politique interne sur précise que n'autorise pas la divulgation d'autres noms. L'approbation sert plutôt uniquement à qui renfermait les noms divulgués par inadvertance.

76. Puisque certains incidents impliquent la divulgation par inadvertance du nom d'un Canadien, l'OSSNR s'inquiète du fait que ce processus ne semble pas satisfaire aux critères énoncés dans l'autorisation du ministre, qui exigent que des mesures satisfaisantes protègent les renseignements personnels des Canadiens, de sorte que les communications privées ne soient utilisées ou conservées que si elles sont essentielles aux affaires internationales, à la défense ou à la sécurité[49]. La pratique ne semble pas inclure une quelconque évaluation du caractère essentiel des renseignements conservés ou divulgués aux fins des affaires internationales, de la défense ou de la sécurité. La divulgation du nom d'un Canadien ou d'une personne se trouvant au Canada dans un rapport de SIGINT risque de contrevenir à l'article 8 de la *Charte.* La pratique ne semble pas établir si, malgré les renseignements

---

[46] Les renseignements concernant des Canadiens ou des personnes se trouvant au Canada ne peuvent être inclus dans des rapports de SIGINT que s'ils correspondent à la définition que fait la LDS du renseignement étranger; s'ils sont essentiels à la protection des vies ou à la sécurité des particuliers de toute nationalité; s'ils portent sur une activité criminelle grave qui menace la sécurité du Canada. Le CST est aussi autorisé à divulguer de l'IIC s'il en vient à la conclusion que cette divulgation est nécessaire aux affaires internationales, à la défense, à la sécurité ou à la cybersécurité, et si le récipiendaire a les autorisations nécessaires et des motifs opérationnels valables. (Article 44 de la *Loi sur le CST*)

[47] Réponse du CST à la DDR-6, question 4(b), reçue le 28 octobre 2019 par l'OSSNR.

[48] Incidents

[49] Même si les organismes qui composent le Groupe des cinq respectent les lois et les politiques de leurs homologues, ils ne sont tenus de mener leurs activités en conformité avec les MA du CST.

que le gouvernement possède déjà, la personne conserve un droit « résiduel » à la vie privée à l'égard de ces renseignements et de leur traitement par le gouvernement[50].

77. En outre, l'OSSNR constate qu'il est trompeur de qualifier le processus de mesure d'atténuation, puisque le processus ne corrige pas le problème engendré par la divulgation par inadvertance. Aucun fondement probatoire n'étaye la conclusion voulant que attirerait une attention indésirable sur la personne et lui serait plus dommageable que Canadien ou personne se trouvant au Canada . Il n'est pas non plus évident de savoir pourquoi les rapports attireraient une attention indésirable sur le nom divulgué par inadvertance, mais non la réduction du nombre de rapports.

78. L'OSSNR conclut par ailleurs à l'absence de lien convaincant entre la quantité de rapports dans lesquels une personne est nommée par inadvertance et la justification de la personne. Il est difficile de concilier l'idée qu'une personne nommée dans verrait son nom tous les rapports (ou annulation des rapports en entier), mais le nom d'une personne pourrait être conservé dans un rapport accessible.

79. **Constatation nº 6 : n'est pas une méthode appropriée pour atténuer l'effet et le risque d'atteinte à la vie privée que présente la divulgation d'un nom par inadvertance.**

Recommandation nº 5 : Le CST devrait abolir la pratique consistant à S'il continue d'utiliser comme mesure d'atténuation, le CST devrait obtenir un avis juridique sur la légalité de la pratique.

VI CONCLUSION

80. L'examen du DIVP est le tout premier examen du CST réalisé par l'OSSNR depuis l'entrée en vigueur de la *Loi sur l'OSSNR*, en 2019. Puisque de nombreuses difficultés ont limité la portée de l'examen de l'Office, ceux qu'elle réalisera à l'avenir étudieront la façon dont le CST traite les atteintes à la vie privée et les mesures stratégiques qu'elle prend pour en réduire la fréquence.

81. Dans l'ensemble, l'OSSNR félicite le CST d'avoir signalé et atténué rapidement les atteintes à la vie privée. Cependant, le CST devrait prendre d'autres mesures pour veiller à ce que les effets des incidents sur la vie privée soient minutieusement examinés, atténués et documentés. L'OSSNR presse le CST d'abolir la pratique consistant à , surtout qu'elle risque de contrevenir à l'article 8 de la *Charte.*

82. Tablant sur le présent examen, l'OSSNR sera heureuse de travailler avec le CST afin d'approfondir sa connaissance et sa compréhension de la mission et des difficultés du CST. Sur une note importante, l'OSSNR compte coordonner ses activités avec celles du commissaire à la protection de la vie privée, dans le but d'établir le processus de signalement

[50] Dans l'arrêt *R c. Wakeling,* par exemple, la Cour suprême du Canada a conclu qu'une attente résiduelle, mais moindre, en matière de vie privée subsiste à l'égard des renseignements obtenus par écoute électronique après leur collecte licite. *Wakeling c. États-Unis d'Amérique,* 2014 CSC 72.

des futurs incidents liés à la vie privée au CST, y compris les incidents qui portent une atteinte importante à la vie privée.

ANNEXE A : Objectifs

Le présent examen avait pour objectifs l'évaluation de ce qui suit :

- politiques et procédures au moyen desquelles le CST détermine si un incident porte une atteinte importante à la vie privée[51];
- méthode qui permet au CST de déterminer et de classer par catégorie les incidents liés à la vie privée et les erreurs de procédure[52];
- portée selon laquelle les politiques et procédures du CST atténuent les effets des incidents liés à vie privée et des erreurs de procédure.

L'examen du DIVP permet aussi à l'OSSNR de dégager les tendances ou les lacunes systémiques qui pourraient justifier des mesures correctives, une modification des procédures ou politiques du CST ou un examen approfondi d'un incident ou d'une activité en particulier. Cet examen a été réalisé au cours des trois premiers mois de l'existence de l'OSSNR. Des problèmes technologiques, dont des obstacles à la consultation des documents, et la période de temps limitée allouée à l'évaluation ont réduit la portée de l'examen. Par conséquent, il n'a pas été possible de faire une analyse en vue de cerner les tendances et les lacunes systémiques. Ce sera toutefois une des priorités des prochains examens de l'OSSNR.

[51] Les *Lignes directrices sur les atteintes à la vie privée* du Secrétariat du Conseil du Trésor qualifient l'atteinte d'importante si elle porte sur des renseignements personnels sensibles et s'il est raisonnable de craindre qu'une personne ou un grand nombre de personnes subissent un dommage ou un préjudice grave.
[52] Effectué par le Bureau du commissaire du Centre de la sécurité des télécommunications, l'examen précédent du DIVP (2017-2018) encourageait le CST à normaliser ses méthodes de saisie des entrées dans le DIVP, le DIA et le DEPM.

ANNEXE B : Portée et méthode

Le présent examen porte sur un échantillon d'incidents signalés dans le DIVP, le DIA et le DEPM entre le 1er juillet 2018 et le 31 juillet 2019. Les chercheurs de l'OSSNR ont sollicité des renseignements supplémentaires au sujet de 72 des 123 incidents signalés dans le DIVP pendant la période de référence. Que ce soit en format papier ou électronique, ils ont étudié des dossiers, fichiers, pièces de correspondance et autres documents, tels que des politiques, procédures et avis juridiques utiles à pour l'échantillon.

Même si l'examen annuel du DIVP a toujours couvert une période de 12 mois, le présent examen s'étale sur 13 mois, afin de tenir compte de l'entrée en vigueur de la *Loi sur le CST*, le 1er août 2019. Il importe de signaler que, pour cette période, nous avons retenu la date d'inscription des incidents dans le DIVP, et non la date à laquelle les incidents sont survenus.

Les chercheurs de l'OSSNR ont fait parvenir huit demandes de renseignements au CST entre le 7 août et le 16 octobre 2019. L'OSSNR a reçu des réponses entre le 23 août et le 31 octobre 2019. Le CST a préparé cinq comptes rendus et séances d'information à l'intention de l'OSSNR. Les dates et les sujets sont précisés à l'Annexe D. En outre, les chercheurs de l'OSSNR ont officieusement rencontré leurs homologues du CST, afin de discuter de l'évolution de l'examen et de préciser des demandes de renseignements et de documents.

Les chercheurs ont aussi examiné les politiques, procédures et pratiques du CST relatives au signalement des incidents liés à la vie privée et des erreurs de procédure, ainsi qu'aux mesures correctives correspondantes. Ils ont par ailleurs effectué une vérification indépendante des mesures d'atténuation du CST en comparant les renseignements obtenus [53] et [54]. Compte tenu des répercussions opérationnelles et des contraintes de temps, l'OSSNR a choisi au hasard 10 incidents à des fins de vérification dans le système de ciblage du CST[55].

[53] est un dépôt de rapports sur des RENSEIGNEMENTS SPÉCIAUX (RS) et de certains produits de cybersécurité du CST qui peuvent être communiqués

[54] la base de données SIGINT du CST sur le ciblage et la gestion des sélecteurs.

[55] Courriel envoyé par le CST au chercheur de l'OSSNR, et reçu le 21 octobre 2019.

ANNEXE C : Types d'incident et méthodes d'atténuation

Les incidents liés à la vie privée peuvent être classés par type d'incidents, soit :

- Les **incidents de ciblage** se produisent lorsque le CST ou un organisme secondaire cible sans le savoir un Canadien ou une personne se trouvant au Canada. L'incident en serait un de ciblage ou de divulgation de nom si les renseignements découlant de ce ciblage étaient inscrits dans un rapport révélant le nom d'un Canadien ou d'une personne se trouvant au Canada. Pour les incidents de ciblage, l'analyste doit immédiatement dé-cibler les sélecteurs associés à la personne et protéger cette dernière dans . Un produit de SIGINT qui se fonde sur des données de consultation doit être annulé.
- Les **incidents de divulgation de nom** concernent les cas où le CST divulgue sans le savoir le nom d'un Canadien ou d'une personne se trouvant au Canada, ou l'un ou l'autre des sélecteurs y étant associés, dans un produit de SIGINT; la personne concernée n'est toutefois pas ciblée directement. Le produit de SIGINT doit être annulé ou corrigé comme il se doit.
- Les **incidents de recherche** consistent à associer, dans certaines bases de données, des sélecteurs d'interrogation à un Canadien ou à une personne se trouvant au Canada, à l'insu de cette personne. Les mesures d'atténuation visent à éliminer les résultats ou les historiques de recherche, et à protéger les sélecteurs dans [56].
- Pour les **incidents de divulgation,** le CST divulgue par inadvertance des renseignements qui identifient un Canadien en empruntant les mauvaises voies ou en s'adressant aux mauvais destinataires. Parmi les mesures d'atténuation, notons le caviardage approprié de tous les documents.
- Les **incidents de collecte** concernent les erreurs techniques associées aux méthodes de collecte qui permettent la saisie accidentelle de données concernant des Canadiens ou des personnes se trouvant au Canada. Dans pareils cas, la cause de la collecte par inadvertance doit être établie et corrigée comme il se doit.
- Les **incidents de manipulation et de conservation des données** consistent en des problèmes techniques qui relèvent du mandat de la cyberdéfense et par lesquels des données sont accidentellement rendues accessibles dans des documents non classifiés ou accidentellement conservés pendant une période plus longue que celle autorisée. Les mesures d'atténuation diffèrent pour chacun de ces incidents, mais se traduisent généralement par la suppression des données.

[56] Sachez que, dans certains cas, les sélecteurs doivent être ajoutés à
puis protégés, car ils n'ont pas été ciblés avant l'incident.

ANNEXE D : Réunions et séances d'information

- 19 août 2019 : Séance d'information sur le Dossier relatif aux incidents liés à la vie privée
- 9 octobre 2019 : Réunion avec un analyste de politiques
- 16 octobre 2019 : Réunion avec un superviseur et un analyste, Conformité, Sécurité et Gestion du risque
- 23 octobre 2019 : Réunion avec le gestionnaire de l'équipe responsable de la protection de la vie privée et des divulgations
- 23 octobre : Démonstration

ANNEXE E : Constatations et recommandations

Constatation nº 1 : Lorsqu'une politique impose des mesures de conformité à des incidents liés à la vie privée, le CST utilise ces mesures de façon opportune et conforme à la politique.

Constatation nº 2 : Malgré son approche à niveaux multiples qui renforce les mesures de protection de la vie privée, le CST ne se sert pas du DIVP, ni d'aucun autre recueil similaire d'incidents liés à la vie privée, pour éviter de répéter des incidents systémiques ou pour relever les lacunes des politiques ou pratiques actuelles susceptibles de réduire la fréquence des incidents liés à la vie privée.

Recommandation nº 1 : Le CST devrait examiner tous les incidents liés à la vie privée, dans l'optique de cerner les tendances systémiques ou les lacunes des politiques ou pratiques actuelles.

Constatation nº 3 : L'approche irrégulière qu'emprunte le CST pour évaluer et consigner les incidents liés à la vie privée ne permet pas l'atteinte des objectifs de transparence et de reddition de compte de l'autosignalement de ces incidents.

Recommandation nº 2 : devrait émuler la méthode de signalement des incidents liés à la vie privée de , de sorte que chaque incident comportant un intérêt en matière de protection de la vie privée au Canada fasse l'objet d'un examen.

Constatation nº 4 : Les mesures d'atténuation que le CST applique à certains incidents liés à la vie privée après leur découverte se limitent à la suppression de renseignements touchant la protection de la vie privée, sans que soit vérifiée l'utilisation ou l'extraction des renseignements avant leur suppression.

Recommandation nº 3 : Le CST devrait toujours examiner l'utilisation qui pourrait avoir été faite des renseignements comportant un intérêt dans l'optique de la protection de la vie privée au Canada, afin de déterminer si les circonstances d'une atteinte particulière à la vie privée justifient d'autres mesures d'atténuation.

Constatation nº 5 : L'évaluation du CST ne suffit pas à déterminer si un incident porte une atteinte importante à la vie privée.

Recommandation nº 4 : Le CST devrait normaliser la politique d'évaluation qui permet d'établir si un incident lié à la vie privée porte une atteinte importante à la vie privée. De plus, une fois les renseignements personnels sensibles analysés, le CST devrait élaborer des méthodes d'analyse afin de déterminer s'il y a eu dommage ou préjudice grave, sans s'appuyer uniquement sur le traitement d'une demande d'intervention.

Constatation nº 6 : n'est pas une méthode appropriée pour atténuer l'effet et le risque d'atteinte à la vie privée que présente la divulgation d'un nom par inadvertance.

Recommandation nº 5 : Le CST devrait abolir la pratique consistant à S'il continue d'utiliser comme mesure d'atténuation, le CST devrait obtenir un avis juridique sur la légalité de la pratique.

ANNEXE F : Dossier relatif aux incidents liés à la vie privée du CST