Cour fédérale Federal Court

~~**TRÈS SECRET**~~

Date : 20190201

Dossier : CSIS-28-18

Citation : 2019 CF 141

Ottawa (Ontario), le 1er février 2019

EN PRÉSENCE de l'honorable juge Fothergill

DANS L'AFFAIRE d'une demande de mandats présentée par [redacted] en vertu des articles 12 et 21 de la *Loi sur le Service canadien du renseignement de sécurité*, L.R.C. (1985), chapitre C-23

ET DANS L'AFFAIRE VISANT le terrorisme islamiste – [redacted]

MOTIFS DE L'ORDONNANCE

I. Aperçu

[1] Le 16 octobre 2018, j'ai décerné une série de mandats en vertu des articles 12 et 21 de la *Loi sur le Service canadien du renseignement de sécurité*, L.R.C. (1985), ch. C-23 [*Loi sur le SCRS*] dans le cadre d'une enquête menée par le Service canadien du renseignement de sécurité [SCRS ou Service] sur le terrorisme islamiste et une personne connue. Deux de ces mandats autorisent le directeur du SCRS et tout employé agissant sous son autorité à installer

tout « objet » dans un ordinateur ou un appareil de communication portable, à l'entretenir, à l'enlever [redacted], en vue d'intercepter des communications et d'obtenir des informations. Il s'agit de la technique qui, généralement parlant, consiste à installer un « implant » dans un appareil.

[2] En pratique, un implant destiné à la collecte permet au Service d'obtenir, en secret, une copie de ce que la cible [redacted] sur un ordinateur ou un appareil de communication portable [appareil] ou par l'entremise de celui-ci. Le Service a aussi recours à des implants pour fouiller des appareils à distance et obtenir des informations, notamment des images, des documents, des courriels, [redacted] Il s'agit d'une collecte qui s'effectue en continu, à l'insu de l'utilisateur.

[3] L'avocat représentant la procureure générale du Canada a reconnu que les mandats demandés prévoient des pouvoirs nouveaux qui pourraient soulever des questions relatives aux droits garantis par la *Charte canadienne des droits et libertés* [Charte][1] et au droit au respect de la vie privée des personnes que l'exercice de ces pouvoirs pourrait toucher. La Cour a entendu les observations orales de l'avocat de la procureure générale, de l'employé du SCRS qui a présenté la demande de mandats et de deux déposants.

[4] La Cour a aussi nommé un *amicus curiae* possédant l'habilitation de sécurité nécessaire. Celui-ci a eu accès aux documents utiles et a eu la possibilité de contre-interroger les déposants et de présenter des observations orales et écrites. La Cour a demandé à l'*amicus curiae* de lui

[1] Partie I de la *Loi constitutionnelle de 1982*, annexe B de la *Loi de 1982 sur le Canada*, 1982, ch. 11 (R.-U.)

faire part de son opinion réfléchie et professionnelle quant aux questions de nature juridique, entre autres, que soulevait la demande. L'*amicus curiae* n'était pas tenu d'adopter une position antagoniste s'il n'estimait pas que c'était nécessaire ou justifié.

[5] Après avoir entendu les déposants et pris connaissance des documents présentés ainsi que des observations de l'avocat de la procureure générale et de l'*amicus curiae*, j'ai conclu que la demande satisfaisait aux exigences prévues aux alinéas 21(2)a) et b) de la *Loi sur le SCRS* et que les mandats pouvaient être décernés sous réserve de modifications mineures. Voici les motifs de cette décision.

II. Nouveaux pouvoirs demandés

[6] Avant de procéder à l'installation d'un implant, le SCRS cherche à repérer l'appareil utilisé par la cible de l'enquête. Pour ce faire, il utilise habituellement les méthodes suivantes : recours à des sources humaines, filature, entrevues, utilisation d'émulateurs de station de base ou demande d'assistance à des services d'application de la loi ou de renseignement canadiens ou étrangers. Cette démarche peut aussi être facilitée par l'interception de communications et l'obtention d'informations auprès de fournisseurs de services de communication. Si la cible [redacted] le SCRS peut demander au Centre de la sécurité des télécommunications de lui prêter assistance dans les activités d'enquête menées en vertu des mandats.

[7] Lorsqu'il installe un implant à distance, le Service recueille au préalable des informations lui permettant de confirmer que l'implant sera bien installé dans un appareil dont la cible est propriétaire ou qu'elle utilise. Les nouveaux pouvoirs demandés dans les mandats sont censés prévoir qu'en pratique, le Service peut ne pas être en mesure de déterminer, avant l'installation, que l'appareil appartient à la cible ou est utilisé par elle.

[8] Les mandats autorisent les employés du SCRS à installer à distance un implant dans tout appareil [redacted] de la cible [redacted] de la cible [redacted]

[9] Tout dépendant du type d'implant, le SCRS peut devoir obtenir un mandat sur Internet. Ce mandat l'autorise à intercepter les communications qui parviennent à un compte auprès d'un fournisseur de services Internet [redacted] de la cible [redacted] ou qui en proviennent.

[10] Avant que commence l'interception des communications et l'obtention des informations mentionnées dans les mandats dans un appareil où un implant a été installé à distance [redacted] une analyse (*survey*) de l'appareil est effectuée, laquelle permet d'obtenir, en tout ou en partie, les informations suivantes : [redacted]

[redacted] informations sur le système d'exploitation, marque et modèle de l'appareil, adresses réseau, [redacted]

[11] D'autres informations peuvent être obtenues à cette étape afin d'assurer la sécurité de l'implant : [redacted]

[12] Selon que s'applique le mandat sur les appareils portables ou le mandat sur les interceptions générales et les fouilles, un employé du Service désigné détermine, au moyen des informations issues de l'analyse, si l'appareil est a) un appareil portable dont la cible est propriétaire ou qu'elle loue ou utilise ou b) un ordinateur qui contient des informations pouvant être obtenues en vertu du mandat sur les interceptions générales et les fouilles. Si l'appareil entre dans l'une ou l'autre de ces catégories, les informations issues de l'analyse sont conservées, et l'interception et la collecte commencent. Si ce n'est pas le cas, les informations en question sont détruites dès qu'il est matériellement possible de le faire, dans les six mois suivant l'obtention.

[13] Le directeur général régional peut autoriser l'interception des communications effectuées au moyen d'un appareil dont la cible de l'enquête n'est pas propriétaire et qu'elle n'a pas loué, si l'employé du Service désigné a des motifs raisonnables de croire que celle-ci l'utilise. Il est possible de conserver les informations obtenues lors de l'analyse qui peuvent aider le directeur

général régional à s'acquitter de cette responsabilité, à cette fin. En général, les circonstances de l'enquête l'amènent à prendre la décision rapidement.

[14] Les mandats autorisent aussi [redacted] servant de [redacted] ne requiert pas d'analyse, car il a déjà été déterminé que l'implant a été installé dans un appareil dont la cible de l'enquête est propriétaire ou qu'elle utilise.

[15] En outre, les mandats autorisent [redacted] d'un appareil appartenant à un tiers, c'est-à-dire l'installation d'un implant dans un appareil qui, à l'issue de l'étape de l'analyse, s'avère ne pas avoir de lien avec la cible. Les mandats permettent au Service [redacted] dans l'appareil du tiers, [redacted] qui lui permettra de distinguer cet appareil de l'appareil dont la cible est propriétaire ou qu'elle utilise. [redacted] Le SCRS détruit cette information, qui n'est pas liée à une cible d'enquête, dès qu'il lui est matériellement possible de le faire, dans les six mois suivant l'obtention.

[16] La plupart des informations obtenues à l'étape de l'analyse ne révéleront que peu d'informations biographiques de base sur la personne qui est propriétaire de l'appareil ou qui l'utilise, voire aucune; cependant, ce pourrait être le cas de certaines d'entre elles. Tout dépendant [redacted] peuvent révéler des

renseignements personnels sensibles. [redacted]

[redacted]

III. Question

[17] La demande de mandats en l'espèce soulève le point de droit suivant : les mesures proposées par le Service à l'étape de l'analyse suffisent-elles à protéger les droits garantis par la Charte et le droit au respect de la vie privée des tiers innocents dont il pourrait recueillir les renseignements personnels dans le cadre de l'installation à distance d'un implant dans un appareil?

IV. Analyse

[18] Selon les dispositions habituelles des mandats autorisant l'interception de communications, l'acquisition d'informations et d'images ainsi que le repérage ou la géolocalisation d'une cible, le Service peut installer un implant dans un appareil. Le SCRS a déjà cherché à intercepter des communications ou à obtenir des informations provenant d'un appareil en y installant un implant à distance. Le 15 décembre 2017, une formation collégiale des juges de la Cour a reçu des explications relatives à cette technique et à l'étape de l'analyse consistant à repérer le bon appareil.

[19] Au cours de cet exposé, le juge en chef Paul Crampton s'est dit d'avis que l'étape de l'analyse devrait être obligatoire avant que la collecte de données au moyen d'un implant puisse

commencer. La Cour se penchait alors pour la première fois sur le libellé de la nouvelle condition figurant dans les mandats.

A. *Principes généraux*

[20] La Cour ne peut décerner un mandat permettant au Service de recueillir des informations et des renseignements en vertu de l'article 12 de la *Loi sur le SCRS* que si les exigences prévues au paragraphe 21(2) de cette même loi sont respectées. Notamment, la Cour doit être convaincue que le mandat est nécessaire pour permettre au Service de faire enquête sur des menaces envers la sécurité du Canada et que d'autres méthodes d'enquête ont été essayées en vain ou semblent avoir peu de chances de succès. Dans *Atwal c. Canada*, [1988] 1 CF 107, au paragraphe 37, la Cour d'appel fédérale a souligné que « les autorisations d'interception de communications privées fondées sur la [*Loi sur le SCRS*] seront, en pratique, plus difficilement précises à l'avance que les autorisations prévues au *Code* criminel ».

[21] Si elle n'est pas menée de manière raisonnable, une fouille effectuée en vertu d'un mandat décerné au SCRS peut être abusive, donc contraire à l'article 8 de la Charte. Il se peut que le juge qui a décerné le mandat ait omis de limiter la portée de l'autorisation ou que les personnes qui ont effectué la fouille n'aient pas souscrit aux principes de réduction au minimum des répercussions lorsqu'elles ont exécuté les mandats (*Canada (Procureure générale) c. Huang*, 2018 CAF 109, au paragraphe 28).

[22] S’agissant d’un ordinateur ou d’un téléphone, l’attente en matière de vie privée est élevée. Comme l’a soutenu la Cour suprême du Canada dans l’arrêt *R. c. Vu,* 2013 CSC 60 [*Vu*], aux paragraphes 40 à 44, il est difficile d’imaginer une atteinte plus grave à la vie privée que la fouille d’un de ces appareils. En effet, un ordinateur personnel contient d’immenses quantités d’informations, dont certaines touchent à l’« ensemble de renseignements biographiques d’ordre personnel ». En outre, les ordinateurs renferment des informations générées automatiquement, souvent à l’insu de l’utilisateur, et peuvent conserver des fichiers et des données longtemps après que l’utilisateur croit les avoir détruits. L’ordinateur connecté à Internet sert de portail à une quantité presque infinie de données qui sont partagées entre différents utilisateurs et stockées presque n’importe où dans le monde. De même, depuis un ordinateur connecté à un réseau, les services de police et de renseignement peuvent avoir accès à des informations qui se trouvent dans d’autres appareils.

[23] Dans l’arrêt *R. c. Marakah*, 2017 CSC 59, au paragraphe 37, la Cour suprême du Canada a souligné que les conversations électroniques sont susceptibles de révéler une somme considérable de renseignements personnels. Le maintien d’un « espace privé » protégeant les renseignements personnels contre les intrusions de l’État est la raison d’être de l’article 8 de la Charte. Cet espace privé s’étend bien au-delà de l’appareil mobile d’une personne. En effet, il peut englober les conversations électroniques par lesquelles elle communique des renseignements personnels. Il est raisonnable de s’attendre à ce que les interactions privées, et non seulement le contenu d’un téléphone cellulaire à un moment précis, demeurent privées.

B. *Fouilles à distance*

[24] Grâce à un implant installé à distance, le Service peut intercepter [redacted] il est tout à fait possible qu'un implant soit installé sur un appareil dont un tiers innocent est propriétaire ou qu'il utilise. Cette possibilité devient très forte lorsque [redacted] est associée à un endroit public comme un café Internet.

[25] L'*amicus curiae* a avisé la Cour qu'au Canada, les précédents ayant trait aux conséquences juridiques de l'installation d'implants à distance sont peu nombreux, se référant à un passage de l'ouvrage de Gerald Chan et de Susan Magotiaux, *Digital Evidence: A Practitioner's Handbook* (Emond Professional, Toronto, 2018, p. 47).

> [TRADUCTION]
>
> Qu'arrive-t-il si l'État veut accéder à des données stockées sur un ordinateur sans pénétrer dans le lieu où il se trouve? Les tribunaux canadiens n'ont pas encore étudié de façon exhaustive certaines méthodes créatives permettant l'accès aux données à distance. Cependant, aux États-Unis, des intervenants étatiques ont cherché à obtenir des tribunaux l'autorisation d'obtenir un tel accès au moyen de logiciels installés secrètement dans un appareil visé.

[26] Dans son article « Modern Technology and Privacy Rights: Leading Canadian and U.S. Case Law » (Ontario Bar Association, 2013, p. 8), le procureur adjoint de la Couronne Brock Jones fait allusion à une affaire où les autorités chargées des libérations conditionnelles

n’ont pas pu obtenir un mandat de perquisition en vue de constater des violations d’une ordonnance de surveillance de longue durée.

> [TRADUCTION]
>
> En se fiant à une adresse IP liée aux courriels envoyés de l’« ordinateur cible » présumé ou qui lui sont parvenus, le gouvernement s’expose à tomber dans un piège. Quiconque envoie les courriels en question peut avoir utilisé un logiciel d’usurpation pour masquer sa véritable adresse IP. Par conséquent, l’installation du cheval de Troie peut se faire aux dépens d’utilisateurs innocents et de leurs appareils. L’ordinateur en question peut aussi se trouver dans un lieu public comme un café ou une bibliothèque. Ainsi, les activités anodines de nombreuses personnes innocentes pourraient être captées par le logiciel espion. L’application gouvernementale permettrait d’exercer une surveillance par l’entremise de la webcaméra de l’ordinateur, et ce, en temps réel. Par conséquent, le gouvernement doit demander une autorisation d’écoute électronique plutôt qu’un mandat. Les demandes futures doivent répondre aux préoccupations de la Cour, avant qu’un mandat puisse être décerné. [Non souligné dans l’original.]

[27] Dans *In re Warrant to Search a Target Computer at Premises,* 2013 WL 1729765, aux pages 3 et 4, le juge Stephen W.M. Smith de la Cour du district Sud du Texas, division de Houston, a refusé une demande de mandat visant un ordinateur à distance. Si la décision doit être interprétée dans le contexte propre à cette juridiction, il n’en reste pas moins que le juge Smith a posé des questions qui peuvent être pertinentes en l’espèce.

> [TRADUCTION]
>
> Cette « méthode » d’installation de logiciel n’est expliquée nulle part. En outre, le gouvernement n’explique pas comment il s’assurera que seules les personnes « qui mènent l’activité illégale […] seront visées par la technologie ». Que se passera-t-il si l’ordinateur visé se trouve dans une bibliothèque publique, dans un café Internet ou dans un lieu de travail accessible à d’autres

> personnes, ou s'il est utilisé par des membres de la famille ou des amis qui n'ont rien à voir avec l'activité illégale? Qu'arrivera-t-il si la fausse adresse de courriel est utilisée à des fins légitimes par des personnes qui n'ont pas partie liée au complot criminel? Et si l'adresse de courriel est consultée depuis plus d'un ordinateur ou au moyen d'un téléphone cellulaire et d'autres appareils numériques? S'il existe des réponses satisfaisantes à ces questions, le gouvernement ne les donne pas dans sa demande. [Non souligné dans l'original.]

[28] Dans l'article « Beware of Government Agents Bearing Trojan Horses » (*Akron Law Review*, vol. 48, n^{o} 2, article 4, p. 345 à 347), Brian Owsley, professeur adjoint à l'école de droit de l'Université Texas Tech, laisse entendre que les préoccupations de cette nature pourraient être atténuées grâce à un processus d'autorisation préalable et à la mise en place de protocoles. En particulier, a) il faut interdire aux enquêteurs de conserver des informations de tiers non liées à l'enquête; b) les enquêteurs doivent, dans les informations stockées sur l'ordinateur visé, établir une distinction entre les informations qui concernent leur cible et les documents non pertinents, par exemple des photos personnelles et des données financières sans lien avec des activités criminelles; c) il est impératif de détruire les copies papier des documents non pertinents et de supprimer tout fichier électronique.

C. *Protocoles de réduction au minimum des répercussions*

[29] La destruction des données obtenues de tiers innocent dans le cadre d'une fouille n'est qu'une des manières de limiter le caractère intrusif de la fouille. Le mandat lui-même peut minimiser l'empiètement sur les droits garantis par la Charte et sur le droit des tiers au respect de leur vie privée.

[30] Dans *R. c. Thompson*, [1990] 2 CSC 1111 [*Thompson*], aux paragraphes 113 et 114, la Cour suprême du Canada a étudié, dans une autorisation d'intercepter les communications privées, une disposition sur les « endroits fréquentés » qui autoriserait la police à surveiller les communications effectuées à un endroit que la cible est susceptible de fréquenter, dans ce cas un téléphone public. Selon le juge John Sopkina :

> Dans toute autorisation, il peut y avoir atteinte à la vie privée de tiers innocents. Par exemple, le dispositif d'écoute installé sur le téléphone de la résidence d'une cible enregistrera les communications des autres occupants de la maison. C'est l'un des inconvénients malheureux de la surveillance électronique. Mais il s'agit d'un inconvénient que le Parlement a évidemment estimé justifié dans des circonstances appropriées au cours d'une enquête portant sur un crime grave.
>
> À mon avis, la possibilité d'atteinte à la vie privée de personnes innocentes peut prendre des proportions tellement importantes dans certains cas qu'elle doit être reconnue expressément au même titre que les intérêts qu'il y a à enquêter sur un crime. Une clause des « endroits fréquentés » est justement à l'origine de cette possibilité si parmi les lieux fréquentés on retrouve des téléphones publics utilisés par le grand public ou d'autres lieux semblables. Je ne dis pas qu'il devrait y avoir une interdiction constitutionnelle d'intercepter les communications dans les lieux fréquentés par le public; dans ce cas, les auteurs de complots en vue d'importer des stupéfiants pourraient pratiquement se soustraire à ce qui est peut-être le seul moyen d'enquête efficace contre eux simplement en utilisant des lieux publics pour faire leurs affaires.

[31] La Cour suprême a conclu que la disposition sur les « endroits fréquentés » ne contrevenait pas aux dispositions applicables du *Code criminel* et que, partant, les autorisations étaient valides. Toutefois, compte tenu de l'ampleur de l'atteinte autorisée à la vie privée, l'absence totale de toute mesure de protection du public entraînait la possibilité que soient

effectuées des fouilles, des perquisitions ou des saisies abusives. Selon le juge Sopinka (au paragraphe 119) :

> À mon avis, les interceptions effectuées conformément à ces autorisations, qui étaient simplement des recherches à l'aveuglette non fondées sur des motifs raisonnables et probables de croire que la cible utiliserait alors les téléphones publics, étaient abusives. Dans la plupart des cas, il serait préférable qu'il y ait une véritable surveillance physique du téléphone public pour s'assurer qu'il est utilisé par la cible. On dit qu'il s'agit de la pratique policière normale. Je partage cependant l'opinion du juge Martin et du professeur Stanley A. Cohen que d'en faire une exigence absolue imposerait un fardeau trop lourd aux responsables de l'application de la loi canadienne.

[32] Ce principe demeure valable et s'applique en l'espèce, même si l'arrêt *Thompson* a été rendu il y a presque trente ans, lorsque l'internet n'en était qu'à ses balbutiements. Il se peut que des conditions prévoyant la réduction au minimum des répercussions ne soient pas nécessaires dans tous les cas; cela dépend de l'ampleur de l'atteinte possible à la vie privée de tiers innocent.

[33] Récemment, dans l'arrêt *Vu*, la Cour suprême du Canada a statué que la fouille d'un ordinateur doit être autorisée explicitement par un mandat. Partant, la police ne pourrait pas s'appuyer sur un mandat l'autorisant à perquisitionner le domicile où elle a saisi l'ordinateur.

[34] Dans *Vu*, la Cour suprême propose en effet de traiter un ordinateur comme un lieu distinct dont la fouille requiert en soi une autorisation préalable. Toutefois, le juge Thomas Cromwell n'était pas persuadé que l'article 8 de la Charte requiert que la manière de fouiller un ordinateur soit toujours précisée à l'avance. Il a appuyé sa conclusion sur deux motifs. Premièrement, la manière dont une fouille a été effectuée dans le cadre d'une enquête criminelle

fait généralement l'objet d'un contrôle a posteriori, démarche plus propice à l'élaboration de nouvelles règles sur la façon d'effectuer des fouilles que ne l'est la procédure *ex parte* de délivrance des mandats. Deuxièmement, le fait d'exiger que soient imposés des protocoles de perquisition avant l'exécution de la fouille rendrait vraisemblablement l'étape de l'autorisation beaucoup plus complexe, en plus de créer des difficultés d'ordre pratique. Toute tentative d'imposer des protocoles de perquisition à l'étape de l'autorisation risque de créer des angles morts dans une enquête et de contrecarrer les objectifs légitimes de l'application de la loi dont tient compte le processus d'autorisation préalable. Ces problèmes sont amplifiés par l'évolution rapide et constante de la technologie.

[35] S'il est possible que des protocoles de fouille ne soient pas constitutionnellement requis en toutes circonstances, le juge saisi de la demande d'autorisation doit tout de même s'assurer que les mandats qu'il décerne répondent aux objectifs de la procédure d'autorisation préalable. Il possède en outre le pouvoir discrétionnaire d'imposer des conditions à cette fin. Le juge Cromwell a souligné que l'autorisation peut comporter des directives sur la manière de procéder à la fouille et il n'a pas écarté la possibilité que l'amélioration des connaissances en matière de fouilles d'ordinateurs ainsi que l'évolution des technologies puissent finir par justifier l'imposition de protocoles de perquisition dans un éventail de situations élargi (*Vu*, au paragraphe 62).

[36] L'*amicus curiae* souligne qu'il existe des différences importantes entre les pouvoirs prévus par les mandats qu'exécute la police et ceux qu'exécute le SCRS. Dans *Vu*, le juge Cromwell soutient qu'il n'y a pas lieu que tous les mandats comportent un protocole de fouille

parce que, notamment, il est préférable d'examiner le caractère raisonnable de la fouille a posteriori. Toutefois, très peu de mandats décernés au directeur du SCRS font l'objet d'un tel examen, en grande mesure parce qu'il y a peu de chances qu'ils donnent lieu à des accusations criminelles. La préoccupation du juge Cromwell au sujet de la complexité de l'enquête et de la possibilité d'en miner l'efficacité par inadvertance est infondée en l'espèce. Les déposants ont proposé un protocole viable, actuellement utilisé à titre informel.

[37] Compte tenu de l'ampleur de l'atteinte éventuelle à la vie privée de tiers innocents, la procureure générale du Canada et l'*amicus curiae* conviennent que les mandats qui autorisent l'installation à distance d'implants dans des appareils doivent comporter des mesures de réduction au minimum des répercussions. L'*amicus curiae* a proposé que l'étape de l'analyse soit rendue obligatoire avant que la collecte de données puisse commencer, comme l'a recommandé le juge en chef lors de l'exposé entendu en formation plénière le 15 décembre 2017. L'*amicus curiae* a aussi recommandé que les données obtenues à l'étape de l'analyse se limitent strictement aux catégories énumérées aux paragraphes 10 et 11 des présents motifs.

[38] Moyennant l'apport des modifications susmentionnées, je suis convaincu du caractère raisonnable des fouilles qui seront effectuées en vertu des mandats demandés par le directeur du SCRS. Les protocoles de fouille sont suffisamment rigoureux pour protéger les droits garantis par la Charte et le droit des tiers innocents à la protection de leur vie privée. Partant, il y a lieu de décerner les mandats.

V. Conclusion

[39] Tout mandat autorisant l'installation à distance d'un implant sur tout appareil, y compris un appareil dont un tiers innocent est propriétaire ou qu'il utilise doit, pour être décerné, comporter les protocoles de fouille suivants.

1. Tout appareil dans lequel un implant a été installé à distance [redacted] fait l'objet d'une analyse avant que commencent l'interception des communications et l'obtention des informations mentionnées dans les mandats.

2. Les données obtenues à l'étape de l'analyse se limitent aux catégories énumérées aux paragraphes 10 et 11 des présents motifs.

3. Après examen des informations obtenues à l'étape de l'analyse, un employé du Service désigné détermine s'il existe des motifs raisonnables de croire que l'appareil est a) un appareil portable dont la cible est propriétaire ou qu'elle utilise ou b) un ordinateur qui contient des informations pouvant être obtenues en vertu du mandat sur les interceptions générales et les fouilles.

4. Si l'appareil respecte l'une ou l'autre des conditions 3a) et b), les informations issues de l'analyse peuvent être conservées, et l'interception et la collecte visant l'appareil peuvent commencer.

5. Si ce n’est pas le cas, les informations issues de l’analyse sont détruites dès qu’il est matériellement possible de le faire et, au plus tard dans les six mois suivant l’obtention, sans être autrement utilisées.

«Simon Fothergill»
Juge

Cour fédérale Federal Court

COUR FÉDÉRALE

AVOCATS INSCRITS AU DOSSIER

DOSSIER:	CSIS 28-18
INTITULÉ:	DANS L'AFFAIRE D'UNE DEMANDE DE MANDATS PRÉSENTÉE PAR [redacted] EN VERTU DES ARTICLES 12 ET 21 DE LA LOI SUR LE SERVICE CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ, L.R.C. (1985), chapitre C-23 **ET DANS L'AFFAIRE VISANT LE TERRORISTE ISLAMISTE –** [redacted]
LIEU DE L'AUDIENCE:	OTTAWA, ONTARIO
DATE DE L'AUDIENCE:	SEPTEMBER 25, 2018
MOTIFS DE L'ORDONNANCE:	LE JUGE FOTHERGILL
DATE DES MOTIFS:	1 FÉVRIER 2019

COMPARUTIONS:

Stéphanie Dion Andrew Cameron	POUR LE DEMANDEUR
Ian Carter	*AMICUS CURIAE*

AVOCATS INSCRITS AU DOSSIER:

Procureur général du Canada Ottawa (Ontario)	POUR LE DEMANDEUR
Bayne Sellar Ertel Carter Ottawa (Ontario)	*AMICUS CURIAE*