Cour fédérale | Federal Court

~~**TRÈS SECRET**~~

Date : 20210903

Dossiers : CSIS 17-19
CSIS 18-19
CSIS 19-19

Référence : 2021 CF 919

[TRADUCTION FRANÇAISE, NON RÉVISÉE]

Ottawa (Ontario), le 3 septembre 2023

En présence de l'honorable monsieur le juge Gleeson

ENTRE :

DANS L'AFFAIRE D'UNE DEMANDE DE MANDAT PRÉSENTÉE PAR [redacted] EN VERTU DES ARTICLES 12 ET 21 DE LA *LOI SUR LE SERVICE CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ*, LRC 1985, c C-23

ET DANS L'AFFAIRE VISANT LE TERRORISME ISLAMISTE [redacted]

ENTRE :

DANS L'AFFAIRE D'UNE DEMANDE DE MANDAT PRÉSENTÉE PAR [redacted] EN VERTU DES ARTICLES 12 ET 21 DE LA *LOI SUR LE SERVICE CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ*, LRC 1985, c C-23

ET DANS L'AFFAIRE VISANT LE TERRORISME ISLAMISTE [redacted]

ENTRE :

DANS L'AFFAIRE D'UNE DEMANDE DE MANDAT PRÉSENTÉE PAR [redacted] EN VERTU DES ARTICLES 12 ET 21 DE LA *LOI SUR LE SERVICE CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ*, LRC 1985, c C-23

ET DANS L'AFFAIRE VISANT LE TERRORISME ISLAMISTE [redacted]

ORDONNANCE ET MOTIFS

[Le 29 septembre 2022, le procureur général du Canada a présenté une requête en vertu des articles 3, 55, 397 et 399 des *Règles des Cours fédérales*, DORS 98/106, pour demander la modification de l'ordonnance rendue le 3 septembre 2021 afin de préciser les circonstances dans lesquelles s'applique la mise en garde prévue au paragraphe 43. Cette requête visait à modifier le libellé de la mise en garde elle-même, à préciser les systèmes de technologie de l'information pour lesquels la mise en garde doit s'appliquer et à indiquer que la mise en garde ne s'applique pas lorsqu'il s'agit de personnes que le Service connaît déjà. La Cour a accueilli cette requête par ordonnance confidentielle, le 1er décembre 2022. Le paragraphe 43 de l'ordonnance publique est le reflet de la modification du libellé de la mise en garde.]

I. Aperçu

[1] Pour le Service canadien du renseignement de sécurité [SCRS ou Service], l'une des premières étapes d'une enquête sur les menaces pour la sécurité du Canada consiste à établir l'identité des personnes susceptibles d'être impliquées dans des activités liées à la menace, par exemple grâce à l'obtention des données d'identification de l'abonné à un compte de communication (un numéro de téléphone ou un identificateur électronique, [le ou les identificateurs électroniques] découvert au cours de l'enquête.

[2] Le Service a demandé et obtenu des autorisations judiciaires préalables pour recueillir des « données d'identification de base » [DIB] auprès de fournisseurs de services de communication [FSC] pour faciliter l'identification de l'abonné à un compte de communication qui, selon ce qu'a pu démontrer le Service, est lié à l'enquête en cours (*X (Re)*, 2017 CF 1048, aux paragraphes 3, 6 et 62 à 69 [*Décision de 2017*]; *X (Re)*, 2018 CF 874, au paragraphe 95

[*Décision de 2018*]; considérées ensemble, il s'agit des *Décisions sur les DIB*). Comprendre le lien entre l'enquête et le compte permet à la Cour d'évaluer si le droit à la protection contre les perquisitions, les fouilles et les saisies abusives garanti à l'abonné par l'article 8 de la *Charte canadienne des droits et libertés,* partie I de la *Loi constitutionnelle de 1982,* annexe B de la *Loi de 1982 sur le Canada* (R-U), 1982, c 11 [*Charte*] doit céder le pas aux intérêts de l'État quant à l'obtention des DIB (*Décision de 2017,* aux paragraphes 3, 6, 60 et 61).

[3] Les DIB sont un sous-ensemble des informations sur l'abonné. Aux termes des mandats dont il a été question dans les *Décisions sur les DIB*, il s'agit des éléments suivants (*Décision de 2017,* aux paragraphes 2 et 32) :

A. le nom de l'abonné à un compte;

B. l'adresse de l'abonné;

[et certaines autres informations liées au compte];

[4] Le Service a constaté que, dans nombre de cas, les DIB ne suffisent pas à lui permettre d'établir l'identité des utilisateurs ou des titulaires d'un compte de communication donné. Pour régler ce problème, il a présenté trois demandes de mandat distinctes en vertu des articles 12 et 21 de la *Loi sur le service canadien du renseignement de sécurité,* LRC 1985, c C-23 [*Loi sur le SCRS*]. Il cherchait ainsi à obtenir le pouvoir d'élargir la gamme de renseignements personnels pouvant être recueillis auprès des FSC. Dans les trois mandats demandés, il nomme cette gamme élargie « données d'identification » [DI]. La définition en est donnée au paragraphe 12.

[5] Les trois demandes étaient axées sur des volets distincts de l'enquête du Service sur la menace que fait peser le terrorisme islamiste. Il demandait l'autorisation d'obtenir des DI relatives à […] comptes de communication donnés afin de pouvoir établir l'identité de leurs abonnés, ayant épuisé les techniques ne nécessitant pas de mandat.

[6] Les demandes ont été acceptées partiellement : les parties ont adopté une approche en deux étapes quant aux mandats sur les DI afin que le Service ne puisse obtenir que les informations dont il pouvait établir la nécessité pour la progression des enquêtes en cours, dans le souci de réduire au minimum le caractère intrusif des fouilles autorisées.

[7] Au cours de la première étape, le Service a été autorisé à recueillir un sous-ensemble des DI qu'il souhaitait obtenir. Ces « DI de la 1re étape », qui constituaient un ensemble plus étendu que les DIB, excluaient toutefois des informations sur l'abonné dont la collecte pourrait être plus intrusive, ainsi que les DI d'autres personnes susceptibles d'être liées au compte de communication donné. Advenant que les DI de la 1re étape ne lui permettent pas d'établir l'identité d'un abonné, la seconde étape donnerait au Service la possibilité de présenter une autre demande visant cette fois la collecte des DI exclues de l'autorisation accordée à la première étape.

[8] Les présents motifs portent sur le traitement des demandes et sur la raison d'être de l'approche en deux étapes quant au pouvoir de recueillir des DI. Y est aussi abordée la nécessité d'ajouter des conditions aux mandats en ce qui a trait à la conservation et à l'utilisation des DI par le Service.

II. Contexte

A. *Pourquoi trois demandes?*

[9] Les demandes en cause s'inscrivent dans la démarche effectuée par le Service pour améliorer son processus de demandes de mandats sur les DIB ou, en l'espèce, de mandats sur les DI. Plutôt que de présenter une demande appuyée par un affidavit général traitant de la menace dans son ensemble, c'est-à-dire le terrorisme islamiste, le Service en a présenté trois, distinctes et axées sur des manifestations particulières de cette menace [CSIS 17-19, CSIS 18-19 et CSIS 19-19, chacun lié à un aspect différent de l'enquête du Service sur le menace terroriste islamiste].

[10] Par cette approche améliorée, le Service a cherché à faciliter la présentation de la preuve à l'appui et à mieux faire état du lien nécessaire qu'il aurait établi entre les comptes de communication d'intérêt et son enquête en cours.

[11] Dans le dossier n^{o} CSIS 19-19, [...].

B. *Définition de « données d'identification »*

[12] Aux termes des trois demandes de mandat en l'espèce, les DI sont :

[TRADUCTION]

[_Les DIB ainsi que certaines autres informations relatives au compte pour aider l'identification de l'utilisateur ou du propriétaire du compte_]

[13] Telles que définies ci-haut, les DI concernent indubitablement davantage de renseignements personnels que les DIB (se reporter au paragraphe 4); il s'agit d'informations plus détaillées dont la collecte est susceptible d'être plus intrusive que ce qui a été envisagé dans les *Décisions sur les DIB*. Les DI comprennent aussi des informations liées à […] par exemple [et certaines autres informations liées au compte].

C. *L'instance*

[14] La Cour a entendu le témoignage de la déposante principale des trois demandes, […] lors d'une audience *ex parte* à huis clos. […] a exposé de quelle manière chacune des catégories de DI visées par les demandes serait utile au Service dans son enquête, en particulier pour faciliter l'identification des abonnés aux comptes de communication donnés.

[15] Les mandats sur les DI dont j'ai été saisi ne comprenaient pas la disposition qui constituait la condition 1 dans les mandats sur les DIB présentés auparavant. Selon cette condition, s'agissant [de certaines autres informations liées au compte] le Service devait [prendre certaines mesures. Cette exigence] figure maintenant dans la définition des DI (se reporter au point « K » du paragraphe 12). J'ai convenu avec le procureur général du Canada [procureur général] que cela rendait superflue la condition 1 des mandats sur les DIB.

[16] À l'issue de l'audience, j'ai pris ma décision en délibéré quant aux trois demandes et j'ai nommé un *amicus curiæ* [*amicus*] pour aider à évaluer si la définition élargie des DI soulevait d'autres questions que celles qu'avait abordées le juge en chef Paul Crampton dans les *Décisions sur les DIB.*

[17] Lors de la présentation des demandes, le procureur général a soulevé deux questions.

A. Les demandes de mandats respectent-elles les exigences de la *Loi sur le SCRS*?

B. Les informations demandées se limitent-elles à ce qui est nécessaire pour établir l'identité sans autre empiètement sur la vie privée?

[18] La seconde question a mis en cause des considérations qui ont mené à la nomination de l'*amicus,* M. Cameron. J'ai alors reformulé la seconde question ainsi :

> La définition élargie des DI soulève-t-elle d'autres questions ou met-elle en cause d'autres considérations que celles qui ont été abordées dans les *Décisions sur les DIB*?

[19] À l'issue de son examen documentaire, M. Cameron a soulevé des questions relatives, d'une part, à la collecte des DI et, d'autre part, à leur conservation et à leur utilisation.

[20] S'agissant de la conservation et de l'utilisation, l'*amicus* était d'avis que la Cour, si elle autorisait la collecte des DI, devrait aussi envisager l'ajout de conditions aux mandats. Pour sa part, le procureur général estimait que de nouvelles conditions n'étaient pas nécessaires et que, de toute façon, les types de conditions suggérés constituaient des entraves opérationnelles et

techniques pour le Service. Après avoir présenté d'autres affidavits, leurs déposants, […] et […] ont été interrogés.

[21] J'aborderai tour à tour et dans cet ordre les questions relatives à la collecte et à la conservation soulevées par l'*amicus*.

III. Autorisation de la collecte des DI

[22] Le procureur général a soutenu que la définition élargie des DI, telle qu'établie dans les trois demandes, n'empêchait pas la Cour de mettre en balance les intérêts concurrents dont font état les *Décisions sur les DIB*, à savoir, d'une part la nécessité pour l'État d'obtenir ces informations et, d'autre part, les droits en matière de vie privée des personnes. La preuve a permis d'établir le lien nécessaire, c'est-à-dire l'exigence constitutionnelle pour autoriser l'activité intrusive, ainsi que le besoin du Service quant à la collecte plus intrusive des DI.

[23] Selon l'*amicus*, l'article 21 de la *Loi sur le SCRS* établit comme principe général que le fardeau du procureur général quant à la justification d'une fouille s'alourdit proportionnellement au caractère intrusif de celle-ci. Appliquant ce principe aux trois demandes de mandats sur les DI, l'*amicus* a soutenu que la Cour devait aborder et adopter avec circonspection le critère du lien tel qu'établi pour les DIB, car il avait été déterminé que celles-ci étaient des informations dont la collecte était minimalement intrusive.

[24] Pour faire valoir cette opinion, M. Cameron a souligné que la définition élargie des DI entraînerait une collecte plus intrusive de renseignements personnels que ce dont il avait été

question dans les *Décisions sur les DIB*. En effet, les DI englobent des informations plus détaillées sur l'abonné (p. ex. […] ainsi que […]).

[25] De l'avis de M. Cameron, le simple fait d'établir un lien entre l'enquête et le compte de communication pourrait ne pas suffire à autoriser la collecte, plus intrusive, des DI. Il a souligné, à titre d'exemple, qu'un tribunal pourrait ne pas être convaincu que la preuve établit l'existence de motifs raisonnables de croire que toutes les catégories de DI sont nécessaires d'entrée de jeu pour permettre au Service d'enquêter sur la menace ni que toutes ces catégories sont importantes relativement à la menace (alinéas 21(2)a) et b) de la *Loi sur le SCRS*). Partant, il a avancé que le bien-fondé d'une autorisation de recueillir des DI de toutes les catégories sera une question souvent soulevée, particulièrement lorsque le Service, dans la demande de mandat, sera uniquement en mesure d'établir qu'une collecte moins intrusive pourrait ne pas lui suffire pour établir l'identité d'un abonné.

[26] Par suite de ces observations, le procureur général et l'*amicus* ont fait une proposition commune, à laquelle j'ai souscrit : le traitement en deux étapes des demandes de mandats sur les DI. À la première étape, j'ai examiné les demandes en fonction d'une définition restreinte des DI excluant les renseignements personnels [d'un certain type] ou ceux dont la collecte était manifestement plus intrusive que ce qui avait été envisagé dans les *Décisions sur les DIB*.

[27] Voici la définition des DI de la 1re étape.

[TRADUCTION]

Pour un compte :

[_Les DIB plus un sous-ensemble de DI qui se limite aux informations de l'abonné du compte et est moins intrusif que l'ensemble des DI_]

[28] L'*amicus* a reconnu la portée restreinte des DI de la 1re étape, mais a souligné que, néanmoins, leur collecte pourrait être plus intrusive que celle des informations abordées dans les *Décisions sur les DIB*. Il a avancé que, partant, la Cour devrait être consciente qu'un simple lien entre l'enquête et un compte de communication pourrait ne pas constituer un motif suffisant pour décerner un mandat sur des DI de la 1re étape.

[29] Bien que je ne sois pas en désaccord avec l'*amicus* lorsqu'il avance que le fardeau du procureur général quant à la justification d'une fouille s'alourdit proportionnellement au caractère intrusif de celle-ci, je tiens à apporter deux précisions. En premier lieu, bien que les DI de la 1re étape, telles que définies ci-dessus, touchent davantage de catégories d'informations que les DIB, elles n'en diffèrent pas par nature. Partant, je considère que leur collecte n'est pas nécessairement plus intrusive que celle des DIB.

[30] En second lieu, je ne crois pas que la *Décision de 2017* permette d'affirmer qu'un simple lien entre une enquête du Service et un compte de communication justifiera toujours la délivrance d'un mandat sur les DIB. En fait, respecter l'exigence relative au lien permet à la Cour de tenir compte en bonne et due forme des intérêts des personnes ou des catégories de personne dont le droit au respect de la vie privée est en cause, c'est-à-dire évaluer l'attente subjective de la personne en matière de vie privée, assujettir à des contrôles sévères les pouvoirs dont jouit le Service pour enquêter sur des menaces pour la sécurité du Canada ainsi que prendre

en considération l'ensemble des circonstances (*Décision de 2017*, au paragraphe 63). Cela s'applique également aux demandes d'autorisation de recueillir des DI.

[31] Conscient de ces facteurs, et après les avoir pris en considération, j'étais convaincu qu'il existait des motifs raisonnables de croire qu'une menace pesait sur la sécurité du Canada et qu'un lien avait été établi entre l'enquête du Service et chacun des comptes de communication donnés pour lesquels il avait demandé l'autorisation de recueillir des DI. En outre, j'étais convaincu qu'il existait des motifs raisonnables de croire que la preuve établissait que le Service avait besoin des DI de la 1re étape, telles que définies au paragraphe 27 et relativement aux comptes de communication donnés, pour faire progresser son enquête. Les mandats sur les DI de la 1re étape […] dans le dossier no CSIS 19-19 ont été décernés au Service.

[32] Le procureur général n'a pas présenté de demande supplémentaire visant la collecte des DI de la 2e étape.

[33] Comme il a été souligné plus haut, l'*amicus* a aussi soulevé des préoccupations relatives à la conservation et à la consultation, par le Service, des DI recueillies légalement. Je suis demeuré saisi des demandes en vue de déterminer si, compte tenu des questions soulevées par l'*amicus* et dans l'intérêt public, il y aurait lieu d'ajouter des conditions relatives à la conservation et à l'utilisation des DI. Je passe maintenant à cette question.

IV. Conditions relatives à la conservation et à l'utilisation de données d'identification

[34] S’agissant des DI telles que définies dans les trois demandes (se reporter au paragraphe 12), l’*amicus* estimait que, même s’il était démontré que la collecte des DI était nécessaire à la progression d’une enquête du Service, un examen pourrait révéler qu’une partie des DI recueillies légalement ne sont pas nécessaires – ou pertinentes – pour l’enquête. Partant, une autorisation de collecte ne devrait pas nécessairement justifier la conservation pour une durée indéfinie d’informations jugées non nécessaires ou non pertinentes pour une enquête, particulièrement si elles ont trait […] pas plus que la consultation de celles-ci sans restrictions ni mises en garde.

[35] L’*amicus* soutient que, pour autoriser la collecte élargie des DI, la Cour devrait être convaincue que le Service a réglé les questions de conservation et de consultation quant aux informations qui, après examen, sont jugées non nécessaires ou non pertinentes. Si elle n’est pas convaincue du caractère adéquat des pratiques de gestion de l’information du Service à cet égard, la Cour pourrait ajouter des conditions au mandat (alinéa 21(4)f) de la *Loi sur le SCRS*). Il pourrait s’agir, à titre d’exemple, d’exiger la destruction des informations non nécessaires ou non pertinentes ou, lorsqu’il est nécessaire de les conserver pour de quelconques motifs établis, d’en exiger le marquage ou la mise sous séquestre à des fins de gestion de la conservation et de la consultation. Selon l’*amicus,* une autorisation de collecte qui a une portée large et qui n’impose pas de limites à la conservation ni à la consultation ouvre la porte à une conservation abusive des données.

[36] L’*amicus* ajoute que, même si la collecte des DI de la 1re étape se limite à des informations sur l’abonné au compte, il n’est pas exclu que l’abonné en question n’ait virtuellement aucun lien avec l’enquête sur la menace. À titre d’exemple, l’abonné pourrait avoir

[…]. L'*amicus* avance qu'en l'absence d'implication dans des activités liées à la menace, il est possible de présumer que les DI ne sont ni nécessaires ni pertinentes pour l'enquête du Service. Bien que la collecte des informations en cause ait été autorisée et que, partant, le critère de conservation (la stricte nécessité) prévue à l'article 12 de la *Loi sur le SCRS* soit respecté conformément à l'interprétation et à l'application de cette disposition dans *X (Re)*, 2016 CF 1105, l'*amicus* soutient que la Cour pourrait tout de même imposer des conditions d'utilisation et de conservation parce que les informations auront été obtenues en vertu d'une autorisation qu'elle a accordée.

[37] Le procureur général reconnaît que le juge qui donne l'autorisation peut imposer, dans un mandat, les conditions qu'il estime indiquées dans l'intérêt public. Il souligne cependant qu'en la matière, il devrait exercer son pouvoir discrétionnaire en fonction des articles 12 et 21 de la *Loi sur le SCRS* et des limites imposées par l'article 8 de la *Charte* tel qu'interprété par les tribunaux. Le procureur général avance qu'il n'est pas obligatoire de réduire au minimum la nature intrusive des activités lorsque la collecte est autorisée par un mandat, mais il reconnaît que des conditions sont souvent imposées à cette fin dans ce contexte, particulièrement lorsque des tiers pourraient être touchés dans l'exercice des pouvoirs prévus par les mandats.

[38] Le procureur général soutient que la collecte des DI de la 1re étape porte uniquement sur les abonnés aux comptes et est étroitement circonscrite. Le Service a besoin de ces informations pour établir l'identité de ces utilisateurs et évaluer la nature de leurs liens avec la menace visée par l'enquête, et la restriction relative à la conservation prévue à l'article 12 de la *Loi sur le SCRS* – le critère de la stricte nécessité – permet, en soi, de conserver les informations : il n'est pas nécessaire d'ajouter des conditions (*X (Re)*, 2016 CF 1105).

[39] Selon le procureur général, même si un examen révèle que l'abonné à un compte qui a trait à des activités liées à la menace n'y est finalement pas impliqué, ses DI constituent néanmoins des informations pertinentes et nécessaires pour l'enquête du Service. Le procureur général appuie sa position sur la preuve de nature opérationnelle présentée par […].

[40] Dans son affidavit opérationnel, […] traite de l'importance de la conservation des DI et de la possibilité de les consulter, même lorsqu'un examen des DI et que d'autres démarches d'enquête portent à croire que la personne ne mène pas d'activités liées à la menace. Ces informations, affirme-t-elle, permettent au Service de boucler l'enquête; leur conservation évite que des rapports opérationnels incomplets ou fragmentaires nuisent aux enquêtes ou laissent des lacunes dans les renseignements. Selon les éléments de preuve présentés par […] le Service conserve aussi les informations pour les raisons suivantes :

[TRADUCTION]

[utilisation future dans le cadre de la même enquête ou d'autres enquêtes; et]

v. en disposer pour des fins de responsabilisation, d'assujettissement à des mesures de contrôles et pour d'autres considérations administratives.

[41] Les éléments de preuve présentés par […] traitent des défis techniques et des limites avec lesquels le Service doit composer pour respecter les conditions sur la conservation et l'utilisation des DI.

[42] Ayant soigneusement examiné la preuve, particulièrement le contenu de l'affidavit opérationnel de […] je suis d'avis que les DI de la 1re étape, telles que définies au

paragraphe 27, constituent des informations pertinentes et nécessaires pour l'enquête du Service sur le terrorisme islamiste, même lorsque le Service n'a pas de motifs raisonnables de croire que la personne menait ou mène des activités liées à la menace. Je souligne également que la condition 1 des mandats prévoit la destruction de toute information recueillie qui ne fait pas partie des DI dont la collecte a été autorisée en vertu du mandat. Partant, je ne suis pas convaincu qu'il est nécessaire ou indiqué d'ajouter des conditions relatives à la conservation et à l'utilisation des DI de la 1re étape recueillies légalement. Avec cette conclusion, j'exprime cependant deux réserves.

[43] En premier lieu, le procureur général et l'*amicus* ont convenu d'une mise en garde pouvant être jointe aux DI au moment de la collecte et les accompagner tant que le Service n'a pas de motifs raisonnables de croire que la personne menait ou mène des activités liées à la menace. En voici le libellé.

> [TRADUCTION]
>
> Les informations contenues dans présent rapport ont été recueillies à titre préliminaire pour les fins de l'enquête, car il existait des motifs raisonnables de soupçonner ~~que la~~ qu'une coordonnée liée à [*indiquer les données d'identification dans le présent rapport ou le nom de la personne*] avait servi ou servait à mener des activités liées à la menace. En date du ~~présent rapport~~ [*insérer la date de l'évaluation*], le Service n'a pas de motifs raisonnables de soupçonner que la personne dont traite le présent rapport a mené ou mène des activités liées à la menace. Jusqu'à ce que le Service ait de tels motifs, la présente mise en garde doit accompagner tout rapport reprenant les données d'identification qui figurent dans le présent document ainsi que dans toute renseignement divulgué à des partenaires étrangers ou nationaux ~~divulgation des données d'identification à l'extérieur du Service.~~

[44] La mise en garde met adéquatement en contexte les DI de personnes dont l'implication possible dans des activités liées à la menace n'a pas été constatée. En outre, elle s'adresse à quiconque consulte les DI et accompagne tout rapport qui les reprend. Selon les éléments de preuve techniques présentés par […] la mise en garde peut être jointe aux informations qui viennent d'être recueillies ou aux rapports existants.

[45] Je suis convaincu que la mise en garde proposée est adéquate en l'espèce. Elle sera jointe, lorsque c'est possible, aux DI de la 1re étape que le Service est autorisé à recueillir en vertu des mandats décernés, ainsi qu'à tout rapport reprenant les DI en question. Je reconnais que, dans le cadre de demandes futures, les circonstances de la collecte des DI de la 1re étape pourraient être différentes et rendre inutile la mise en garde susmentionnée.

[46] En second lieu, il n'y a pas lieu de considérer que s'appliquera à une demande visant la collecte des DI de la 2e étape – dont la définition est élargie – ma conclusion selon laquelle, d'une part, les DI de la 1re étape, telles que définies dans les demandes en l'espèce, constituent des informations pertinentes et nécessaires pour l'enquête du Service et, d'autre part, il n'y a pas lieu d'ajouter de conditions relatives à l'utilisation et à la conservation. Lorsqu'il se présentera de nouveau devant la Cour pour demander l'autorisation de recueillir des DI de la 2e étape, le Service devrait être prêt à répondre aux questions abordées dans les présents motifs, notamment la possibilité que les informations visées par une demande de collecte des DI de la 2e étape doivent être assujetties, en tout ou en partie, à des conditions sur la conservation et l'utilisation.

ORDONNANCE

LA COUR ORDONNE ci qui suit :

1. La mise en garde figurant au paragraphe 43 des présents motifs sera jointe aux données d'identification de la première étape recueillies en vertu des mandats décernés […] dans les dossiers n^{os} CSIS 17-19, CSIS 18-19 et CSIS 19-19 ainsi qu'à tout rapport reprenant ces données, lorsque le Service n'a pas de motifs raisonnables de soupçonner que la personne en cause menait ou mène des activités liées à la menace.

2. Dans les 30 jours suivant la date de la présente ordonnance et les motifs qui l'accompagnent, l'*amicus curiæ* et l'avocat du procureur général les passeront en revue pour formuler conjointement des recommandations à la Cour quant aux parties qui peuvent être rendues publiques et à l'échéancier connexe.

« Patrick Gleeson »
Juge

COUR FÉDÉRALE

AVOCATS INSCRITS AU DOSSIER

DOSSIERS :	CSIS 17-19 / CSIS 18-19 / CSIS 19-19
INTITULÉ :	DANS L'AFFAIRE D'UNE DEMANDE DE MANDAT PRÉSENTÉE PAR [redacted] EN VERTU DES ARTICLES 12 ET 21 DE LA *LOI SUR LE SERVICE CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ*, LRC 1985, c C-23 ET DANS L'AFFAIRE VISANT LE TERRORISME ISLAMISTE [redacted] DANS L'AFFAIRE D'UNE DEMANDE DE MANDAT PRÉSENTÉE PAR [redacted] EN VERTU DES ARTICLES 12 ET 21 DE LA *LOI SUR LE SERVICE CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ*, LRC 1985, c C-23 ET DANS L'AFFAIRE VISANT LE TERRORISME ISLAMISTE [redacted] DANS L'AFFAIRE D'UNE DEMANDE DE MANDAT PRÉSENTÉE PAR [redacted] EN VERTU DES ARTICLES 12 ET 21 DE LA *LOI SUR LE SERVICE CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ*, LRC 1985, c C-23 ET DANS L'AFFAIRE VISANT LE TERRORISME ISLAMISTE [redacted]
LIEU DE L'AUDIENCE :	OTTAWA (ONTARIO)
DATE DE L'AUDIENCE :	LE 24 SEPTEMBRE 2019 LE 17 FÉVRIER 2020
ORDONNANCE ET MOTIFS :	LE JUGE GLEESON
DATE DES MOTIFS :	LE 3 SEPTEMBRE 2021

COMPARUTIONS :

Penny Brady Isabelle MacKay	POUR LE DEMANDEUR
Gordon Cameron	*AMICUS CURIAE*

AVOCATS INSCRITS AU DOSSIER :

Procureur général du Canada	POUR LE DEMANDEUR
Gordon Cameron	*AMICUS CURIAE*