Recueil des décisions des Cours fédérales

Federal Courts Reports

NOTE DE L'ARRÊTISTE : Ce document fera l'objet de retouches de forme avant la parution de sa version définitive dans le *Recueil des décisions des Cours fédérales*.

CSIS-1-21

2022 CF 1444

Dans l'affaire concernant une demande présentée par [...] en vue d'obtenir des 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

Et dans l'affaire concernant les activités de [...] liées à des menaces

RÉPERTORIÉ : LOI SUR LE SERVICE CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ (RE)

Cour fédérale, juge en chef Crampton—Ottawa, 25 janvier, 9 et 10 février, 23 mars et 21 octobre 2022.

Note de l'arrêtiste : Les sections caviardées par la Cour sont indiquées par [***].

Renseignement de sécurité — Il s'agissait d'une demande supplémentaire de mandat présentée en vertu des articles 12 et 21 de la Loi sur le Service canadien du renseignement de sécurité (la Loi sur le SCRS ou la Loi) pour faire autoriser l'usage par le Service canadien du renseignement de sécurité (le SCRS) d'un nouvel outil technologique à l'égard de personnes faisant l'objet d'une enquête — Le SCRS souhaitait adopter une nouvelle technologie particulière (la technologie) au Canada et l'utiliser à quatre fins précises sans mandat dans le cadre d'enquêtes menées conformément à l'article 12 de la Loi — Parmi les quatre usages proposés de la technologie, trois s'appliqueraient exclusivement au Canada, tandis qu'un quatrième s'appliquerait également à l'extérieur du Canada — Le procureur général du Canada (PGC) a admis que les quatre usages de la technologie proposés au Canada constitueraient des « fouilles » ou « perquisitions » au sens où il faut l'entendre pour l'application de l'article 8 de la Charte canadienne des droits et libertés — Toutefois, le PGC a affirmé que ces fins proposées ne seraient pas « abusives » pour l'application de l'article 8 — Il s'agit d'une technologie à fonctionnalités précises, qui peut être utilisée au Canada à quatre fins précises qui sont minimalement envahissantes — Ainsi, ces usages seraient autorisés par l'article 12 de la Loi sur le SCRS, sans qu'il soit nécessaire d'obtenir un mandat — Néanmoins, le SCRS a sollicité un mandat provisoire [***] à des fins précises impliquant des personnes faisant l'objet d'enquêtes au Canada, par excès de prudence, pour éviter d'enfreindre la Charte — Même si la technologie a d'abord été mise à l'essai dans le cadre d'un projet pilote, le SCRS a sursis à l'utilisation de la technologie le temps d'obtenir des précisions sur l'application de l'article 8 de la Charte à ses activités de collecte de renseignements sur des ressortissants étrangers dépourvus de lien avec le Canada — Il s'agissait de savoir si l'article 12 de la Loi sur le SCRS autorise le SCRS à utiliser la technologie au Canada aux quatre fins qu'il a précisées, et ce sans mandat; et si l'article 12 de la Loi sur le SCRS autorise le SCRS à utiliser la technologie à l'extérieur du Canada à l'égard de ressortissants étrangers dépourvus de lien avec le Canada de la manière plus envahissante qu'il a précisée, et ce sans mandat — Le PGC et l'amicus s'entendaient pour dire que les quatre usages de la technologie proposés par le SCRS au Canada constitueraient des fouilles ou perquisitions au sens où il faut l'entendre pour l'application de l'article 8 de la Charte — Le PGC

et l'amicus s'entendaient également pour dire que les quatre usages proposés de la technologie au Canada seraient autorisés par l'article 12 de la Loi sur le SCRS, dès lors que, de par leur nature, ils sont minimalement envahissants — De plus, le PGC et l'amicus s'entendaient pour dire que l'article 12 n'a rien d'abusif — Ainsi, la loi ayant autorisé les fouilles ou perquisitions proposées n'avait rien d'abusif — Les quatre usages proposés de la technologie au Canada étaient considérés comme minimalement envahissants en ce qui a trait aux intérêts en matière de vie privée des personnes dont les données sont recueillies; et ne nécessiteraient pas l'obtention d'un mandat — La plupart des conditions proposées par l'amicus pour l'usage de la technologie ont été acceptées, entre autres la nécessité de définir un délai de conservation par le SCRS des données recueillies de manière incidente — Dès lors que certains autres principes généraux sont suivis, la collecte incidente de données relatives à des tiers non liés à des menaces ne serait pas effectuée de manière abusive — En ce qui concerne l'évaluation des usages proposés de la technologie à l'extérieur du Canada, le SCRS a proposé de recourir à la technologie pour recueillir les données dans deux situations — Il serait satisfait au critère des motifs raisonnables de soupçonner que prévoit l'article 12 de la Loi sur le SCRS dans les deux situations — De plus, selon l'évaluation des usages proposés par le SCRS de la technologie à l'extérieur du Canada, l'article 12 autorise la portée envahissante de ces usages proposés de la technologie à l'extérieur du Canada sans mandat — En conclusion, les quatre usages proposés par le SCRS de la technologie au Canada ne nécessiteraient pas l'obtention d'un mandat, une conclusion qui tenait pour acquis que les principes opérationnels et les mesures seraient suivis par le SCRS — Également, les usages proposés par le SCRS de la technologie à l'extérieur du Canada à l'égard de ressortissants étrangers dépourvus de lien avec le Canada ne nécessiteraient pas non plus l'obtention d'un mandat — La technologie peut être utilisée au Canada, comme proposée, sans mandat; la technologie peut être utilisée à l'extérieur du Canada à l'égard de ressortissants étrangers dépourvus de lien avec le Canada, sans mandat, dans les deux situations décrites.

Droit constitutionnel — Charte des droits — Fouilles, perquisitions ou saisies abusives — Le Service canadien du renseignement de sécurité (SCRS) cherchait à faire autoriser l'usage d'un nouvel outil technologique à l'égard de personnes faisant l'objet d'une enquête — Le SCRS souhaitait adopter une nouvelle technologie particulière (la technologie) au Canada et l'utiliser à quatre fins précises sans mandat dans le cadre d'enquêtes menées conformément à l'article 12 de la Loi sur le Service canadien du renseignement de sécurité SCRS (la Loi sur le SCRS ou la Loi) — Parmi les quatre usages proposés de la technologie, trois s'appliqueraient exclusivement au Canada, tandis qu'un quatrième s'appliquerait également à l'extérieur du Canada — Par conséquent, il s'agissait de déterminer si l'article 12 de la Loi sur le SCRS autorise le SCRS à utiliser la technologie à l'extérieur du Canada à l'égard de ressortissants étrangers dépourvus de lien avec le Canada de la manière plus envahissante qu'il a précisée, et ce sans mandat — Le PGC et l'amicus s'entendaient pour dire que les quatre usages de la technologie proposés par le SCRS au Canada constitueraient des fouilles ou perquisitions au sens où il faut l'entendre pour l'application de l'article 8 de la Charte — Cependant, le PGC et l'amicus divergeaient d'opinion quant à savoir si le recours à la technologie à l'extérieur du Canada à l'égard d'étrangers dépourvus de tout lien avec le Canada constituerait également des fouilles ou perquisitions — Le PGC et l'amicus s'entendaient pour dire que les quatre usages proposés de la technologie au Canada seraient autorisés par l'article 12 de la Loi sur le SCRS, dès lors que, de par leur nature, ils sont minimalement envahissants — De plus, le PGC et l'amicus s'entendaient pour dire que l'article 12 n'a rien d'abusif — Ainsi, la loi ayant autorisé la fouille ou perquisition n'avait rien d'abusif — En ce qui concerne l'évaluation des usages proposés de la technologie à l'extérieur du Canada, le SCRS a proposé de recourir à la technologie pour recueillir les données dans deux situations — Il serait satisfait au critère des motifs raisonnables de soupçonner que prévoit l'article 12 de la Loi sur le SCRS dans les deux situations — En vertu de la Charte, le mot « chacun » doit être interprété invariablement de la même manière à l'article 8 qu'aux autres dispositions de la Charte — À la lumière de la jurisprudence analysée, les ressortissants étrangers qui n'ont pas l'un des trois liens reconnus avec le Canada ((i) citoyenneté canadienne, (ii) présence au Canada ou (iii) faire l'objet de poursuites pénales au Canada), ne sont pas visés par le mot « chacun » qui figure à l'article 8 de la Charte — Le paragraphe 12(2) habilite expressément le SCRS à exercer les fonctions que le paragraphe (1) lui confère même à l'extérieur du Canada — Comme le SCRS n'est pas contraint d'obtenir une autorisation judiciaire préalable, en application de la Charte ou d'une autre règle de droit, pour

utiliser la technologie aux fins envahissantes à l'extérieur du Canada qui étaient en cause dans la présente instance, de telles activités ne nécessiteraient pas l'obtention d'un mandat — Finalement, aucun argument n'a été présenté au soutien de la thèse selon laquelle les usages sans mandat de la technologie proposés par le SCRS seraient contraires au droit international ou à son esprit — Par conséquent, aucun principe de droit international en vigueur n'interdirait les usages plus que minimalement envahissants de la technologie proposés par le SCRS sans mandat à l'égard de ressortissants étrangers dépourvus de lien avec le Canada à l'extérieur du Canada.

Il s'agissait d'une demande supplémentaire de mandat présentée en vertu des articles 12 et 21 de la *Loi sur le Service canadien du renseignement de sécurité SCRS* (la Loi sur le SCRS ou la Loi) pour faire autoriser l'usage par le Service canadien du renseignement de sécurité (le SCRS) d'un nouvel outil technologique à l'égard de personnes faisant l'objet d'une enquête. Le SCRS souhaitait adopter une nouvelle technologie particulière (la technologie) au Canada et l'utiliser à quatre fins précises sans mandat dans le cadre d'enquêtes menées conformément à l'article 12 de la Loi. Parmi les quatre usages proposés de la technologie, trois s'appliqueraient exclusivement au Canada, tandis qu'un quatrième s'appliquerait également à l'extérieur du Canada. Le procureur général du Canada (PGC) a admis que les quatre usages de la technologie proposés au Canada constitueraient des « fouilles » ou « perquisitions » au sens où il faut l'entendre pour l'application de l'article 8 de la *Charte canadienne des droits et libertés*. Toutefois, il a affirmé que ces fins proposées ne seraient pas « abusives » pour l'application de l'article 8. En effet, (i) elles seraient minimalement envahissantes et seraient donc permises par l'article 12 de la Loi sur le SCRS; (ii) l'article 12 n'a rien d'abusif; (iii) les fouilles ou perquisitions ne seraient pas effectuées d'une manière abusive.

Le nouvel outil est une technologie à fonctionnalités précises. Le PGC a affirmé que la technologie peut être utilisée au Canada à quatre fins précises qui sont minimalement envahissantes. Ainsi, ces usages seraient autorisés par l'article 12 de la Loi sur le SCRS, sans qu'il soit nécessaire d'obtenir un mandat. Néanmoins, le SCRS a sollicité un mandat provisoire [***] (le mandat provisoire) à des fins précises impliquant des personnes faisant l'objet d'enquêtes au Canada. Initialement, le PGC a expliqué que les pouvoirs sollicités sont justifiés, car ils sont minimalement envahissants pour l'application de l'article 12 de la Loi sur le SCRS, et ne nécessitent pas de mandat. Il sollicitait néanmoins le mandat par excès de prudence, pour éviter d'enfreindre la Charte par inadvertance, pendant que (i) le SCRS se familiarise avec les données qui résulteront de l'utilisation de la [technologie], et (ii) pendant que la Cour considère si cet usage particulier des données peut être autorisée en vertu de l'article 12 de la Loi sur le SCRS. Le jour même où le mandat provisoire a été décerné, un second mandat a été décerné, autorisant le PGC à utiliser la technologie à des fins reconnues par le SCRS et qui ne sont pas minimalement envahissantes. Bien que les deux mandats aient expiré en 2022, de nouveaux mandats ont été décernés. Ces mandats étaient subordonnés à l'engagement du SCRS suivant lequel il présenterait une demande d'annulation ou de modification du mandat provisoire prolongé suivant la décision rendue en l'espèce. Pour aider la Cour dans son analyse des questions juridiques que soulevait la demande, un *amicus curiae* (l'*amicus*) a été nommé dans ce dossier.

Le SCRS a mis la technologie à l'essai dans le cadre d'un projet pilote pendant plusieurs mois en 2018. Pendant cette période, il l'a utilisée sans mandat à plusieurs reprises à l'égard de personnes faisant l'objet d'une enquête, canadiennes ou non, se trouvant au Canada ou à l'étranger. Cependant, des questions relatives à la protection des renseignements personnels ayant été soulevées au sein du SCRS, il a été mis fin au projet pilote en juillet 2018. Par la suite, la technologie a servi exclusivement aux activités d'enquête visant des ressortissants étrangers se trouvant à l'extérieur du Canada et dépourvus de lien avec le Canada, et autres. En juillet 2020, le SCRS a sursis à l'utilisation de la technologie le temps d'obtenir des précisions sur l'application de l'article 8 de la Charte à ses activités de collecte de renseignements sur des ressortissants étrangers dépourvus de lien avec le Canada.

Il s'agissait de savoir si l'article 12 de la Loi sur le SCRS autorise le SCRS à utiliser la technologie au Canada aux quatre fins qu'il a précisées, et ce sans mandat; et si l'article 12 de la Loi sur le SCRS autorise le SCRS à utiliser la technologie à l'extérieur du Canada à l'égard de ressortissants

étrangers dépourvus de lien avec le Canada de la manière plus envahissante qu'il a précisée, et ce sans mandat.

Jugement : la technologie peut être utilisée au Canada, comme proposée, sans mandat; la technologie peut être utilisée à l'extérieur du Canada à l'égard de ressortissants étrangers dépourvus de lien avec le Canada, sans mandat, dans les deux situations décrites.

En l'espèce, le PGC et l'*amicus* s'entendaient pour dire que les quatre usages de la technologie proposés par le SCRS au Canada constitueraient des fouilles ou perquisitions au sens où il faut l'entendre pour l'application de l'article 8. En effet, les personnes au Canada ont une attente raisonnable en matière de vie privée en ce qui a trait aux données susceptibles d'être obtenues au moyen de la technologie. Cependant, le PGC et l'*amicus* divergeaient d'opinion quant à savoir si le recours à la technologie à l'extérieur du Canada à l'égard d'étrangers dépourvus de tout lien avec le Canada constituerait également des fouilles ou perquisitions. Pour ce qui est de la question de savoir si les usages proposés de la technologie au Canada constitueraient des fouilles ou perquisitions abusives, les fouilles et perquisitions exécutées sans mandat, comme celles qui étaient proposées dans la présente affaire, sont présumées abusives. Or, cette présomption peut être réfutée. Il s'agit de démontrer (i) que la fouille ou perquisition est autorisée par la loi, (ii) que la loi elle-même n'a rien d'abusif et (iii) que la fouille ou perquisition n'a pas été effectuée de manière abusive. Le PGC et l'*amicus* s'entendaient pour dire que les quatre usages proposés de la technologie au Canada seraient autorisés par l'article 12 de la Loi sur le SCRS, dès lors que, de par leur nature, ils sont minimalement envahissants. De plus, le PGC et l'*amicus* étaient d'accord pour dire que l'article 12 n'a rien d'abusif, même si, selon l'*amicus*, l'examen du second volet de ce critère à trois volets ne devrait pas s'arrêter là. La loi ayant autorisé les fouilles ou perquisitions proposées n'avait rien d'abusif.

Pour ce qui est de la question de savoir si les fouilles ou perquisitions seraient effectuées d'une manière qui n'est pas abusive, le premier usage proposé de la technologie au Canada porte une atteinte minimale aux intérêts en matière de vie privée des personnes faisant l'objet d'enquêtes du SCRS sur les plans informationnels et géographiques et également ne constituerait pas une fouille ou perquisition « abusive » au sens où il faut l'entendre pour l'application de l'article 8 de la Charte. Par conséquent, cet usage serait autorisé par l'article 12 de la Loi sur le SCRS, sans qu'il soit nécessaire d'obtenir un mandat, à condition que les renseignements recueillis de manière incidente sur des tiers qui ne présentent pas de menace soient supprimés rapidement, avant tout examen. Il ne serait pas judicieux d'assortir d'une condition le premier usage proposé de la technologie, ni les autres usages proposés, au Canada. Pareille atteinte minime aux droits à la vie privée de tiers ne serait pas abusive. En effet, la valeur des renseignements que la technologie permettrait au SCRS d'obtenir l'emporterait sur toute atteinte. L'*amicus* a proposé des conditions pour que les usages proposés de la technologie ne soient pas jugés abusifs lesquelles demandaient que soit imposé des limites précises sur le pouvoir du SCRS de (i) communiquer les données précises et de (ii) conserver les données recueillies de manière incidente à l'égard de tiers innocents. Cependant, la condition proposée portant que les données précises recueillies ne soient pas communiquées à des organismes canadiens ou étrangers n'a pas été acceptée. Cela s'expliquait par le fait qu'interdire la communication des données précises aux partenaires canadiens et étrangers irait à l'encontre de la Loi sur le SCRS et de la jurisprudence applicable. Plus précisément, le paragraphe 19(2) habilite le SCRS à communiquer les renseignements qu'il obtient dans l'exercice de ses fonctions prévues à la loi à des fins précises. Le risque de communication de données non liées à des menaces à un partenaire étranger — ou à un partenaire canadien en dehors des circonstances limitées précisées à cette disposition — est très faible. Selon toute probabilité, une telle communication serait limitée aux situations où l'évaluation des renseignements révèle à tort une menace. Par conséquent, il ne serait pas judicieux d'entraver la capacité du SCRS à communiquer des données précises à ses partenaires canadiens ou étrangers. En bref, il faut définir un délai de conservation des données recueillies de manière incidente par le SCRS. Dès lors que certains autres principes généraux sont suivis, la collecte incidente de données relatives à des tiers non liés à des menaces ne serait pas effectuée de manière abusive.

En ce qui concerne le deuxième usage proposé de la technologie au Canada, il viserait des personnes connues faisant l'objet d'enquêtes du SCRS au Canada. À une exception près, le deuxième usage de la technologie ne serait pas plus envahissant que le premier, en ce qui a trait aux intérêts en matière de vie privée des personnes dont les données sont recueillies. Le deuxième usage proposé ne permettrait pas au SCRS de voir (i) la teneur de communications faites au moyen de l'appareil en question ou (ii) les renseignements stockés dans l'appareil ou accessibles par ce dernier. De même, le SCRS aurait tout avantage à limiter la collecte de données précises de tiers non liés à des menaces. Il ne serait pas judicieux d'imposer comme condition que les données recueillies ne soient pas communiquées aux organismes canadiens ou étrangers pour les mêmes raisons que celles discutées à l'égard du premier usage proposé. En ce qui concerne les données recueillies de manière incidente, à une exception près, cet usage de la technologie ne satisfait à l'article 8 de la Charte que si les données recueillies de manière incidente sont traitées suivant les principes énoncés ci-dessus à l'égard du premier usage, c.-à-d. qu'il faut définir un délai de conservation des données recueillies de manière incidente par le SCRS.

En ce qui concerne le troisième usage proposé de la technologie au Canada, le PGC a soutenu avec raison que cet usage proposé serait minimalement envahissant pour les mêmes raisons que celles énoncées à l'égard du second usage, tant que les principes opérationnels et les mesures traités ci-dessus sont suivis. Les deux premières conditions convenues pour les autres usages étaient judicieuses. L'*amicus* a proposé une troisième condition, qui reprenait le libellé du troisième des quatre types de menaces envers la sécurité du Canada, dont la définition figure à l'article 2 de la Loi sur le SCRS. Aucune raison ne justifiait qu'on limite le troisième usage proposé de la technologie à un seul des quatre types de menaces envers la sécurité du Canada décrits à l'article 2 de la Loi sur le SCRS. En outre, sur le plan pratique, pareille condition serait susceptible d'entraver la capacité du SCRS à évaluer les menaces.

En ce qui concerne le quatrième usage proposé de la technologie au Canada, il faisait intervenir des activités d'enquête se déroulant également à l'étranger. Cet usage de la technologie serait minimalement envahissant, à l'instar des deuxième et troisième usages, pour essentiellement les mêmes motifs. Certes, la collecte de tels renseignements est susceptible d'aider le SCRS à [***]. Or, ces renseignements à eux seuls sont minimalement envahissants. Comme les renseignements obtenus au moyen du quatrième usage seraient [***] que ceux qui résulteraient des deuxième et troisième usages proposés, ils seraient encore moins envahissants que ces derniers. Il s'ensuivait que le quatrième usage proposé de la technologie ne requiert pas l'obtention d'un mandat.

En ce qui concerne l'évaluation des usages proposés de la technologie à l'extérieur du Canada le SCRS a proposé de recourir à la technologie pour recueillir les données dans deux situations. Il serait satisfait au critère des motifs raisonnables de soupçonner que prévoit l'article 12 de la Loi sur le SCRS dans les deux situations. Ainsi, il restait à décider si l'article 12 autorise la portée envahissante de ces usages proposés de la technologie à l'extérieur du Canada sans mandat. Cette question pouvait être tranchée en répondant aux trois questions suivantes : 1) Les ressortissants étrangers dépourvus de lien avec le Canada sont-ils visés par le mot « chacun » qui figure à l'article 8 de la Charte? 2) L'article 12 autorise-t-il les activités d'enquête plus que minimalement envahissantes à l'extérieur du Canada visant des ressortissants étrangers qui ne sont pas protégés par la Charte? 3) Un principe de droit international empêche-t-il les usages plus que minimalement envahissants proposés par le SCRS de la technologie à l'extérieur du Canada à l'égard de ressortissants étrangers dépourvus de lien avec le Canada? L'article 8 de la Charte est ainsi libellé : « [c]hacun a droit à la protection contre les fouilles, les perquisitions ou les saisies abusives ». Le mot « chacun » doit être interprété invariablement de la même manière à l'article 8 qu'aux autres dispositions de la Charte. Donner au mot « chacun » une interprétation plus large à l'article 8 qu'à d'autres dispositions (p. ex., articles 2, 7, 9, 10 et 12) aurait pour effet d'élever les droits protégés par cette disposition au-dessus de ceux que protègent d'autres dispositions de la Charte. À la lumière de la jurisprudence analysée, les ressortissants étrangers qui n'ont pas l'un des trois liens reconnus avec le Canada ((i) citoyenneté canadienne, (ii) présence au Canada ou (iii) faire l'objet de poursuites pénales au Canada) ne sont pas visés par le mot « chacun » qui figure à l'article 8 de la Charte. Par conséquent, les ressortissants étrangers dépourvus de lien reconnu avec le Canada ne peuvent invoquer les droits prévus à l'article 8 de la Charte. La réponse à la première

question était donc non. En ce qui concerne la deuxième question, en l'occurrence, la loi pertinente était l'article 12 de la Loi sur le SCRS. Le paragraphe 12(2) habilite expressément le SCRS à « exercer les fonctions que le paragraphe (1) lui confère même à l'extérieur du Canada ». Comme le SCRS n'est pas contraint d'obtenir une autorisation judiciaire préalable, en application de la Charte ou d'une autre règle de droit, pour utiliser la technologie aux fins envahissantes à l'extérieur du Canada qui étaient en cause dans la présente instance, de telles activités ne nécessitent pas l'obtention d'un mandat. Autrement dit, le SCRS n'est pas tenu d'obtenir un mandat à l'égard des usages proposés de la technologie à l'extérieur du Canada. Par conséquent, la réponse à la deuxième question était oui. Finalement, en ce qui concerne la troisième question, l'*amicus* n'a présenté aucun argument à la Cour au soutien de sa thèse selon laquelle les usages sans mandat de la technologie proposés par le SCRS dans la présente instance seraient contraires au droit international ou à son esprit. Par conséquent, aucun principe de droit international n'interdisait les usages plus que minimalement envahissants de la technologie proposés par le SCRS sans mandat à l'égard de ressortissants étrangers dépourvus de lien avec le Canada à l'extérieur du Canada. Contrairement à ce qu'a affirmé l'*amicus*, cette interprétation ne revenait pas à donner au SCRS « carte blanche en matière de fouille et de perquisition à l'égard de ressortissants étrangers ». Entre autres, le SCRS serait toujours assujetti aux balises énoncées à l'article 12, dont les critères des « motifs raisonnables de soupçonner » et de « la mesure strictement nécessaire ». En outre, la Loi sur le SCRS prévoit des mesures de surveillance des activités du SCRS sous le régime de l'article 12. La réponse à la troisième question était donc non.

En conclusion, les quatre usages proposés par le SCRS de la technologie au Canada ne nécessitent pas l'obtention d'un mandat, une conclusion qui tenait pour acquis que les principes opérationnels et les mesures seraient suivis par le SCRS. Également, les usages proposés par le SCRS de la technologie à l'extérieur du Canada à l'égard de ressortissants étrangers dépourvus de lien avec le Canada ne nécessiteraient pas non plus l'obtention d'un mandat.

LOIS ET RÈGLEMENTS CITÉS

Charte canadienne des droits et libertés, qui constitue la partie I de la Loi constitutionnelle de 1982, annexe B, Loi de 1982 sur le Canada, 1982, ch. 11 (R.-U.) [L.R.C. (1985), appendice II, nº 44], art. 2, 7, 8, 10, 12, 15.

Instructions visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères (Directeur du Service canadien du renseignement de sécurité), 2019-1302.

Loi sur le Service canadien du renseignement de sécurité, L.R.C. (1985), ch. C-23, art. 2, 11.01–11.25, 12, 16, 17, 19, 21.

Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères, L.C. 2019, ch. 13, art. 49.1.

JURISPRUDENCE CITÉE

DÉCISIONS APPLIQUÉES :

X (Re), 2017 CF 1047, [2018] 3 R.C.F. 111; *Loi sur le Service canadien du renseignement de sécurité (Re)*, 2020 CF 697, [2021] 2 R.C.F. 289; *R. c. Spencer*, 2014 CSC 43, [2014] 2 R.C.S. 212; *Slahi c. Canada (Justice)*, 2009 CF 160, [2009] 3 R.C.F. F-6 conf. par 2009 CAF 259; *Singh c. Ministre de l'Emploi et de l'Immigration*, [1985] 1 R.C.S. 177; *X (Re)*, 2014 CAF 249, [2015] 1 R.C.F 684.

DÉCISIONS EXAMINÉES :

Hunter et autres c. Southam Inc., [1984] 2 R.C.S. 145; *R. c. Mills*, 2019 CSC 22, [2019] 2 R.C.S. 320; *Rothman c. La Reine*, [1981] 1 R.C.S. 640; *R. c. Vu*, 2013 CSC 60, [2013] 3 R.C.S. 657; *Mahjoub c. Canada (Citoyenneté et Immigration)*, 2017 CAF 157, [2018]

2 R.C.F. 344; *Ruby c. Canada (Solliciteur général)*, 2002 CSC 75, [2002] 4 R.C.S. 3; *R. c. Kang-Brown*, 2008 CSC 18, [2008] 1 R.C.S. 456; *R. c. Chehil*, 2013 CSC 49, [2013] 3 R.C.S. 220; *R. c. Cornell*, 2010 CSC 31, [2010] 2 R.C.S. 142; *R. c. Cook*, [1998] 2 R.C.S. 597; *R. c. Hape*, 2007 CSC 26, [2007] 2 R.C.S. 292; *Canada (Justice) c. Khadr*, 2008 CSC 28, [2008] 2 R.C.S. 125; *R. v. Harrer*, [1995] 3 R.C.S. 562; *Tabingo c. Canada (Citoyenneté et Immigration)*, 2013 CF 377, [2014] 4 F.C.R. 150, conf. par *Austria c. Canada (Citoyenneté et Immigration)*, 2014 CAF 191, *sub nom. Tabingo c. Canada (Citoyenneté et Immigration)*, [2015] 3 R.C.F. 346; *Amnesty International Canada c. Canada (Procureur général)*, 2008 CF 336, *sub nom. Amnistie internationale Canada c. Canada (Chef d'état-major de la Défense)*, [2008] 4 R.C.F. 546, conf. par 2008 CAF 401, [2009] 4 R.C.F. 149; *Jia c. Canada (Citoyenneté et Immigration)*, 2014 CF 596, [2015] 3 R.C.F 143.

DÉCISIONS MENTIONNÉES :

Loi sur le Service canadien du renseignement de sécurité (Re), 2021 CAF 92, [2021] 4 R.C.F. 41; *Loi sur le service canadien du renseignement de sécurité (Re)*, 2020 CF 616, [2021] 1 R.C.F. 417; *R. c. Thompson*, [1990] 2 R.C.S. 1111; *R. v. Baskaran*, 2020 ONCA 25 (CanLII); *R. v. Brewster*, 2016 ONSC 4133 (CanLII); *X (Re)*, 2016 CF 1105, [2017] 2 R.C.F. 396; *Articles 12 et 21 de la Loi sur le Service canadien du renseignement de sécurité*, L.R.C. (1985), chapitre C-23, 2019 CF 141, [2019] 2 R.C.F. 359; *R. v. Latimer*, 2020 BCSC 2173; *Mahjoub (Re)*, 2013 CF 1096; *Canada (Procureur général) c. Almalki*, 2010 CF 1106, [2012] 2 R.C.F. 508; *Canada (Procureur général) c. Charkaoui*, 2018 CF 849; *R. c. Lloyd*, 2016 CSC 13, [2016] 1 R.C.S. 130; *Dagenais c. Société Radio-Canada*, [1994] 3 R.C.S. 835; *Société Télé-Mobile c. Ontario*, 2008 CSC 12, [2008] 1 R.C.S. 305; *Canada (Commissaire à l'information) c. Canada (Ministre de la Défense nationale)*, 2011 CSC 25, [2011] 2 R.C.S. 306; *Renvoi relatif à la Politique réglementaire de radiodiffusion CRTC 2010-167 et l'ordonnance de radiodiffusion CRTC 2010-168*, 2012 CSC 68, [2012] 3 R.C.S. 489; *Canada (Ministre de la Citoyenneté et de l'Immigration) c. Vavilov*, 2019 CSC 65, [2019] 4 R.C.S. 653.

DOCTRINE CITÉE

Chambre des communes. Comité permanent de la sécurité publique et nationale. *Témoignages*, 41e lég., 2e sess., fascicule no 42 (1er décembre 2014).

Forcese, Craig, « Pragmatism and Principle : Intelligence Agencies and International Law » (2016), 102 Va. L. Rev. 67, Ottawa Faculty of Law Working Paper No. 2016-29.

Schmitt, Michael N., éd., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge : Cambridge University Press, 2017).

Sénat. Comité permanent du Sénat sur la sécurité nationale et la défense, 41e lég., 2e sess., fascicule no 14 (9 mars 2015).

DEMANDE supplémentaire de mandat présentée en vertu des articles 12 et 21 de la *Loi sur le Service canadien du renseignement de sécurité SCRS* pour faire autoriser l'usage par le Service canadien du renseignement de sécurité d'un nouvel outil technologique à l'égard de personnes faisant l'objet d'une enquête. La technologie peut être utilisée au Canada, comme proposée, sans mandat; la technologie peut être utilisée à l'extérieur du Canada à l'égard de ressortissants étrangers dépourvus de lien avec le Canada, sans mandat, dans les deux situations décrites.

ONT COMPARU :

Amy Joslin-Besner, *Jeffrey Johnston* et *Jay Pelletier* pour le demandeur.

Gib van Ert en qualité d'*amicus curiae*.

AVOCATS INSCRITS AU DOSSIER

Le sous-procureur général du Canada pour le demandeur.

Gib van Ert en qualité d'*amicus curiae*.

Ce qui suit est la version française des motifs du jugement et du jugement rendus par

LE JUGE EN CHEF CRAMPTON :

I. Introduction

[1] Le savoir-faire en matière de collecte de renseignement sur des activités clandestines au pays et à l'étranger est en constante évolution. C'est pourquoi l'intérêt public requiert du Service canadien du renseignement de sécurité (SCRS ou le Service) qu'il ne se laisse pas distancer. Toutefois, les mesures qu'il prend à cette fin doivent respecter le cadre de la loi.

[2] La présente instance soulève deux principales questions. Premièrement, le SCRS peut-il adopter une nouvelle technologie (la technologie) au Canada et l'utiliser à quatre fins précises sans mandat dans le cadre d'enquêtes menées conformément à l'article 12 de la *Loi sur le Service canadien du renseignement de sécurité*, L.R.C. (1985), ch. C-23 (la Loi sur le SCRS)? Parmi les quatre usages proposés de la technologie, trois s'appliqueraient exclusivement au Canada, tandis qu'un quatrième s'appliquerait également à l'extérieur du Canada.

[3] Le procureur général du Canada (PGC) admet que les quatre usages de la technologie proposés au Canada constitueraient des « fouilles » ou « perquisitions » au sens où il faut l'entendre pour l'application de l'article 8 de la *Charte canadienne des droits et libertés*, qui constitue la partie I de la *Loi constitutionnelle de 1982*, annexe B, *Loi de 1982 sur le Canada*, 1982, ch. 11 (R.-U.) [L.R.C. (1985), appendice II, nº 44] (la Charte). Toutefois, il affirme que ces fins proposées ne seraient pas « abusives » pour l'application de l'article 8. En effet, (i) elles seraient minimalement envahissantes et seraient donc permises par l'article 12 de la Loi sur le SCRS; (ii) l'article 12 n'a rien d'abusif; (iii) les fouilles ou perquisitions ne seraient pas effectuées d'une manière abusive.

[4] Pour les motifs énoncés ci-après, je suis d'accord. La technologie peut être utilisée au Canada aux quatre fins précises proposées par le SCRS, sans mandat, à condition que les usages de la technologie soient conformes aux motifs énoncés ci-après, tout particulièrement les paragraphes 62, 88, 116 à 117, 126 à 127 et 141.

[5] Deuxièmement, le SCRS peut-il utiliser la technologie à l'extérieur du Canada à l'égard de ressortissants étrangers dépourvus de lien reconnu avec le Canada, et ce sans mandat? Une telle utilisation de la technologie serait plus que minimalement envahissante. Cependant, pour les motifs qui suivent, je suis d'avis que point n'est besoin pour le SCRS de solliciter un mandat pour utiliser la technologie à l'extérieur du Canada aux fins précisées.

[6] En bref, les ressortissants étrangers dépourvus de lien reconnu avec le Canada ne peuvent faire valoir les protections prévues à l'article 8. Ces protections comptent

notamment l'obligation de faire autoriser la fouille ou la perquisition par un arbitre entièrement neutre et impartial en mesure d'agir judiciairement pour mettre en balance les intérêts de l'État et ceux de la personne visée, dans certaines circonstances (*Hunter et autres c. Southam Inc.*, [1984] 2 R.C.S. 145 (*Hunter*), aux pages 160 à 162 et 168 à 169). Aucun principe de droit international susceptible d'interdire au SCRS d'utiliser la technologie à l'extérieur du Canada aux fins précisées et à l'égard de telles personnes, sans mandat, n'a été présenté à la Cour.

[7] Vu la nature confidentielle de la technologie, j'en fournis une description détaillée à l'annexe I des présents motifs, qui restera classifiée. La description générale fournie ci-après dans le corps des motifs a pour objet de faciliter la compréhension du public quant aux questions soulevées en l'espèce, et ce même si la version publique de la présente décision devra tout de même être caviardée, pour des raisons liées à la sécurité nationale.

II. Faits

A. *Principaux usages de la technologie et genèse de l'instance*

[8] En décembre 2021, le SCRS a présenté à la Cour une demande supplémentaire de mandat pour faire autoriser l'usage d'un nouvel outil technologique à l'égard de personnes faisant l'objet d'une enquête menée sous le régime de l'article 12 de la Loi sur le SCRS. Il s'agit [***] une technologie [***] à [***] fonctionnalités. Parmi ces dernières, mentionnons la capacité de déterminer [***] (appareil) [***]. En outre, il est possible de déterminer [***] d'un appareil [***]. Pour obtenir ces renseignements [***] il faut connaître [***] associé à un appareil, [***].[1]

[9] À l'heure actuelle, la technologie permet d'obtenir des renseignements [***] datant [***].

[10] [***]. Il peut alors en inférer [***] de cette personne, ce qui permet de faire avancer l'enquête. La quantité d'information recueillie sur l'objet de l'enquête dépend [***].

[11] La technologie permet également au SCRS de repérer [***] et de déterminer [***]. En outre, la technologie peut aider le SCRS à trouver les [***] et à [***]. D'autres usages possibles de la technologie sont décrits à l'annexe I.

[12] Dans ses observations écrites, le représentant du PGC affirme que la technologie peut être utilisée au Canada à quatre fins précises qui sont minimalement envahissantes. Ainsi, ces usages seraient autorisés par l'article 12 de la Loi sur le SCRS, sans qu'il soit nécessaire d'obtenir un mandat. Les trois premiers usages s'appliquent en sol canadien. Le quatrième usage implique l'accès aux données [***] d'un appareil [tant à l'intérieur qu'à l'extérieur du Canada]. Selon un aspect important de la thèse du PGC à cet égard, les quatre usages sans mandat de la technologie au Canada ne nécessitent pas [***].

[13] Le PGC soutient également que les ressortissants étrangers dépourvus de lien avec le Canada qui se trouvent à l'extérieur du Canada ne sont pas visés par les

[1] [***]

protections prévues par l'article 8 de la Charte. Par conséquent, selon le PGC, le SCRS peut utiliser la technologie à l'égard de ces personnes d'une manière qui est plus que minimalement envahissante, et ce sans mandat. Notamment, il peut [***].

[14] Malgré ce qui précède, le SCRS a sollicité un mandat provisoire [***] (le mandat provisoire), pour lui permettre d'obtenir [***] de personnes faisant l'objet d'enquêtes au Canada, *en vue* [***] *à ces dernières*. Dans sa première lettre à la Cour au sujet du mandat, le PGC explique que les pouvoirs sollicités [TRADUCTION] « sont justifiés, car ils sont minimalement envahissants pour l'application de l'article 12 de la Loi sur le SCRS, et ne nécessitent pas de mandat ». Il sollicite néanmoins le mandat par excès de prudence, pour éviter d'enfreindre la Charte par inadvertance, pendant que (i) le SCRS se familiarise avec les données qui résulteront de l'utilisation de la technologie, et (ii) pendant que la Cour considère si cet usage particulier des données [***] peut être autorisée en vertu de l'article 12 de la Loi sur le SCRS. Le PGC se réserve le droit de se présenter à nouveau à la Cour pour soutenir que les pouvoirs sollicités ne nécessitent pas l'obtention d'un mandat, pour les raisons indiquées plus haut.

[15] À l'audience sur la demande de mandat provisoire tenue le 25 janvier 2022, j'ai soulevé la possibilité que les données [***] des appareils de tiers soient incluses de manière incidente dans l'exercice des pouvoirs visés par le mandat. Pour réduire substantiellement le risque d'une telle situation, j'ai fait modifier le mandat. Ainsi, le pouvoir de recueillir [***] indiqués dans le mandat, pour chacune des personnes nommées dans l'enquête. Faute d'avoir pu obtenir du représentant du PGC un mécanisme semblable ayant pour objet de limiter [***] aux autres articles du mandat, j'ai supprimé ces derniers.

[16] Le jour même où j'ai décerné le mandat provisoire, j'en ai décerné un second, le mandat concernant la [***]. Suivant ce dernier, le SCRS est autorisé à utiliser la technologie à des fins qui ne sont pas minimalement envahissantes, aux dires de ce dernier. Il est autorisé entre autres [***] des appareils des personnes nommées dans l'enquête et dans le mandat provisoire.

[17] Les deux mandats mentionnés plus haut ont expiré le 26 février 2022. Cependant, le juge Norris a décerné le 24 février 2022 d'autres mandats, modifiés, qui ne sont pas pertinents pour la présente instance. Ces mandats étaient subordonnés à l'engagement du SCRS suivant lequel il présenterait une demande d'annulation ou de modification du mandat provisoire prolongé suivant la présente décision.

[18] Pour aider la Cour dans son analyse des questions juridiques que soulève la demande, j'ai nommé M. Gib van Ert à titre d'*amicus curiae* (*amicus*).

B. *Projet pilote du SCRS et contrôle par l'OSSNR*

[19] Le SCRS a mis la technologie à l'essai dans le cadre d'un projet pilote pendant plusieurs mois en 2018. Pendant cette période, il l'a utilisée sans mandat à environ [***] reprises à l'égard de personnes faisant l'objet d'une enquête, canadiennes ou non, se trouvant au Canada ou à l'étranger. Au total, [***] rapports opérationnels, [***] en ont résulté. Cependant, des questions relatives à la protection des renseignements personnels ayant été soulevées au sein du SCRS, il a été mis fin au projet pilote en juillet 2018. Par la suite, la technologie a servi exclusivement aux activités d'enquête visant (i) des ressortissants étrangers se trouvant à l'extérieur du Canada et dépourvus

de lien avec le Canada ou (ii) [***]. En juillet 2020, le SCRS a sursis à l'utilisation de la technologie le temps d'obtenir des précisions sur l'application de l'article 8 de la Charte à ses activités de collecte de renseignements sur des ressortissants étrangers dépourvus de lien avec le Canada.

[20] Pendant la deuxième moitié de 2018, le Comité de surveillance des activités de renseignement de sécurité (CSARS) a entrepris un examen de l'utilisation par le SCRS de la technologie au cours du projet pilote tenu plus tôt dans l'année. C'est l'organisme qui lui a succédé, l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR), qui a clos l'examen. Il a rédigé un rapport intitulé *Examen de l'utilisation par le SCRS de l'outil de collecte de données de géolocation* [***] (examen de l'OSSNR 2018-05) (rapport de l'OSSNR). Le rapport a été « communiqué » au ministre de la Sécurité publique et de la Protection civile en août 2019.

[21] L'OSSNR conclut notamment que l'usage de la technologie [***] constitue des « fouilles » ou « perquisitions » au sens où il faut l'entendre pour l'application de l'article 8 de la Charte. Selon l'OSSNR, « il y avait un risque que le SCRS contrevienne à l'article 8 de la *Charte* pendant la période d'essai au cours de laquelle il a utilisé [la technologie] sans mandat » (rapport de l'OSSNR, à la page 12). Il recommande ce qui suit [à la page 13] :

> […] que le SCRS examine l'utilisation qu'il a faite de [la technologie] jusqu'ici et qu'il détermine quels rapports opérationnels qui en découlent contreviennent à l'article 8 de la *Charte*. Il devrait ensuite supprimer de ses systèmes ces rapports opérationnels et tout document lié à ces résultats.

[22] Selon l'auteur de l'affidavit technique représentant le SCRS (auteur de l'affidavit 1), le SCRS a fini par décider qu'il lui fallait conserver les [***] rapports opérationnels mentionnés plus haut pour respecter ses obligations juridiques. Ces rapports et les pièces jointes ont été mis à l'écart de sorte que les renseignements qu'ils contiennent ne servent pas à faire avancer d'autres enquêtes par le SCRS.

C. *Temps mis par le SCRS à informer la Cour qu'il avait utilisé la technologie à l'égard des personnes nommées dans les mandats décernés par la Cour*

[23] Mentionnons que le SCRS ou le PGC aurait dû informer la Cour du rapport de l'OSSNR prévu bien avant sa communication en août 2019. Ainsi, en attendant le dépôt de la présente demande plus de deux ans plus tard, soit en décembre 2021, ils ont manqué à (i) l'engagement pris en 2016 à l'égard de la Cour par le directeur du SCRS et (ii) à l'obligation de faire preuve du degré le plus élevé de bonne foi applicable dans les instances *ex parte*, tout particulièrement celles intentées sous le régime de la Loi sur le SCRS (*Loi sur le Service canadien du renseignement de sécurité (Re)*, 2021 CAF 92, [2021] 4 R.C.F. 41 (*Loi sur le SCRS (Re)* 2021 CAF), au paragraphe 126).

[24] Plus précisément, le directeur du SCRS à cette époque, M. Michel Coulombe, avait pris l'engagement d'aviser la Cour [TRADUCTION] « dès qu'une question surgit » à propos des mandats décernés par la Cour dans un contrôle par le CSARS, et ce « même si le rapport n'est pas final » (audience en formation plénière, 10 juin 2016, transcription, aux pages 18 et 55). Cet engagement partait du principe que le rapport final et les recommandations étaient susceptibles de différer des renseignements

initiaux communiqués à la Cour. En 2018, le directeur actuel du SCRS a répété sa volonté de respecter l'esprit de cet engagement.

[25] Les explications du PGC quant au défaut d'informer la Cour du rapport de l'OSSNR avant la présente instance ne tiennent pas la route. Premièrement, le PGC affirme (i) que les mandats visaient des personnes qui faisaient l'objet ou allaient par la suite faire l'objet d'une enquête ou d'une collecte de renseignements visé par un mandat et (ii) que les mandats avaient été obtenus et avaient expiré avant la communication du rapport de l'OSSNR. Or, ce n'est pas une raison pour le SCRS de mépriser son engagement ou le degré élevé de transparence auquel il est tenu.

[26] Les personnes visées par des mandats mentionnées dans le rapport de l'OSSNR étaient [***]. Parmi les [***] mandats visant [***] étaient [***] pendant l'examen par l'OSSNR tandis que [***] en juillet 2018 pour un an. Un autre avait été renouvelé pour un an en juillet 2018 et a expiré en juin 2019. On peut raisonnablement inférer de la date du rapport de l'OSSNR, communiqué en août 2019, que les questions qu'il aborde existaient depuis assez longtemps qu'elles auraient dû faire intervenir l'engagement pris par le directeur envers la Cour, mentionné plus haut, et l'obligation de faire preuve du degré le plus élevé de bonne foi dans les communications, bien avant.

[27] Quant aux [***], la technologie a été utilisée à leur égard à l'extérieur du Canada. Des mandats visant [***] d'entre eux ont été sollicités au milieu de 2019 [***]. Le mandat visant le [***] été sollicité [***] dépôt de la demande dans la présente instance. Or, la Cour a été mise au courant de l'utilisation de la technologie à l'égard de ces [***] personnes et des [***] mentionnés plus haut seulement le 18 mai 2022. Il se peut fort bien que la Cour ne l'ait jamais su, si ce n'était de ma directive exigeant du PGC et du SCRS qu'ils informent la Cour si la technologie avait été utilisée à l'égard d'une personne visée ou qui l'était par un mandat décerné par la Cour.

[28] Le PGC a précisé que la Cour n'avait pas été informée de l'utilisation de la technologie à l'égard de ces personnes, car aucun des renseignements ainsi recueillis n'avait servi à justifier une demande de mandat. Cependant, comme le PGC et le SCRS en ont été avisés à plusieurs reprises par le passé, l'information sur les techniques employées à l'égard de personnes faisant l'objet d'une enquête au sujet desquelles une demande de mandat a été présentée ou le sera est utile à la Cour pour l'exercice de son pouvoir discrétionnaire et pour la surveillance des mandats en vigueur.

[29] Dès lors que l'information peut se révéler pertinente dans l'exercice par la Cour de son pouvoir discrétionnaire l'habilitant à décerner ou à modifier un mandat, elle se doit d'être communiquée (*Loi sur le SCRS (Re)* 2021 CAF, au paragraphe 127). L'obligation de faire preuve du degré le plus élevé de bonne foi et de transparence n'exige guère moins.

[30] C'est le cas, que l'information ait servi à justifier une demande de mandat ou non.

[31] Il est entendu que c'est également le cas même si l'auteur de l'affidavit représentant le SCRS juge que l'information n'est pas de celles qui doivent être indiquées dans la demande de mandat, conformément aux alinéas 21(2)a) et b) de la Loi sur le SCRS (*Loi sur le SCRS (Re)* 2021 CAF, au paragraphe 133), et ce pour deux raisons. Premièrement, il se peut que l'information se révèle pertinente dans l'exercice

par la Cour de son pouvoir discrétionnaire. Deuxièmement, il se peut que la Cour ne partage pas l'avis de l'auteur de l'affidavit sur la teneur et l'application des alinéas 21(2)a) et b).

[32] Vu la décision de la Cour dans l'affaire *Loi sur le service canadien du renseignement de sécurité (Re)*, 2020 CF 616, [2021] 1 R.C.F. 417, ainsi que les principes généraux énoncés par la suite dans l'arrêt *Loi sur le SCRS (Re)* 2021 CAF, aux paragraphes 120 à 133, le PGC et le SCRS reconnaissent que l'obligation élevée de franchise requiert la communication de toute l'information susceptible de se révéler pertinente pour la Cour appelée à décider s'il faut décerner un mandat et, dans l'affirmative, quelles conditions imposer. Il peut s'agir d'information n'ayant pas servi à justifier une demande de mandat. Le PGC et le SCRS acceptent également que la conclusion de l'OSSNR — selon laquelle l'utilisation par le SCRS de la technologie au Canada était susceptible d'enfreindre l'article 8 de la Charte — fasse intervenir l'obligation élevée d'exposer les faits de manière complète et sincère. Ils reconnaissent aussi que la Cour est habilitée, si elle est informée de faits qui font intervenir cette obligation, de mettre fin à un mandat, de refuser d'en décerner d'autres ou d'ordonner quelque autre réparation.

III. Questions

[33] La présente instance soulève deux principales questions, qui sont énoncées ci-après :

1. L'article 12 de la Loi sur le SCRS autorise-t-il le SCRS à utiliser la technologie au Canada aux quatre fins qu'il a précisées, et ce sans mandat?

2. L'article 12 de la Loi sur le SCRS autorise-t-il le SCRS à utiliser la technologie à l'extérieur du Canada à l'égard de ressortissants étrangers dépourvus de lien avec le Canada de la manière plus envahissante qu'il a précisée, et ce sans mandat?

IV. Évaluation des usages proposés au Canada (question nº 1)

A. *Résumé des quatre usages proposés et introduction*

[34] Comme il est mentionné plus haut, trois des usages proposés de la technologie auraient lieu entièrement au Canada. Les voici :

i) À l'égard de personnes faisant l'objet d'enquêtes du SCRS, [***] au Canada [***].

ii) À l'égard de personnes faisant l'objet d'enquêtes du SCRS [***] au Canada, [***].

iii) [***] au Canada [***].

[35] Le quatrième usage proposé de la technologie [***] implique de recueillir les données [***] d'appareils (tant à l'intérieur qu'à l'extérieur du Canada).[2]

[2] [***]

[36] Les principes juridiques généraux applicables à l'utilisation par le SCRS d'une nouvelle technologie visant à recueillir des renseignements concernant les appareils de communication mobile de personnes faisant l'objet d'une enquête ont été analysés en profondeur dans la décision *X (Re)*, 2017 CF 1047, [2018] 3 R.C.F. 111 (*IMSI*). Dans cette affaire, la Cour applique la jurisprudence définissant ce qui constitue des fouilles ou perquisitions et ce qui les rend « abusives » au sens où il faut l'entendre pour l'application de l'article 8 de la Charte. À l'instar de la présente espèce, l'affaire *IMSI* porte sur une demande présentée en vertu des articles 12 et 21 de la Loi sur le SCRS.

[37] Dans cette affaire, la Cour estime que le recours sans mandat par le SCRS à un émulateur de station de base (ESB) pour repérer les caractéristiques des appareils de communication mobile d'une personne faisant l'objet d'une enquête au Canada constitue bel et bien des « fouilles » ou « perquisitions », mais elles ne sont pas « abusives ». Par ces caractéristiques, on entend les numéros *International Mobile Subscriber Identity* (identité internationale d'abonnement mobile) et *International Mobile Equipment Identity* (identité internationale d'équipement mobile). Il s'agit de numéros émis par les appareils de l'objet de l'enquête à certains moments.

[38] Dans l'affaire *Loi sur le Service canadien du renseignement de sécurité (Re)*, 2020 CF 697, [2021] 2 R.C.F. 289 (*SCRS 2020*), la Cour rend des conclusions semblables sur le recours à (i) la technologie relative aux ESB visant à trouver les mêmes renseignements que ceux dont il est question dans l'affaire *IMSI* [***]. Cependant, elle finit par conclure que le SCRS doit obtenir un mandat pour [***] déterminer [***] des intéressés, car cette méthode révèle beaucoup plus de renseignements personnels sur l'utilisateur de l'appareil de communication *SCRS 2020*, paragraphes 118 à 125, 166 à 169 et 176 à 181). Ces conclusions intéressent une demande présentée en vertu des articles 16 et 21 de la Loi sur le SCRS.

[39] Dans l'affaire *IMSI*, la Cour conclut que l'obtention des caractéristiques permettant de détecter l'appareil mobile de l'objet d'une enquête ne constitue pas des fouilles ou perquisitions « abusives ». Elle fonde cette conclusion sur trois principales constatations : (i) la fouille ou la perquisition était autorisée par une disposition légale, à savoir l'article 12 de la Loi sur le SCRS, (ii) la disposition n'a rien d'abusif et (iii) la fouille ou perquisition ne serait pas effectuée de manière abusive (*IMSI*, paragraphes 198 à 201, 236 et 238 à 243).

[40] L'article 12 est ainsi rédigé :

> **Informations et renseignements**
>
> **12 (1)** Le Service recueille, au moyen d'enquêtes ou autrement, dans la mesure strictement nécessaire, et analyse et conserve les informations et renseignements sur les activités dont il existe des motifs raisonnables de soupçonner qu'elles constituent des menaces envers la sécurité du Canada; il en fait rapport au gouvernement du Canada et le conseille à cet égard.
>
> **Aucune limite territoriale**
>
> **(2)** Il est entendu que le Service peut exercer les fonctions que le paragraphe (1) lui confère même à l'extérieur du Canada.

[41] Dans son examen des pouvoirs conférés par l'article 12, la Cour dans la décision *IMSI* fait la remarque suivante [au paragraphe 196] :

> Selon le libellé simple de l'article 12, le SCRS recueille, au moyen d'une enquête ou autrement, dans la mesure strictement nécessaire, et analyse et conserve les informations et les renseignements sur les activités dont il existe des motifs raisonnables de soupçonner qu'elles constituent des menaces envers la sécurité du Canada. Cela donne au SCRS le pouvoir explicite d'enquêter sur de telles menaces dans ces circonstances.

[42] La Cour fait ensuite observer que l'article 12 habilite le SCRS à recueillir, à analyser et à conserver des renseignements obtenus de façon non envahissante ou très envahissante. Cependant, dès lors que le SCRS « passe à des activités de collecte plus envahissantes, le Service doit obtenir un mandat » (*IMSI*, au paragraphe 219). N'oublions pas que cet énoncé concerne l'application de l'article 8 de la Charte aux activités de collecte envahissantes menées par le SCRS au Canada. Il est possible d'inférer de cette jurisprudence et des dispositions de l'article 21 qui portent sur les mandats que le législateur entendait implicitement que le SCRS demande une autorisation judiciaire avant de se livrer à des activités de collecte qui ne sont pas minimalement envahissantes (*IMSI*, au paragraphe 219).

[43] Le PGC et l'*amicus* s'entendent pour dire que la décision de la Cour dans l'affaire *IMSI* offre un bon point de départ pour l'analyse de certaines des questions importantes en l'espèce.

[44] Dans mon examen, je vais garder à l'esprit la nécessité d'adopter à l'égard de l'article 8 une « approche téléologique axée principalement sur la protection de la vie privée considérée comme une condition préalable à la sécurité individuelle, à l'épanouissement personnel et à l'autonomie ainsi qu'au maintien d'une société démocratique prospère » (*R. c. Spencer*, 2014 CSC 43, [2014] 2 R.C.S. 212, au paragraphe 15).

B. *Les usages proposés de la technologie au Canada constitueraient-ils des fouilles ou perquisitions?*

[45] Dans l'affaire *IMSI*, la Cour conclut que l'objet de l'enquête a une attente raisonnable en matière de vie privée en ce qui a trait aux caractéristiques permettant de repérer ses appareils mobiles (*IMSI*, aux paragraphes 140, 177 et 189). Cette attente découle de la nature des renseignements que le SCRS a commencé à recueillir au sujet des activités privées de l'intéressé, une fois qu'il a mis la main sur les identifiants numériques des appareils. L'atteinte par le SCRS à cette attente raisonnable constitue une fouille ou perquisition au sens où il faut l'entendre pour l'application de l'article 8 et fait intervenir les intérêts en matière de respect de la vie privée qui y sont protégés (*IMSI*, aux paragraphes 111, 149 et 247).

[46] En l'espèce, le PGC et l'*amicus* s'entendent pour dire que les quatre usages de la technologie proposés par le SCRS au Canada constitueraient des fouilles ou perquisitions au sens où il faut l'entendre pour l'application de l'article 8. En effet, les personnes au Canada ont une attente raisonnable en matière de vie privée en ce qui a trait aux données [***], susceptibles d'être obtenues au moyen de la technologie. Cependant, le PGC et l'*amicus* divergent d'opinion quant à savoir si le recours à la technologie à l'extérieur du Canada à l'égard d'étrangers dépourvus de tout lien avec le Canada constituerait également des fouilles ou perquisitions. J'en traite à la partie IV.C.(3)d).

C. *Les usages proposés de la technologie au Canada constitueraient-ils des fouilles ou perquisitions abusives?*

[47] Les fouilles et perquisitions exécutées sans mandat, comme celles qui sont proposées dans la présente affaire, sont présumées abusives. Or, cette présomption peut être réfutée. Il s'agit de démontrer (i) que la fouille ou perquisition est autorisée par la loi, (ii) que la loi elle-même n'a rien d'abusif et (iii) que la fouille ou perquisition n'a pas été effectuée de manière abusive (*Spencer*, au paragraphe 68).

1) Les fouilles ou perquisitions proposées sont-elles autorisées par la loi?

[48] Le PGC et l'*amicus* s'entendent pour dire que les quatre usages proposés de la technologie au Canada seraient autorisés par l'article 12 de la Loi sur le SCRS, dès lors que, de par leur nature, ils sont minimalement envahissants. L'*amicus* affirme qu'il faut pour cela que le SCRS respecte certaines conditions dont traite la partie IV.C. (3), qui porte sur le caractère non abusif des fouilles ou perquisitions proposées.

2) La loi qui les autorise a-t-elle quelque chose d'abusif?

[49] Le PGC et l'*amicus* sont d'accord pour dire que l'article 12 n'a rien d'abusif. Cependant, selon l'*amicus*, l'examen du second volet de ce critère à trois volets ne devrait pas s'arrêter là. À son avis, la Cour est par ailleurs tenue d'examiner [***], ainsi que [***].

[50] Selon l'*amicus*, on ne peut raisonnablement conclure que [***] prévoient l'utilisation des données [***] aux fins de sécurité nationale.

[51] Au soutien de sa thèse, il fait remarquer que le rapport de l'OSSNR contient la remarque suivante à la page 7 :

[***].

[52] En outre, l'*amicus* fait observer que plusieurs [***], présentés en pièces jointes à un affidavit souscrit par l'auteur de l'affidavit 1, contiennent des remarques semblables. À propos des données que permet d'obtenir la technologie, il cite l'énoncé suivant : [***].[3]

[53] [Ce paragraphe décrit un argument juridique mis de l'avant par l'*amicus* à savoir si un instrument, autre qu'une loi ou un règlement, doit être pris en compte en plus de l'article 12 de la Loi sur le SCRS, lorsqu'il s'agit d'évaluer si l'utilisation de la technologie est autorisée par la loi. L'*amicus* propose que la prise en considération de l'instrument soutient la conclusion que ce dernier est « abusif » au sens où il faut l'entendre pour l'examen auquel la Cour doit procéder à la lumière de l'article 8 de la Charte.]

[54] En réponse, le PGC fait valoir que, pour l'application de l'article 8, [***] peut se révéler pertinente lorsqu'il s'agit de déterminer si une activité envahissante menée dans le cadre d'une enquête constitue une fouille ou perquisition. En revanche, elle ne l'est pas lorsqu'il s'agit de déterminer si une fouille ou perquisition est abusive, sauf s'il existe une preuve d'activité illégale. Le PGC fait observer qu'il n'existe aucune preuve de la sorte, ni à l'égard de l'obtention des données [***]. En fait, la preuve, s'il en est, va

[3] [***]

dans l'autre sens. Tout particulièrement, aux termes d'un document [***] qui présente un [***], [TRADUCTION] « la collecte des données est effectuée en toute légalité [***] ».[4]

[55] Le PGC affirme que la thèse de l'*amicus* à cet égard confond l'absence de renonciation à l'attente raisonnable en matière de vie privée et le pouvoir légal non abusif de porter atteinte à cette attente raisonnable. Ce dernier ne dépend pas du consentement de l'utilisateur à une telle intrusion ou de son attente raisonnable à cet égard. Le PGC soutient que, sans attente raisonnable en matière de vie privée, il n'y a pas de fouille ou de perquisition. Partant, point n'est besoin de déterminer si la loi qui autorise la fouille ou perquisition a quelque chose d'abusif.

[56] Au soutien de sa thèse, le PGC soulève la conclusion de la Cour dans l'affaire *IMSI* selon laquelle l'interception d'identifiants d'appareils mobiles sans mandat est légale, et ce même si [***]. Autrement dit, [***] n'est pas pertinent à la détermination de [***].

[57] Le PGC fait également observer que la Cour suprême du Canada, dans une affaire criminelle, reconnaît que les policiers « peuvent faire appel à la créativité et au subterfuge » et « user d'artifices et d'autres formes de supercherie » dans leur travail d'enquête (*R. v. Mills*, 2019 CSC 22, [2019] 2 R.C.S. 320, au paragraphe 43; *Rothman c. La Reine*, [1981] 1 R.C.S. 640, à la page 697).

[58] [Ce paragraphe décrit les conclusions de la Cour à l'effet que l'instrument était pertinent lorsqu'il s'agit de déterminer si l'utilisateur d'un appareil a une attente raisonnable en matière de vie privée à l'égard de ses données, mais n'était pas pertinent lorsqu'il s'agit pour la Cour de décider si l'atteinte à cette attente raisonnable proposée par le SCRS est autorisée par une loi qui n'a rien d'abusif.]

[59] Vu ce qui précède, et comme l'*amicus* reconnaît que l'article 12 de la Loi sur le SRCS n'a rien d'abusif, il s'ensuit que la loi ayant autorisé la fouille ou perquisition n'a rien d'abusif.

3) Les fouilles ou perquisitions seraient-elles effectuées d'une manière qui n'est pas abusive?

a) *Premier usage proposé de la technologie au Canada*

(i) Objets d'enquête

[60] Dans un tel scénario, la technologie serait utilisée à l'égard de personnes connues faisant l'objet d'enquêtes du SCRS. Ainsi, [***].

[61] Pareil usage de la technologie sans mandat s'assimile à celui dont il est question aux paragraphes 14 et 15 des présents motifs relativement au mandat provisoire. Comme il est indiqué plus haut, le SCRS avait demandé ce mandat par précaution, pour veiller à ne pas enfreindre la Charte par inadvertance, pendant que (i) le SCRS se familiariser avec les données qui résulteront (de l'utilisation de la technologie), et (ii) pendant que la Cour considère si cet usage particulier des données [***] peut être autorisée en vertu de l'article 12 de la Loi sur le SCRS. À l'époque, le SCRS a

[4] [***]

expressément indiqué qu'il se réservait le droit de se présenter à nouveau devant la Cour pour plaider que cette utilisation de la technologie était minimalement envahissante et ne nécessitait donc pas l'obtention d'un mandat.

[62] Pour nombre des mêmes motifs que ceux formulés dans les affaires *IMSI* et *SCRS 2020*, je suis d'avis que l'usage proposé de la technologie (i) porte une atteinte minimale aux intérêts en matière de vie privée des personnes faisant l'objet d'enquêtes du SCRS sur les plans informationnels et géographiques et (ii) ne constituerait pas une fouille ou perquisition « abusive » au sens où il faut l'entendre pour l'application de l'article 8 de la Charte (*IMSI*, aux paragraphes 161 à 163 et 187 à 189; *SCRS 2020*, aux paragraphes 124 à 125 et 166 à 168). Par conséquent, cet usage serait autorisé par l'article 12 de la Loi sur le SCRS, sans qu'il soit nécessaire d'obtenir un mandat, à condition que les renseignements recueillis de manière incidente sur des tiers qui ne présentent pas de menace soient supprimés rapidement, avant tout examen. J'y reviens ci-après.

[63] Suivant le premier usage de la technologie proposé au Canada, le SCRS effectuerait des recherches concernant des personnes connues faisant l'objet d'enquêtes [***]. Le SCRS pourrait alors solliciter un mandat [***].

[64] Sans mandat, les données [***] obtenues par le SCRS au moyen de la technologie auraient une portée très limitée. Tout au plus, il s'agirait [***]. Si l'obtention par le SCRS de ces données porte atteinte à l'attente raisonnable en matière de vie privée des personnes faisant l'objet d'enquêtes à l'égard des données [***] de [***], une telle atteinte est minimale, [***].

[65] Comme dans l'affaire *IMSI*, le SCRS ne serait pas en mesure d'intercepter les communications effectuées au moyen des appareils ou les renseignements stockés dans l'appareil ou accessibles au moyen de l'appareil. En outre, cet usage proposé de la technologie ne révélerait rien des activités des objets d'enquêtes du SCRS. [***], l'objet de l'enquête ne remarquerait aucun changement dans l'utilisation de ses appareils.

[66] Soulignons que le PGC admet que le SCRS ne serait pas autorisé à utiliser la technologie pour [***], sans mandat. [***]. Par conséquent, l'utilisation de la technologie à ces fins nécessiterait l'obtention d'un mandat.

[67] Certes, en attribuant [***] à l'appareil [***] d'une personne faisant l'objet d'une enquête, le SCRS est peut-être à même de brosser un tableau de cette personne ou d'ajouter à celui qu'il possède déjà. Or, on voit difficilement comment les inférences qu'il peut tirer sur les activités privées de cette personne seraient particulièrement solides ou intimes (*IMSI*, aux paragraphes 163 et 189; [SCRS_2020], aux paragraphes 123 à 125 et 166 à 168). Je suis convaincu que ces inférences n'intéresseraient pas des renseignements biographiques essentiels. [***].

[68] Comme dans les affaires *IMSI* et [SCRS_2020], le fait que la technologie est minimalement envahissante, très précise et étroitement ciblée étaye ma conclusion selon laquelle la fouille ou perquisition n'est pas abusive (*IMSI*, aux paragraphes 7, 207, 209 et 236(i); [SCRS_2020], aux paragraphes 123 à 125, 161 et 166 à 168). Cette grande précision et cette portée étroitement ciblée s'appliquent à l'information obtenue

par le SCRS [***] qui est ensuite filtrée davantage grâce aux paramètres [***] indiqués pour obtenir les résultats souhaités au moyen de la technologie.

[69] Signalons que je n'attribue guère d'importance au fait que les données [***] qui résultent de l'utilisation de la technologie sont, [***] et ce pour deux raisons. Premièrement, l'information [***]. Deuxièmement, la nature de l'information obtenue est telle que le degré (minime) d'atteinte ne change pas sensiblement du fait [***]. Autrement dit, rien dans la nature [***] d'un appareil [***]. La collecte est tout autant envahissante dans un cas comme dans l'autre : elle l'est minimalement.

(ii) Tiers ne présentant pas de menace

[70] Certaines techniques d'enquête légitimes ont pour inconvénient malheureux la possibilité que les renseignements personnels de « tiers innocents » soient inévitablement captés (*R. c. Thompson*, [1990] 2 R.C.S. 1111 (*Thompson*), aux pages 1143 à 1144. Par conséquent, lorsqu'elle est saisie d'une demande de mandat présentée sous le régime de la Loi sur le SCRS, la Cour est résolue à tenter de limiter pareilles atteintes incidentes à l'intérêt de tiers en matière de vie privée. Autrement dit, la Cour cherche à veiller à ce que la collecte incidente de renseignements concernant des tiers ne soit ni plus envahissante, ni plus large que ce qui est raisonnablement nécessaire au SCRS pour atteindre les objectifs d'enquête légitime (*IMSI*, au paragraphe 253).

[71] Dans certaines enquêtes mettant en jeu les données concernant des appareils de communication mobiles, les tribunaux reconnaissent qu'il peut se révéler raisonnablement nécessaire d'autoriser la collecte d'une petite quantité de données minimalement envahissantes concernant un très grand nombre de tiers (*IMSI*, aux paragraphes 66 à 67; *R. v. Baskaran*, 2020 ONCA 25 (CanLII), aux paragraphes 18 et 21 à 23; *R. v. Brewster*, 2016 ONSC 4133 (CanLII) (*Brewster*), aux paragraphes 60 à 62).

[72] Si les tribunaux acceptent, au moment de l'autorisation, la nécessité pratique d'obtenir une grande quantité de renseignements peu envahissants, ils font néanmoins en sorte que l'information concernant des tiers ne présentant pas de menace soit détruite rapidement et, dans la mesure du possible, ne fasse l'objet d'aucun examen (*IMSI*, aux paragraphes 5, 156 et 252 à 254; *SCRS 2020*, aux paragraphes 17 et 168; *X (Re)*, 2016 CF 1105, [2017] 2 R.C.F. 396, aux paragraphes 186 à 188; *Articles 12 et 21 de la Loi sur le Service canadien du renseignement de sécurité, L.R.C. (1985), chapitre C-23*, 2019 CF 141, [2019] 2 R.C.F. 359, aux paragraphes 32 et 37 à 39).

[73] Ainsi, par « tiers ne présentant pas de menace » on entend les personnes qui ne sont pas impliquées dans les menaces envers la sécurité du Canada, au sens de l'article 2 de la Loi sur le SCRS.

[74] En l'espèce, chacun des quatre usages proposés de la technologie au Canada se soldera probablement par la collecte incidente de données [***] concernant les appareils de tiers ne présentant pas de menace. Seule exception : lorsque la technologie vise.

[75] Heureusement, le SCRS a de bonnes raisons de limiter [***] que vise la technologie pour en tirer les données [***]. [***].

[76] En outre, dans certaines circonstances, les données [***] de tiers peuvent être facilement reconnues et rapidement supprimées sans qu'en souffre l'enquête du SCRS. [***]. Comme dans l'affaire *IMSI*, [***] *IMSI* [***].

[77] C'est pourquoi j'ai fait insérer une condition quant à [***] dans le mandat provisoire décerné le 25 janvier 2022 (voir les paragraphes 14 et 15 des présents motifs). En bref, l'utilisation de la technologie autorisée se limitait aux situations où les données [***] devaient être obtenues à [***] indiqués dans le mandat, à l'égard de chacune des personnes nommées faisant l'objet de l'enquête. Comme dans l'affaire *IMSI*, les données [***] seraient supprimées rapidement conformément à une condition dont était assorti le mandat, sans aucune analyse (*IMSI*, aux paragraphes 5, 7, 156, 236(i), 242 et 253).

[78] Après que j'ai décerné le mandat provisoire, le PGC a déposé d'autres observations. Entre autres, il affirme que limiter l'usage de la technologie [***] restreindrait de manière inacceptable la portée de l'enquête et la ralentirait. Le PGC cite le passage suivant de l'arrêt *R. c. Vu*, 2013 CSC 60, [2013] 3 R.C.S. 657, au paragraphe 57 :

> […] Bref, les tentatives en vue d'imposer des protocoles de perquisition à l'étape de l'autorisation risquent 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 d'ailleurs amplifiés par l'évolution rapide et constante de la technologie.

[79] Le PGC mentionne les remarques semblables figurant dans la décision *R. v. Latimer*, 2020 BCSC 2173, au paragraphe 101.

[80] Le PGC illustre sa thèse de deux exemples. Dans le premier cas, il s'agit d'une enquête [***]. Dans ce cas, selon le PGC, il serait tout à fait possible que le SCRS [***]. Le second exemple concerne [***]. Ce qu'il entend par là, clairement, c'est que des vies innocentes seraient en jeu entre-temps.

[81] Vu ce qui précède et après mûre réflexion, je conviens qu'il ne serait pas judicieux d'assortir d'une condition [***] le premier usage proposé de la technologie, ni les autres usages proposés, au Canada. Signalons que l'*amicus* est du même avis.

[82] Je suis convaincu que, vu la nature de la technologie, le SCRS aura de bonnes raisons de procéder [***] dans la mesure du possible. Il pourrait alors rapidement détecter les données [***] des personnes faisant l'objet de ses enquêtes, [***]. Dans ces cas, il serait facile de distinguer les données [***] des appareils de tiers [***] seraient rapidement supprimées sans aucune analyse. Dans les circonstances, toute atteinte aux droits à la vie privée de tiers serait temporaire et limitée [***].

[83] Pareille atteinte minime aux droits à la vie privée de tiers ne serait pas abusive. En effet, la valeur des renseignements que la technologie permettrait au SCRS d'obtenir l'emporterait sur toute atteinte (*IMSI*, au paragraphe 211). De plus, les paramètres [***], s'ils sont combinés, permettraient de réduire la portée de la collecte — même temporaire — des données [***]. Comme dans l'affaire *IMSI*, la portée étroitement ciblée, la très grande précision et la nature peu envahissante des usages proposés de la technologie permettent de conclure qu'ils ne porteraient pas une atteinte abusive aux droits à la vie privée de tiers.

[84] Un autre facteur permet de faire en sorte que de telles atteintes ne soient pas abusives : la technologie ne peut être utilisée qu'en conformité avec les balises prévues à l'article 12 de la Loi sur le SCRS. Il s'agit notamment de la nécessité pour le SCRS d'avoir des « motifs raisonnables de soupçonner » et d'avoir recours à la technologie « dans la mesure strictement nécessaire ». En outre, [***] pourrait consulter les résultats obtenus au moyen de la technologie. À cet égard, l'auteur de l'affidavit 1 affirme dans son témoignage que [***] employés du SCRS disposent à l'heure actuelle [***] les habilitant à utiliser la technologie (transcription de l'audience du 9 février 2021, à la page 95; voir également *Brewster*, aux paragraphes 60 à 62). Selon lui, seuls ces [***] employés [***] recueillis au moyen de la technologie dans le cadre du premier usage proposé. De même, ils seraient les seuls à déterminer si [***] recueillis au moyen des deuxième et troisième usages, dont il est question ci-après, sont liés à des menaces [***] en vue de décider s'il convient de conserver les données. Je signale que, pour ce faire, ils pourraient cependant consulter le poste opérationnel.

[85] Examinons les situations où l'utilisation de la technologie ne peut raisonnablement [***]. À l'audience sur le mandat provisoire, j'ai soulevé la possibilité d'imposer un seuil maximal relatif au nombre de tiers dont les données [***] pourraient être recueillies [***]. Le PGC a fait à nouveau valoir que l'utilité de la technologie en souffrirait beaucoup. Rappelant le second exemple mentionné plus haut, à propos [***] il affirme qu'un tel seuil [***].

[86] De manière plus générale, le PGC affirme qu'utiliser la technologie n'emporte pas une collecte inacceptable de données à grande échelle ni ne rend la fouille ou perquisition abusive au motif qu'elle a une portée excessive. Ce serait le cas, même si l'utilisation de la technologie permettait de recueillir des données [***] à l'égard d'un grand nombre de tiers innocents. L'*amicus* est du même avis.

[87] Le PGC ajoute que le premier usage proposé de la technologie au Canada permettrait en pratique de recueillir [***] un volume de données de tiers [TRADUCTION] « probablement minime, voire inexistant ». En effet, la technologie [***] à l'objet d'une enquête si elle était utilisée [***] tiers seraient susceptibles de se trouver. Dans un tel cas, [***] seraient recueillis par la technologie. [***].

[88] Vu ce qui précède, je suis convaincu qu'il ne serait pas judicieux d'imposer un seuil maximal arbitraire quant au nombre [***] au moyen de la technologie. C'est le cas même si l'utilisation de la technologie vise [***]. Cependant, dans toutes les circonstances, les [***] données [***] recueillies à l'égard des appareils de tiers non liés à des menaces doivent être rapidement supprimées et ne peuvent faire l'objet d'aucune analyse (voir les paragraphes 62, 116, 117, 126 et 127 des présents motifs). Il est entendu que le SCRS n'est pas autorisé à interroger les bases de données qu'il a élaborées pour l'application de l'article 12 pour vérifier les renseignements de tiers recueillis de manière incidente. Nous y revenons à la rubrique suivante.

[89] Ma décision est justifiée par le fait que le SCRS a tout avantage à limiter le nombre d'appareils appartenant à des tiers non liés à des menaces dont les données [***] sont recueillies. Comme il est expliqué plus haut, [***]. Dans ce cas, la technologie permettrait en fait d'atteindre l'objectif du deuxième usage proposé, expliqué dans la rubrique suivante.

[90] Bref, pour les motifs indiqués plus haut, je suis d'avis que le premier usage proposé au Canada n'emporterait pas une atteinte abusive aux droits à la vie privée de tiers non liés à des menaces, et ce même [lorsque l'utilisation] permettrait de recueillir les [***] données [***] d'un grand nombre de tiers non liés à des menaces.

(iii) Comparaison des données recueillies de manière incidente aux données recueillies antérieurement

[91] Dans ses observations écrites supplémentaires, le PGC fait remarquer que le SCRS est susceptible d'interroger ses bases de données élaborées pour l'application de l'article 12 pour vérifier si [***] recueillis de manière incidente révèlent des menaces. Dans l'affirmative, ces [***] seraient ajoutés aux fonds de renseignements du SCRS pour servir par la suite à des recherches.

[92] À mon avis, une telle vérification dans les fonds de renseignements va à l'encontre de l'objet énoncé du premier usage de la technologie, qui se limite à [***] une personne connue faisant l'objet d'une enquête. En outre, pareil exercice ne serait pas conforme à l'affirmation du PGC selon laquelle le SCRS [TRADUCTION] [***]. Il ajoute ce qui suit :

> [TRADUCTION] [***].

[93] Lorsque le SCRS est en mesure de procéder à [***]. Les données [***] recueillies d'autres appareils [***] devraient être supprimées rapidement sans aucune analyse. Il en est de même des « circonstances [***] » où le SCRS [***] au moyen de la technologie. En effet, le PGC affirme que ces situations se produiraient seulement si le SCRS a des motifs raisonnables de soupçonner que la personne faisant l'objet de l'enquête [***] interroger ses bases de données élaborées en application de l'article 12 [***] recueillis de manière incidente serait autoriser une recherche à l'aveuglette, ce qui serait abusif (*Hunter*, à la page 167; *Thompson*, à la page 1145). Il est entendu que cette observation ne s'applique qu'au premier usage proposé de la technologie au Canada.

(iv) Conditions proposées par l'*amicus*

[94] Selon l'*amicus*, il faut, pour que les usages proposés de la technologie ne soient pas jugés abusifs, imposer des limites précises sur le pouvoir du SCRS de (i) communiquer les données [***] et de (ii) conserver les données [***] recueillies de manière incidente à l'égard de tiers innocents. Plus précisément, l'*amicus* affirme que chaque usage proposé de la technologie au Canada ne porte une atteinte minimale aux droits garantis par l'article 8 que si les conditions suivantes sont imposées :

(a) les données [***] recueillies [***] ne sont pas communiquées à des organismes canadiens ou étrangers;

(b) les données recueillies de manière incidente (à l'égard de personnes dont on n'a pas de motifs raisonnables de soupçonner qu'elles représentent une menace envers la sécurité du Canada) sont supprimées dès que possible sans être téléversées dans les fonds de renseignements du SCRS.

[95] L'*amicus* soutient que le SCRS est impuissant à l'égard de l'utilisation par ses partenaires du milieu de la sécurité des données qui leur seraient communiquées, tout particulièrement ses partenaires étrangers. L'auteur de l'affidavit principal (l'auteur de l'affidavit 2) l'a reconnu. Il a aussi admis ne pas savoir si le SCRS avait pour politique d'informer ses partenaires étrangers s'il concluait [***] qui leur avait été communiqué n'était pas lié à des menaces.

[96] Par conséquent, selon l'*amicus*, la communication des données [***] ouvre la porte à des usages que la Cour ne peut ni entrevoir ni limiter, y compris des usages susceptibles de faire beaucoup de mal aux intéressés. Sans aucune limite sur la communication de ces données, la Cour ne peut conclure que les usages proposés de la technologie seraient minimalement envahissants. Ainsi, l'*amicus* affirme que, s'il n'est pas nécessaire pour le SCRS de communiquer [***] aux fins [***] il devrait s'en abstenir.

[97] En réponse, le PGC affirme qu'interdire la communication des données [***] aux partenaires canadiens et étrangers irait à l'encontre de la Loi sur le SCRS et de la jurisprudence applicable. Je suis d'accord.

[98] L'article 19 de la Loi sur le SCRS est ainsi libellé :

> **Autorisation de communication**
>
> **19 (1)** Les informations qu'acquiert le Service dans l'exercice des fonctions qui lui sont conférées en vertu de la présente loi ne peuvent être communiquées qu'en conformité avec le présent article.
>
> **Idem**
>
> **(2)** Le Service peut, en vue de l'exercice des fonctions qui lui sont conférées en vertu de la présente loi ou pour l'exécution ou le contrôle d'application de celle-ci, ou en conformité avec les exigences d'une autre règle de droit, communiquer les informations visées au paragraphe (1). Il peut aussi les communiquer aux autorités ou personnes suivantes :
>
> > **(a)** lorsqu'elles peuvent servir dans le cadre d'une enquête ou de poursuites relatives à une infraction présumée à une loi fédérale ou provinciale, aux agents de la paix compétents pour mener l'enquête, au procureur général du Canada et au procureur général de la province où des poursuites peuvent être intentées à l'égard de cette infraction;
> >
> > **(b)** lorsqu'elles concernent la conduite des affaires internationales du Canada, au ministre des Affaires étrangères ou à la personne qu'il désigne à cette fin;
> >
> > **(c)** lorsqu'elles concernent la défense du Canada, au ministre de la Défense nationale ou à la personne qu'il désigne à cette fin;
> >
> > **(d)** lorsque, selon le ministre, leur communication à un ministre ou à une personne appartenant à l'administration publique fédérale est essentielle pour des raisons d'intérêt public et que celles-ci justifient nettement une éventuelle violation de la vie privée, à ce ministre ou à cette personne.
>
> **Rapport à l'Office de surveillance**
>
> **(3)** Dans les plus brefs délais possible après la communication visée à l'alinéa (2)d), le directeur en fait rapport à l'Office de surveillance.

[99] Comme il ressort de ce qui précède, le paragraphe 19(2) habilite le SCRS à communiquer les renseignements qu'il obtient dans l'exercice de ses fonctions prévues à la loi à des fins précises : pour (i) l'exercice de ses fonctions prévues à la Loi sur le SCRS; (ii) l'administration et l'application de cette loi; (iii) en vertu d'une autre règle de droit ou (iv) dans les circonstances précisées aux alinéas 19(2)a) à d).

[100] Le PGC reconnaît que ces dispositions limitent la communication des données [***] recueillies sans mandat sous le régime de l'article 12. Tout particulièrement, il admet que le SCRS ne pourrait communiquer ces renseignements à des partenaires canadiens ou étrangers que si (i) leur évaluation révèle une menace ou (ii) qu'ils respectent les exigences strictes précisées au paragraphe 19(2).

[101] Quant aux prétentions du PGC, il semble que le risque de communication de données [***] non liées à des menaces à un partenaire étranger — ou à un partenaire canadien en dehors des circonstances limitées précisées à cette disposition — est très faible. Selon toute probabilité, une telle communication serait limitée aux situations où l'évaluation des renseignements révèle à tort une menace.

[102] En général, l'article 17 de la Loi sur le SCRS habilite le SCRS à collaborer avec des représentants du Canada ou d'États étrangers avec l'approbation du ministre. Cette disposition est ainsi libellée :

> **Coopération**
>
> **17 (1)** Dans l'exercice des fonctions qui lui sont conférées en vertu de la présente loi, le Service peut :
>
> > **a)** avec l'approbation du ministre, conclure des ententes ou, d'une façon générale, coopérer avec :
> >
> > > **(i)** les ministères du gouvernement du Canada, le gouvernement d'une province ou l'un de ses ministères,
> > >
> > > **(ii)** un service de police en place dans une province avec l'approbation du ministre provincial chargé des questions de police;
> >
> > **(b)** avec l'approbation du ministre, après consultation entre celui-ci et le ministre des Affaires étrangères, conclure des ententes ou, d'une façon générale, coopérer avec le gouvernement d'un État étranger ou l'une de ses institutions, ou une organisation internationale d'États ou l'une de ses institutions.
>
> **Transmission des ententes à l'Office de surveillance**
>
> **(2)** Un exemplaire du texte des ententes écrites conclues en vertu du paragraphe (1) ou des paragraphes 13(2) ou (3) est transmis à l'Office de surveillance immédiatement après leur conclusion.

[103] La Cour et la Cour d'appel fédérale ont reconnu à plusieurs reprises qu'il est dans l'intérêt public que le SCRS soit habilité à communiquer des renseignements à ses partenaires étrangers (voir p. ex. *Mahjoub (Re)*, 2013 CF 1096, aux paragraphes 57 à 58 et 63; *Canada (Procureur général) c. Almalki*, 2010 CF 1106, [2012] 2 R.C.F. 508, au paragraphe 131; *Canada (Procureur général) c. Charkaoui*, 2018 CF 849, aux paragraphes 151 et 155). La Cour d'appel souligne l'importance du principe « qu'il faut donner pour recevoir » *Mahjoub c. Canada (Citoyenneté et Immigration)*, 2017 CAF

157, [2018] 2 R.C.F. 344 (arrêt *Mahjoub*), au paragraphe 287. Ce principe est reconnu de manière implicite par la Cour suprême du Canada lorsqu'elle affirme que le Canada est un « importateur net » de renseignements relatifs à la sécurité nationale. Cette cour signale l'intérêt qu'a l'État à maintenir ses sources étrangères de renseignements (*Ruby c. Canada (Solliciteur général)*, 2002 CSC 75, [2002] 4 R.C.S. 3, aux paragraphes 43 à 44).

[104] Dans l'arrêt *Mahjoub*, au paragraphe 179, la Cour d'appel précise que : « [l]e régime d'échange de renseignements en vertu de [la Loi sur le SCRS] est assujetti à diverses mesures de protection et divers mécanismes de surveillance et ne donne pas lieu en principe […] à des fouilles abusives en violation de la Charte ».

[105] Précisons que la Cour, dans la décision *IMSI*, est d'avis que le SCRS peut intercepter des identifiants de communications mobiles sans mandat, et ce malgré la possibilité que ces renseignements soient communiqués à des organismes étrangers et malgré les répercussions possibles pour les intéressés (*IMSI*, aux paragraphes 146 et 168).

[106] Vu ce qui précède, j'estime qu'il ne serait pas judicieux d'entraver la capacité du SCRS à communiquer des données [***] à ses partenaires canadiens ou étrangers. Il est judicieux selon moi de rappeler que le PGC reconnaît que le SCRS ne serait habilité à communiquer de tels renseignements que si (i) leur évaluation révèle une menace ou (ii) ils respectent les critères stricts précisés au paragraphe 19(2). Dans ses observations orales, le représentant du PGC souligne que [TRADUCTION] « les renseignements non liés à des menaces ne peuvent jamais être communiqués à des organismes étrangers et, dans la plupart des cas, ne peuvent l'être à des organismes canadiens, sauf dans les quatre situations très précises énumérées aux alinéas 19(2)a) à d) » (voir la transcription de l'audience du 23 mars 2021, à la page 168).

[107] Passons à la condition relative aux données recueillies de manière incidente que propose l'*amicus* (non liées à des menaces). Cette condition obligerait le SCRS à supprimer les données [***] recueillies de manière incidente [TRADUCTION] « le plus rapidement possible et sans les téléverser dans les fonds de renseignements [du SCRS] ».

[108] Au soutien de sa proposition, l'*amicus* fait remarquer que l'auteur de l'affidavit 1 affirme dans son témoignage que la durée de conservation des données [***] recueillies au moyen de la technologie est fonction du temps mis par le SCRS à procéder à l'analyse. Règle générale, elle se mesure [TRADUCTION] « en jours ou en semaines ». Toutefois, selon l'auteur de l'affidavit 1, elle doit parfois être prolongée. En réponse à une question à ce sujet, il dit ceci [TRADUCTION] : « il pourrait être nécessaire dans certaines circonstances de conserver les données plus longtemps, pendant [***] » (transcription de l'audience du 23 mars 2021, à la page 248). En réponse à la question de savoir s'il envisage la possibilité d'une période de conservation s'étalant sur plus [***], il répond par l'affirmative, mais reconnaît qu'une telle situation serait exceptionnelle.

[109] Malgré ce qui précède, le PGC est d'avis que la condition proposée n'est pas nécessaire, et ce pour deux raisons.

[110] Premièrement, selon le PGC, les termes « dans la mesure strictement nécessaire » qui figurent à l'article 12 de la Loi sur le SCRS empêchent dans les faits le SCRS de conserver des renseignements non liés à des menaces, sauf en conformité avec les règles relatives aux ensembles de données du régime prévu aux articles 11.01 à 11.25 de cette loi. Aux termes de l'article 11.09, le SCRS doit présenter une demande d'autorisation judiciaire pour conserver un ensemble de données canadien, dans le délai de 90 jours suivant sa collecte.

[111] Deuxièmement, le PGC affirme que, suivant l'affidavit non contredit et la preuve testimoniale en l'espèce, seules les données [***] dont l'évaluation révèle une menace seront téléversées dans les fonds de renseignements du SCRS. Par conséquent, la condition proposée est redondante.

[112] À mon avis, les prétentions du PGC ne répondent pas complètement aux préoccupations soulevées par l'*amicus*. Comme il est mentionné plus haut, l'auteur de l'affidavit 1 n'était pas en mesure d'indiquer la date à laquelle les données [***] recueillies de manière incidente seraient supprimées. L'article 12 ne précise pas de délai dans ce cas non plus.

[113] Il importe de mentionner que les données en question sont des données [***] recueillies à l'égard des appareils de personnes dont on n'a aucun motif de soupçonner qu'elles présentent une menace envers la sécurité du Canada, au regard des usages proposés de la technologie au Canada.

[114] Dans l'affaire *IMSI*, la courte période de conservation importe dans la conclusion de la Cour selon laquelle le SCRS est habilité à intercepter les identifiants des appareils mobiles en question sans mandat (*IMSI*, aux paragraphes 252 à 254). À cet égard, j'estime le passage suivant particulièrement de circonstance [au paragraphe 254] :

> L'article 12 n'autorise pas la conservation d'IMSI ou d'IMEI de tiers au-delà d'un très court laps de temps ou leur analyse à des fins autres que la simple reconnaissance de l'appareil mobile d'une cible. À cette fin, un « très court laps de temps » se mesure en jours ou en semaines, bien que je demeure disposé à me laisser convaincre qu'il existe de bonnes raisons pour faire correspondre cette période avec le délai [***] qui s'applique à l'élimination des informations sur des tiers en d'autres contextes, dont la conservation de certains types de métadonnées (*X (Re)*, précité, au paragraphe 253). Je prévois que cette question fera l'objet d'autres échanges avec la procureure générale après la publication de la présente décision.

[115] Le PGC n'a pas soulevé de bonnes raisons pour justifier une démarche différente en l'espèce. Cependant, je reconnais qu'un ajustement s'impose étant donné la preuve présentée par l'auteur de l'affidavit 1, dont il est question au paragraphe 108 des présents motifs.

[116] En ce qui concerne cette preuve, j'estime qu'une période allant jusqu'à [***] ne serait pas déraisonnable. Néanmoins, à la lumière des observations présentées par le PGC dans une lettre datée du 24 juin 2022, la Cour comprend que les données [***] qui ne sont pas liées à des menaces sont en règle générale supprimées [TRADUCTION] « dans les jours ou semaines suivant la collecte ». Les données sont supprimées dès que le SCRS a procédé à l'évaluation des renseignements en question et déposé son rapport opérationnel, ou le dernier de tels rapports. Dans les cas très exceptionnels où

un délai de conservation [***] n'est pas suffisant, le SCRS peut en demander la prorogation à la Cour.

[117] En bref, je conviens avec l'*amicus* qu'il faut définir un délai de conservation des données [***] recueillies de manière incidente par le SCRS, comme ce concept est défini plus haut. Ce délai devrait être [***]. Dès lors que certains principes généraux sont suivis, la collecte incidente de données [***] relatives à des tiers non liés à des menaces ne serait pas effectuée de manière abusive. Ces principes sont les suivants : (i) les données [***] recueillies de manière incidente sont supprimées dès que le SCRS est en mesure [***] aux personnes faisant l'objet d'enquêtes; (ii) les données [***] recueillies de manière incidente sont supprimées avant toute utilisation et avant que le SCRS ne découvre l'identité des personnes à qui ces données correspondent; (iii) seuls les employés du SCRS qui sont autorisés à utiliser la technologie peuvent consulter les données [***] recueillies de manière incidente (à l'heure actuelle, il [***]); (iv) ces données [***] sont mise à l'écart pendant la période d'évaluation. Il est entendu que seules les données [***] dont l'évaluation révèle une menace seraient téléversées dans les fonds de renseignements du SCRS. Dans la situation vraisemblablement exceptionnelle où ce dernier souhaite conserver des données [***] recueillies de manière incidente dans un ensemble de données canadien, il doit attendre, pour faire usage de ces renseignements, d'obtenir l'autorisation de la Cour conformément à l'article 11.13 de la Loi sur le SCRS dans le délai de 90 jours, à défaut de quoi il doit supprimer les renseignements en application du paragraphe 11.09(3).

(v) Conclusion

[118] Pour les motifs énoncés aux rubriques IV.C. (3)(i) à (iv) des présents motifs, je suis d'avis que le premier usage proposé de la technologie au Canada ne serait pas effectué de manière abusive.

b) *Deuxième usage proposé de la technologie au Canada*

[119] À l'instar du premier des quatre usages proposés de la technologie, le deuxième usage viserait des personnes connues faisant l'objet d'enquêtes du SCRS [***] au Canada. Cependant, cet usage proposé a pour objet [***].

[120] Selon le PGC, il serait raisonnable pour le SCRS de soupçonner [***] et d'utiliser la technologie dans deux types de situations. La première est celle où [***]. Il fournit l'exemple [***]. Vu l'existence d'un lien avec d'une part l'objet d'une enquête et d'autre part une activité liée à des menaces, je suis d'accord pour dire qu'il existerait dans un tel cas des motifs raisonnables de soupçonner. De tels motifs appellent simplement « plus que de simples soupçons, mais ils ne correspondent pas à une croyance fondée sur des motifs raisonnables et probables » que l'intéressé participe *peut-être* à une activité liée à des menaces (*R. c. Kang-Brown*, 2008 CSC 18, [2008] 1 R.C.S. 456, au paragraphe 75 et *R. c. Chehil*, 2013 CSC 49, [2013] 3 R.C.S. 220, au paragraphe 26).

[121] Le second type de situation où il serait satisfait au critère, selon le PGC, concerne [***]. Dans ce genre de situations, le PGC estime qu'il serait raisonnable pour le SCRS de soupçonner [***]. Vu l'existence d'un lien avec d'une part l'objet d'une enquête et d'autre part un incident lié à des menaces, je suis d'accord pour dire qu'il serait satisfait au critère des motifs raisonnables de soupçonner dans un tel cas.

[122] À mon avis, il serait permis au SCRS d'interroger sans mandat ses bases de données pour vérifier si elles contiennent [***] recueillis dans ces deux types de situations. Contrairement à la situation que présenterait le premier usage proposé, pareil exercice ne constituerait pas une « recherche à l'aveuglette » (voir le paragraphe 93 des présents motifs). La seule raison qui justifie la collecte [***] que détient déjà le SCRS, notamment des renseignements obtenus de manière vraisemblablement légale [***]. Si le SCRS n'était pas habilité à procéder à de telles tâches, la collecte [***] en question ne servirait à rien [***].

[123] Il ressort de ce qui précède qu'à une exception près, le deuxième usage de la technologie ne serait pas plus envahissant que le premier, en ce qui a trait aux intérêts en matière de vie privée des personnes dont les données [***] sont recueillies.

[124] Il existe une seule exception à ce qui précède. Le SCRS serait en mesure de découvrir [***]. Cependant, comme c'était le cas dans l'affaire *IMSI*, [***] sont peu envahissants de par leur nature (*IMSI*, au paragraphes 144, 162 à 163, 172, 186 et 247). En effet, en utilisant la technologie de cette manière, le SCRS ne serait en mesure de tirer que des inférences minimales ou de découvrir des renseignements minimaux sur les habitudes et autres activités privées que protège l'article 8 de la Charte. En effet, l'identité des personnes à qui correspondent [***] ne serait pas connue, à moins que le SCRS leur ait déjà [***] versés dans ses fonds de renseignements.

[125] À l'instar du premier usage proposé de la technologie au Canada, le deuxième ne permettrait pas au SCRS de voir (i) la teneur de communications faites au moyen de l'appareil en question ou (ii) les renseignements stockés dans l'appareil ou accessibles par ce dernier.

[126] Pour les mêmes motifs que ceux énoncés au paragraphe 89 des présents motifs, j'estime que le SCRS aurait tout avantage à limiter la collecte de données [***] de tiers non liés à des menaces. À cet égard, selon le PGC, les mesures en vue d'atténuer le risque et de réduire la portée de la collecte incidente de telles données consisteraient notamment à [TRADUCTION] « [***] ». (Comme dans le cas du premier usage proposé de la technologie, le SCRS [***].)

[127] L'*amicus* est d'accord pour dire que le deuxième usage proposé de la technologie serait minimalement envahissant, à condition qu'il soit assujetti aux mêmes conditions qu'il a suggérées à l'égard du premier usage, à savoir (i) les données [***] recueillies ne sont pas communiquées aux organismes canadiens ou étrangers et (ii) les données recueillies de manière incidente sont supprimées dès que possible, sans être téléversées dans les fonds de renseignements du SCRS. Pour les motifs énoncés aux paragraphes 95 à 106 des présents motifs, je ne crois pas qu'il serait judicieux d'imposer la première condition. Quant à la seconde, je conviens, à une exception près, que cet usage de la technologie ne satisfait à l'article 8 de la Charte que si les données recueillies de manière incidente sont traitées suivant les principes énoncés aux paragraphes 116 à 117. Cette exception permet que les [***] employés du SCRS autorisés à utiliser la technologie consultent un collègue affecté aux opérations pour déterminer si [***] recueilli dans une telle situation est lié ou non à une menace. Elle s'applique également à la troisième situation décrite ci-après.

[128] Je reconnais que le deuxième usage de la technologie au Canada permettrait au SCRS [***]. Dans l'affaire *IMSI*, la Cour fait observer que le SCRS n'est pas autorisé à utiliser la technologie relative aux ESB pour « géolocaliser » quiconque sans mandat (*IMSI*, au paragraphe 5). Cependant, il faut interpréter cette remarque à la lumière de son contexte. Plus précisément, on a informé la Cour que la technologie relative aux ESB servait notamment à mener des « opérations de géolocalisation » (*IMSI*, aux paragraphes 31, 54, 56, 71 et 239). À cet égard, selon la preuve présentée à la Cour, [***] (*IMSI*, aux paragraphes 71 et 156). La Cour savait bien qu'il était possible que l'appareil, comme il était mobile, se déplace. On a aussi expliqué à la Cour [***] situations où le SCRS avait mené une telle opération. Dans ce cas, le SCRS avait obtenu un mandat. Il [***]. Ces situations constitueraient [***] et nécessiteraient des mandats, admet le PGC. La concession semblable faite par le PGC dans l'affaire *IMSI* doit être interprétée à la lumière de ce contexte (*IMSI*, au paragraphe 137). À mon avis, l'utilisation de la technologie en vue [***] ne constitue pas [***].

c) *Troisième usage proposé de la technologie au Canada*

[129] Le troisième usage proposé de la technologie concerne les types [***] au Canada dont il est question aux paragraphes 120 et 121 des présents motifs. La principale différence tiendrait à ce que le SCRS [***]. Le SCRS voudrait utiliser la technologie dans ce troisième type de situations pour [***].

[130] Quant à la collecte de données initiale, [***] permettrait qu'il soit satisfait au critère des motifs raisonnables de soupçonner prévu à l'article 12 de la Loi sur le SCRS. Quant à la conservation des données par le SCRS, l'existence de ces motifs serait démontrée s'il est confirmé que [***] se trouve déjà dans les bases de données du SCRS et a rapport [***].

[131] Selon le PGC, cet usage proposé de la technologie serait minimalement envahissant pour les mêmes raisons que celles énoncées à l'égard du second usage. Je suis d'accord, tant que les principes opérationnels et les mesures dont traitent les paragraphes 116 à 117 et 126 à 127 des présents motifs sont suivis et que le SCRS ne se contente pas [***].

[132] Selon l'*amicus*, cet usage proposé de la technologie porte une atteinte minimale aux droits que protège l'article 8 de la Charte seulement s'il est assujetti à trois conditions. Il n'est pas nécessaire de traiter des deux premières, car elles ont été suggérées à l'égard des deux premiers usages.

[133] Suivant la troisième condition suggérée par l'*amicus*, le troisième usage proposé de la technologie serait limité aux situations où le SCRS a des motifs raisonnables de soupçonner que [***] implique des activités qui se déroulent au Canada et visent à favoriser l'usage de la violence grave ou de menaces de violence contre des personnes ou des biens dans le but d'atteindre un objectif politique, religieux ou idéologique au Canada ou dans un État étranger. Le libellé de cette condition reprend celui du troisième des quatre types de menaces envers la sécurité du Canada, dont la définition figure à l'article 2 de la Loi sur le SCRS.

[134] Selon l'*amicus*, cette condition est nécessaire. À son avis, cet usage proposé de la technologie risque de mener à des excès [***], tout particulièrement étant donné la « fluidité » que le SCRS attribue au concept [***].

[135] À mon avis, il ne serait pas judicieux d'assortir de cette condition le troisième usage proposé. En résumé, aucune raison ne justifie qu'on limite l'usage proposé de la technologie à un seul des quatre types de menaces envers la sécurité du Canada décrits à l'article 2 de la Loi sur le SCRS. En outre, sur le plan pratique, pareille condition serait susceptible d'entraver la capacité du SCRS à évaluer les menaces (*Vu*, au paragraphe 57). [***] ne sont pas faciles à déterminer d'avance. Tout comme les policiers doivent pouvoir jouir « d'une certaine latitude » en ce qui concerne la manière dont ils procèdent aux fouilles et perquisitions (*R. c. Cornell*, 2010 CSC 31, [2010] 2 R.C.S. 142, aux paragraphes 22 à 24), il est judicieux de donner au SCRS une certaine marge lorsqu'il s'agit de décider s'il existe [***] et si l'utilisation de la technologie est susceptible de l'aider à identifier [***].

[136] Soulignons que j'arrive à cette conclusion à propos de cet usage proposé sans mandat en tenant pour acquis que le SCRS appliquera les principes opérationnels et les mesures dont traitent les paragraphes 116 à 117 et 126 à 127 des présents motifs et que, suivant les prétentions du PGC, le SCRS n'utilisera pas la technologie pour [***] quiconque sans mandat.

d) *Quatrième usage proposé de la technologie au Canada*

(i) Introduction

[137] Si les trois premiers usages proposés de la technologie auraient lieu au Canada, le quatrième usage proposé fait intervenir des activités d'enquête se déroulant également à l'étranger. En résumé, la technologie [***].[5]

[138] Pour ce faire, [***]. Le PGC souligne que la collecte [***] par le SCRS se limiterait à cette [***] question.

[139] À mon avis, cet usage de la technologie, [***] serait minimalement envahissant, à l'instar des deuxième et troisième usages dont il est question plus haut, pour essentiellement les mêmes motifs. Comme je l'indique plus haut, ces usages proposés de la technologie peuvent se révéler envahissants notamment s'ils permettent au SCRS de recueillir [***]. Certes, la collecte de tels renseignements est susceptible d'aider le SCRS à [***]. Or, ces renseignements à eux seuls sont minimalement envahissants, pour les motifs expliqués aux paragraphes 123 à 128 et 131. Comme les renseignements [***] obtenus au moyen du quatrième usage seraient [***] que ceux qui résulteraient des deuxième et troisième usages proposés, ils seraient encore moins envahissants que ces derniers.

[140] Il s'ensuit que le quatrième usage proposé de la technologie ne requiert pas l'obtention d'un mandat.

[141] Il est entendu que le PGC et le SCRS ont affirmé devant la Cour que, dès lors que le SCRS est en mesure [***], il serait contraint de solliciter un mandat avant d'utiliser la technologie à l'égard [***].

V. Évaluation des usages proposés de la technologie à l'extérieur du Canada (question 2)

[5] [***]

A. *Introduction*

[142] À l'extérieur du Canada, le SCRS propose de recourir à la technologie pour recueillir [***] les données [***] dans deux situations. Dans le premier cas, [***]. Ces activités d'enquête, qui sont plus que minimalement envahissantes, auraient lieu à l'extérieur du Canada.

[143] Dans la seconde situation, le SCRS [***]. Comme dans le premier cas, cette activité aurait lieu à l'extérieur du Canada.

[144] À mon avis, il serait satisfait au critère des motifs raisonnables de soupçonner que prévoit l'article 12 de la Loi sur le SCRS dans les deux situations décrites plus haut.

[145] Ainsi, il reste à décider si l'article 12 autorise la portée envahissante de ces usages proposés de la technologie à l'extérieur du Canada sans mandat. Pour les motifs qui suivent, j'estime que c'est le cas.

[146] Signalons que le PGC reconnaît le risque que la collecte de données [***] à l'extérieur du Canada dans les deux situations décrites plus haut permette de capter de manière incidente ou par inadvertance les données [***] d'un appareil appartenant à un citoyen canadien. Selon le PGC, dès lors que le SCRS s'aperçoit que de telles données ont été recueillies, ou celles d'une personne ayant un lien avec le Canada, il les isolerait. Le PGC présenterait alors à la Cour ses observations sur la légalité de la collecte incidente ou par inadvertance de telles données sans mandat. Je suis d'accord pour dire que l'isolement immédiat de ces renseignements suivi d'une présentation dans les plus brefs délais à la Cour constitueraient la manière de procéder dans ces situations, si elles se produisaient. Il est entendu qu'en tirant cette conclusion, je tiens pour acquis que le SCRS n'utilisera pas les renseignements mis en isolement avant d'avoir obtenu les directives de la Cour à cet égard.

B. *Analyse*

[147] Le PGC reconnaît que les activités d'enquête du SCRS sont assujetties à la Charte peu importe où elles ont lieu. À cet égard, il signale qu'aux termes du préambule de la Loi sur le SCRS, il importe que le SCRS « exerce ses fonctions dans le respect de la primauté du droit et de la [Charte] ». Néanmoins, le SCRS affirme que les ressortissants étrangers dépourvus de lien avec le Canada ne sont pas protégés par la Charte. Par conséquent, ils ne peuvent avoir d'attente raisonnable en matière de vie privée à l'égard des données [***] de leurs appareils, comme ce concept est interprété dans la jurisprudence portant sur la Charte.

[148] L'*amicus* reconnaît que les ressortissants étrangers dépourvus de lien avec le Canada ne bénéficient pas des droits que garantit l'article 8 de la Charte. Néanmoins, l'*amicus* affirme qu'ils ont tout de même une attente raisonnable en matière de vie privée à l'égard des données [***] de leurs appareils. Ainsi, le SCRS devrait obtenir un mandat pour utiliser la technologie à leur égard d'une manière qui est plus que minimalement envahissante.

[149] À mon avis, il n'est pas particulièrement utile, ni même nécessaire, de se demander si un ressortissant étranger dépourvu de lien avec le Canada a une attente raisonnable en matière de vie privée à l'égard des données [***] de son appareil.

[150] En effet, pour savoir si les usages que le SCRS propose de la technologie à l'égard de ces personnes sont autorisés, il faut répondre aux trois questions suivantes :

1. Les ressortissants étrangers dépourvus de lien avec le Canada sont-ils visés par le mot « chacun » qui figure à l'article 8 de la Charte?

2. L'article 12 autorise-t-il les activités d'enquête plus que minimalement envahissantes à l'extérieur du Canada visant des ressortissants étrangers qui ne sont pas protégés par la Charte?

3. Un principe de droit international empêche-t-il les usages plus que minimalement envahissants proposés par le SCRS de la technologie à l'extérieur du Canada à l'égard de ressortissants étrangers dépourvus de lien avec le Canada?

[151] Si on répond aux première et troisième questions par la négative et à la deuxième par l'affirmative, point n'est besoin d'aller plus loin. Pour les motifs qui suivent, j'estime qu'il s'agit des réponses adéquates. Par conséquent, le SCRS ne nécessite pas de mandat pour utiliser la technologie à l'extérieur du Canada dans les deux situations décrites plus haut, sous réserve de l'exception énoncée au paragraphe 146.

a) *L'article 8 de la Charte s'applique-t-il aux ressortissants étrangers dépourvus de lien avec le Canada?*

[152] L'article 8 de la Charte est ainsi libellé : « [c]hacun a droit à la protection contre les fouilles, les perquisitions ou les saisies abusives ».

[153] Selon le PGC, le mot « chacun » ne vise pas les ressortissants étrangers dépourvus de lien avec le Canada. Par conséquent, ces personnes ne peuvent opposer de droits garantis par la Charte à des actes de l'État canadien. Je suis d'accord.

[154] Le mot « chacun » doit être interprété de la même manière à l'article 8 qu'aux autres dispositions de la Charte (*R. c. Lloyd*, 2016 CSC 13, [2016] 1 R.C.S. 130, aux paragraphes 41 à 42).

[155] Donner au mot « chacun » une interprétation plus large à l'article 8 qu'à d'autres dispositions (p. ex., articles 2, 7, 9, 10 et 12) aurait pour effet d'élever les droits protégés par cette disposition au-dessus de ceux que protègent d'autres dispositions de la Charte. Il faut se garder d'adopter une conception hiérarchique des droits garantis par la Charte (*Dagenais c. Société Radio-Canada*, [1994] 3 R.C.S. 835, à la page 877).

[156] Dans l'affaire *Slahi c. Canada (Justice)*, 2009 CF 160, [2009] 3 R.C.F. F-6 (*Slahi*), aux paragraphes 40 à 48, le juge Blanchard conclut, sur le fondement d'enseignements de la Cour suprême du Canada, que les demandeurs étrangers ne peuvent faire valoir les droits protégés par l'article 7 de la Charte, car ils n'ont pas démontré l'existence d'un lien reconnu avec le Canada. Leur interrogatoire à Guantanamo Bay par des représentants canadiens ne suffit pas à créer de tels droits.

[157] La conclusion du juge Blanchard est fondée sur la jurisprudence de la Cour suprême remontant à l'arrêt *Singh c. Ministre de l'Emploi et de l'Immigration*, [1985] 1

R.S.C. 177 (*Singh*), dans lequel elle est saisie de la question de savoir si les demandeurs d'asile qui se trouvent au Canada peuvent bénéficier des protections offertes par l'article 7 de la Charte. Dans sa réponse affirmative, la juge Wilson, aux noms des juges majoritaires, indique : « […] je suis disposée à accepter que ce mot [chacun] englobe tout être humain qui se trouve au Canada et qui, de ce fait, est assujetti à la loi canadienne » (*Singh*, à la page 202).

[158] Le juge Blanchard, après cette citation de l'arrêt *Singh*, cite un passage des motifs dissidents rédigés par la juge L'Heureux-Dubé dans l'affaire *R. c. Cook*, [1998] 2 R.C.S. 597 (*Cook*) [au paragraphe 86, cité dans *Slahi*, au paragraphe 43] :

> […] L'appelant invoque les droits prévus à l'al. 10*b*), qui étend sa protection à « chacun ». Le terme « chacun » semble avoir un sens assez large. Cependant, son interprétation doit se faire à la lumière des objectifs de la *Charte*. Je ne suis pas convaincue que l'adoption de la *Charte* ait nécessairement conféré des droits à tous les citoyens du monde, de toutes les nationalités, peut [*sic*] importe où ils se trouvent, malgré l'utilisation par le législateur du mot « chacun » pour en désigner les titulaires. Je crois plutôt que l'on peut soutenir que le mot « chacun » a été utilisé pour distinguer les droits accordés à chacun sur le territoire du Canada d'avec ceux qui sont accordés seulement aux citoyens canadiens et ceux qui sont conférés aux inculpés.

[159] Signalons que les juges majoritaires dans l'arrêt *Cook* ne sont pas convaincus par un raisonnement semblable avancé par le PGC, intervenant dans l'instance. Toutefois, en concluant que l'alinéa 10b) de la Charte s'applique aux détectives canadiens qui ont interrogé l'appelant, un citoyen américain, aux États-Unis, ils soulignent les faits de l'affaire. En effet, l'appelant faisait l'objet d'une enquête sur un meurtre commis au Canada, et son procès se déroulerait au Canada. Dans ce contexte, les juges majoritaires font observer que l'appelant « était en voie d'être livré à la justice canadienne » (*Cook*, au paragraphe 53). Cette observation semble avoir fondé leur conclusion selon laquelle il aurait dû être informé de son droit à un avocat prévu à l'alinéa 10b) de la *Charte*. Ils précisent que la « situation diffère considérablement de la myriade de cas où des personnes à l'étranger se réclament des garanties de la *Charte simpliciter* » (*Cook*, au paragraphe 53).

[160] Par la suite, dans l'arrêt *R. c. Hape*, 2007 CSC 26, [2007] 2 R.C.S. 292 (*Hape*), aux paragraphes 83 à 93, la Cour suprême arrive à la conclusion que la démarche des juges majoritaires dans l'arrêt *Cook* met l'accent au mauvais endroit, ce qui cause divers problèmes. Par exemple, des difficultés pratiques et théoriques découlent de « son application à d'autres situations (*p. ex. les fouilles, les perquisitions et les saisies*) » (*Hape*, au paragraphe 83 (non souligné dans l'original)). Pour les besoins de la cause, je conviens avec le PGC qu'il n'est pas nécessaire de pousser l'analyse énoncée dans l'arrêt *Hape*. Cette affaire portait sur l'application de la Charte à la fouille, perquisition et saisie visant la société d'investissement d'un hommes d'affaires canadien ayant pignon sur rue dans les îles Turques et Caïques par des policiers canadiens qui relevaient du chef de la police locale. En l'espèce, il suffit de signaler que la décision des juges majoritaires dans l'affaire *Hape* a infirmé la décision des juges majoritaires dans l'arrêt *Cook*. Ce faisant, ils mentionnent les motifs dissidents qu'y exprime la juge L'Heureux-Dubé (*Hape*, au paragraphe 81), sans faire d'autres remarques sur cette opinion, sauf pour préciser que la juge McLachlin (plus tard juge en chef) y souscrit.

[161] Revenons à la décision *Slahi*. Après avoir cité l'avis dissident de la juge L'Heureux-Dubé dans l'arrêt *Cook*, le juge Blanchard renvoie sommairement à deux autres arrêts de la Cour suprême. Dans le premier, *Canada (Justice) c. Khadr*, 2008 CSC 28, [2008] 2 R.C.S. 125, cette cour affirme au paragraphe 31 : « [l]'article 7 contraint […] le Canada à cette communication à cause de sa participation à une procédure étrangère qui est contraire au droit international et qui compromet la liberté d'un Canadien » [souligné par la Cour dans la décision *Slahi*, paragraphe 45]. Dans le second, *R. c. Harrer*, [1995] 3 R.C.S. 562, au paragraphe 11, le juge LaForest fait l'observation suivante au nom des juges majoritaires :

> Sous réserve de tout argument affirmant le contraire, il me semble que le fait d'écarter automatiquement l'application de la *Charte* à l'extérieur du Canada pourrait avoir pour effet de restreindre indûment la protection à laquelle les Canadiens sont en droit de s'attendre en ce qui concerne la violation de leurs droits par nos gouvernements ou leurs mandataires. [Souligné par la Cour dans la décision *Slahi*, paragraphe 46.]

[162] Eu égard à cette jurisprudence, la Cour dans l'affaire *Slahi* conclut ainsi [aux paragraphes 47 à 48] :

> En résumé, la jurisprudence de la Cour suprême enseigne que des non-Canadiens peuvent se prévaloir des protections prévues à l'article 7 de la Charte lorsqu'ils se trouvent au Canada ou lorsqu'ils font l'objet d'un procès criminel au Canada, et que des citoyens canadiens, dans certaines circonstances, peuvent faire valoir les droits qui leur sont conférés par l'article 7 de la Charte lorsqu'ils se trouvent à l'extérieur du Canada […]
>
> Les demandeurs en l'espèce n'ont pas réussi à établir un lien avec le Canada qui déclencherait les droits prévus à l'article 7 de la Charte au regard des entrevues de Guantanamo Bay. Il faut se rappeler que la Charte, laquelle fait partie intégra[nte] de la loi suprême du Canada, est un document canadien qui a été édicté afin de consacrer et de protéger les droits fondamentaux des Canadiens et des personnes qui se trouvent sur le territoire du Canada. Ce n'est que dans des cas exceptionnels et bien précis qu'elle a une application extraterritoriale, comme il est exigé par le respect des principes de la souveraineté et de la courtoisie judiciaire. La Cour n'est pas disposée à étendre l'application de la Charte au-delà de ce qui a déjà été décidé. Les demandeurs ne sont pas des citoyens canadiens. Ils n'ont pas réussi à établir le lien exigé avec le Canada. Par conséquent, leur situation ne peut pas déclencher l'application d'un droit garanti par l'article 7 de la Charte. [Non souligné dans l'original.]

[163] La conclusion du juge Blanchard est confirmée par la Cour d'appel fédérale (*Slahi c. Canada (Justice)*, 2009 CAF 259), en ces termes [au paragraphe 4] :

> L'unique question à trancher dans les présents appels est celle de savoir si le juge de première instance a commis une erreur en concluant que les appelants ne peuvent se prévaloir de l'article 7 pendant leur détention à la base de Guantanamo par les autorités américaines parce qu'ils ne sont pas des citoyens canadiens. Pour essentiellement les mêmes motifs que le juge de première instance, nous estimons que la conclusion à laquelle il est parvenu est correcte. Une distinction peut être faite d'avec l'arrêt *Khadr* puisque M. Khadr avait la citoyenneté canadienne, ce qui n'est pas le cas des appelants. En outre, ceux-ci ne sont visés au Canada par aucune procédure susceptible de créer un lien entre eux et ce pays.

[164] L'autorisation de pourvoi à la Cour suprême a été refusée (*Slahi c Canada (Justice)*, 2009 CAF 259, autorisation de pourvoi refusée, n^{o} 33409 (18 février 2010)).

[165] Le juge Rennie (plus tard juge à la Cour d'appel fédérale) souscrit au raisonnement du juge Blanchard dans des remarques incidentes qu'il exprime dans la décision *Tabingo c. Canada (Citoyenneté et Immigration)*, 2013 CF 377, [2014] 4 R.C.F. 150 (*Tabingo*). Dans cette affaire de contrôle judiciaire, les demandeurs étrangers faisaient valoir l'atteinte aux droits prévus aux articles 7 et 15 de la Charte. Comme l'intimé n'a pas contesté la qualité pour agir des demandeurs ni l'application de la Charte dans ce cas, le juge Rennie s'abstient de trancher expressément la question de savoir si les demandeurs peuvent faire valoir la Charte. Toutefois, il émet des réserves quant à la justesse de la concession faite par l'intimé (*Tabingo*, au paragraphe 79) en ces termes [au paragraphe 65] :

> Une jurisprudence de la Cour suprême du Canada et la Cour d'appel fédérale donne des indications claires quant aux situations dans lesquelles la Charte s'applique aux actes de responsables canadiens à l'étranger. […] La jurisprudence majoritaire indique que les non-citoyens à l'extérieur du Canada ne peuvent pas se réclamer de la protection de la Charte, si ce n'est dans des circonstances exceptionnelles reliées aux actes de responsables ou de mandataires canadiens à l'étranger.

[166] Le juge Rennie renvoie ainsi à la jurisprudence analysée par le juge Blanchard dans l'affaire *Slahi* ainsi qu'à la décision de la Cour dans l'affaire *Amnesty International Canada c. Canada (Procureur général)*, 2008 CF 336, *sub nom. Amnistie internationale Canada c. Canada (Chef d'État-major de la défense)*, [2008] 4 R.C.F. 546 (*Amnestie internationale*) (conf. par 2008 CAF 401, [2009] 4 R.C.F. 149, au paragraphe 36). Cette dernière portait sur le sort de personnes détenues par les Forces armées canadiennes en Afghanistan pendant un conflit armé. La juge Mactavish (plus tard juge à la Cour d'appel fédérale) conclut que les détenus sont protégés par le droit humanitaire international, mais ne bénéficient pas des droits prévus par les articles 7, 10 et 12 de la Charte. Sa conclusion est fondée sur le fait que le gouvernement de l'Afghanistan n'a pas consenti à l'application des lois canadiennes, dont la Charte, sur son territoire et à ses citoyens (*Amnestie internationale*, aux paragraphes 171 à 172).

[167] Le juge Rennie fait aussi observer dans la décision *Tabingo* que cette jurisprudence est conforme à celle de la Cour d'appel fédérale et de la Cour fédérale. Il affirme ce qui suit [aux paragraphes 75 à 76] :

> D'autres jugements récents de la Cour ont statué que la Charte ne conférait généralement pas de droits aux non-citoyens à l'extérieur du Canada : Zeng c. Canada (Procureur général), 2013 CF 104, aux paragraphes 70 à 72; Kinsel c. Canada (Ministre de la Citoyenneté et de l'Immigration), 2012 CF 1515, [2014] 2 R.C.F. 421, aux paragraphes 45 à 47; Toronto Coalition to Stop the War c. Canada (Sécurité publique et Protection civile), 2010 CF 957, [2012] 1 R.C.F. 413, aux paragraphes 81 et 82. Dans ces trois décisions, la Cour a souscrit à la conclusion du juge Blanchard lorsque celui-ci statuait que seul peut invoquer la Charte un individu qui est présent au Canada, qui est assujetti à des procédures criminelles au Canada ou qui possède la citoyenneté canadienne.
>
> Cette restriction à l'application de la Charte n'est pas un développement récent. Même avant la décision Slahi, la Cour fédérale et la Cour d'appel fédérale avaient interprété l'arrêt Singh comme empêchant que les non-citoyens à l'extérieur du Canada puissent invoquer la Charte : Conseil canadien des Églises c. Canada, [1990] 2 C.F. 534 (C.A.) (conf. pour d'autres motifs [1992] 1 R.C.S. 236); Ruparel c. Canada (Ministre de l'Emploi et de l'Immigration), [1990] 3 C.F. 615 (1re inst.); Lee c. Canada (Ministre de la Citoyenneté et de l'Immigration), 1997] CanLII 4837 (C.F. 1re inst.); Deol c. Canada (Ministre de la Citoyenneté et de l'Immigration), 2001 CFPI 694 (conf. pour d'autres motifs 2002 CAF 271, [2003] 1 C.F. 301). [Non souligné dans l'original.]

[168] Au bout du compte, le juge Rennie rejette sur le fond les arguments des demandeurs fondés sur la Charte. Son raisonnement et ses conclusions sont confirmés par la suite par la Cour d'appel fédérale (*Austria c. Canada (Citoyenneté et Immigration)*, 2014 CAF 191, *sub nom. Tabingo c. Canada (Citoyenneté et Immigration)*, [2015] 3 R.C.F. 346, au paragraphe 96, autorisation de pourvoi refusée, nº 36213 (30 avril 2015)).

[169] La juge Gleason (plus tard juge à la Cour d'appel fédérale) partage dans la décision *Jia c. Canada (Citoyenneté et Immigration)*, 2014 CF 596, [2015] 3 R.C.F. 143, aux paragraphes 108 à 110, les réserves émises par le juge Rennie sur l'application de la Charte aux demandeurs étrangers. À l'instar de son collègue, la juge Gleason s'abstient de se prononcer sur cette question, car elle est en mesure de rejeter au fond les arguments des demandeurs fondés sur les articles 7 et 15 de la Charte.

[170] En résumé, à la lumière de la jurisprudence analysée plus haut (y compris les décisions mentionnées dans les citations tirées de la décision *Tabingo*), je suis d'accord avec le PGC pour dire que les ressortissants étrangers qui n'ont pas l'un des trois liens reconnus avec le Canada, dont la description suit, ne sont pas visés par le mot « chacun » qui figure à l'article 8 de la Charte. Autrement dit, l'interprétation du mot « chacun » qui figure aux articles 2, 7 et 12 et à l'alinéa 10b) et celle du mot « tous » qui figure à l'article 15 de la Charte s'appliquent également à l'article 8. Par conséquent, les ressortissants étrangers dépourvus de lien reconnu avec le Canada ne peuvent invoquer les droits prévus à l'article 8 de la Charte. La réponse à la première question énoncée au paragraphe 150 des présents motifs est non.

[171] Comme il est indiqué dans la décision *Tabingo*, au paragraphe 75, les trois liens reconnus sont les suivants : (i) citoyenneté canadienne, (ii) présence au Canada et (iii) faire l'objet de poursuites pénales au Canada.

[172] Il est entendu que le PGC reconnaît que [***] un lien nécessaire avec le Canada dès lors que le SCRS est en mesure de confirmer que [***]. Dans de telles circonstances, le PGC et le SCRS ont expressément affirmé devant la Cour que le SCRS serait contraint de solliciter un mandat avant d'utiliser à nouveau la technologie à l'égard de cette personne.

b) *L'article 12 autorise-t-il les activités d'enquête à l'extérieur du Canada qui sont plus que minimalement envahissantes si elles visent des ressortissants étrangers qui ne peuvent invoquer les droits garantis par la Charte?*

[173] Ma conclusion quant à la portée des protections prévues par l'article 8 de la Charte ne suffit pas pour me permettre de décider si les usages proposés par le SCRS de la technologie à l'extérieur du Canada sont autorisés sans mandat. Pour répondre à cette question, il faut décider si de telles activités sont autorisées par la loi.

[174] En l'occurrence, la loi pertinente est l'article 12 de la Loi sur le SCRS. La Cour doit donc trancher la question de savoir si cette disposition autorise le SCRS à mener des activités plus que minimalement envahissantes à l'extérieur du Canada, à l'égard de ressortissants étrangers dépourvus de lien avec le Canada.

[175] Le paragraphe 12(2) habilite expressément le SCRS à « exercer les fonctions que le paragraphe (1) lui confère même à l'extérieur du Canada ».

[176] Selon la jurisprudence constante de la Cour, l'article 12 autorise seulement le SCRS à mener sans mandat des activités qui sont minimalement envahissantes. Or, cette jurisprudence intéresse des personnes faisant l'objet d'enquêtes pouvant faire valoir les droits que confère l'article 8 de la Charte.

[177] Dans les cas où les enquêtes du SCRS portent sur des personnes qui ne peuvent faire valoir ces droits, cette restriction des pouvoirs conférés par l'article 12 tombe. Cette conclusion va dans le même sens que l'observation suivante qui figure dans l'arrêt *X (Re)*, 2014 CAF 249, [2015] 1 R.C.F. 684 (arrêt *X (Re)*), au paragraphe 82 :

> […] l'article 12 n'accorde pas au SCRS une dispense de l'application des lois d'application générale. Il s'ensuit que, lorsque les méthodes d'enquête comportent intrusion et que ces méthodes constitueraient autrement un acte criminel ou une violation du droit à la protection contre les fouilles et les saisies [abusives] garanti par la Charte, le Service peut demander à la Cour fédérale qu'elle décerne un mandat en vertu de l'article 21 de la Loi sur le SCRS. [Non souligné dans l'original.]

[178] Certes, « une autorisation préalable, qui prend habituellement la forme d'un mandat valide, a toujours été la condition préalable d'une fouille, d'une perquisition et d'une saisie valides sous le régime de la common law et de la plupart des lois » (*Hunter*, à la page 160). Toutefois, l'article 12 l'emporte sur la *common law*, car il habilite expressément le SCRS à recueillir, dans la mesure strictement nécessaire, et à analyser et conserver les renseignements sur les activités dont on a des motifs raisonnables de soupçonner qu'elles constituent des menaces envers la sécurité du Canada.

[179] L'historique législatif de l'article 12 confirme cette interprétation de la portée des pouvoirs dont dispose le SCRS à l'égard des ressortissants étrangers dépourvus de lien avec le Canada. En effet, quand le Comité permanent de la sécurité publique et nationale a été saisi du projet de loi C-44, la députée et chef du parti Vert, Elizabeth May, a proposé les amendements suivants à la mesure législative, avec le soutien du Nouveau Parti démocratique, alors l'opposition officielle :

> [Le témoin] nous a proposé d'insérer un article distinct à la suite du paragraphe 21(3.1). Comme vous pouvez le constater, cela ferait partie de l'article 8 :
>
> (3.2) Il est entendu qu'un mandat décerné en vertu du présent article est requis pour toute enquête à l'extérieur du Canada :
>
> a) soit dans le cadre de laquelle est exercée une activité qui, si elle était exercée au Canada, nécessiterait un mandat en raison de la Charte canadienne des droits et libertés;
>
> […]
>
> L'amendement dissipe les ambiguïtés. Il garantit que les activités que nous menons à l'étranger respectent la Charte des droits et libertés.

[180] L'amendement n'a pas été adopté (Chambre des communes. Comité permanent de la sécurité publique et nationale. *Témoignages*, 41e lég., 2e sess., fascicule no 42 (1er décembre 2014), à la page 12)). Il ressort de ce fait que le législateur n'entendait pas

exiger l'obtention d'un mandat par le SCRS quand il mène des activités à l'extérieur du Canada qui nécessiteraient un mandat au Canada pour l'application de l'article 8 de la Charte (*Société Télé-Mobile c. Ontario*, 2008 CSC 12, [2008] 1 R.C.S. 305, au paragraphe 42; *Canada (Commissaire à l'information) c. Canada (Ministre de la Défense nationale)*, 2011 CSC 25, [2011] 2 R.C.S. 306, au paragraphe 27 et *Renvoi relatif à la Politique réglementaire de radiodiffusion CRTC 2010-167 et l'ordonnance de radiodiffusion CRTC 2010-168*, 2012 CSC 68, [2012] 3 R.C.S. 489, au paragraphe 73).

[181] Fait intéressant, lorsque le Comité permanent du Sénat sur la sécurité nationale et la défense a examiné à son tour le projet de loi C-44, la sénatrice Olsen a posé une question au directeur du SCRS à l'époque, M. Michel Coulombe, sur les activités menées à l'extérieur du Canada qui nécessiteraient l'obtention d'un mandat. Le directeur a répondu en ces termes : « Pour le moment, que les activités touchent le Canada ou l'étranger, les catégories d'activités nécessitant un mandat seraient les mêmes. Lorsqu'une démarche enfreint l'article 8 de la Charte, il faut obtenir un mandat » (Sénat. Comité permanent du Sénat sur la sécurité nationale et la défense, 41e lég., 2e sess., fascicule no 14 (9 mars 2015), à la page 115).

[182] En résumé, comme le SCRS n'est pas contraint d'obtenir une autorisation judiciaire préalable, en application de la Charte ou d'une autre règle de droit, pour utiliser la technologie aux fins envahissantes décrites aux paragraphes 142 et 143 des présents motifs, j'estime que de telles activités ne nécessitent pas l'obtention d'un mandat. Autrement dit, le SCRS n'est pas tenu d'obtenir un mandat à l'égard des usages proposés de la technologie à l'extérieur du Canada. Cette interprétation des pouvoirs que confère au SCRS l'article 12 de la Loi sur le SCRS est confirmée par l'historique législatif dont il est question plus haut.

[183] Par conséquent, la réponse à la deuxième question énoncée au paragraphe 150 est oui.

c) *Un principe de droit international empêche-t-il les usages plus que minimalement envahissants proposés par le SCRS de la technologie à l'extérieur du Canada à l'égard de ressortissants étrangers dépourvus de lien avec le Canada?*

[184] Selon l'*amicus*, cette interprétation de l'article 12 revient à donner au SCRS [TRADUCTION] « carte blanche en matière de fouille et de perquisition à l'égard de ressortissants étrangers ». Je ne suis pas d'accord.

[185] Il n'a présenté aucun argument à la Cour au soutien de sa thèse selon laquelle les usages sans mandat de la technologie proposés par le SCRS dans la présente instance seraient contraires au droit international ou à son esprit.

[186] Sur le fondement des sources suivantes, l'*amicus* reconnaît que l'espionnage en soi ne contrevient pas au droit international (Michael N. Schmitt, éd., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge : Cambridge University Press, 2017), à la page 169; Craig Forcese, « Pragmatism and Principle : Intelligence Agencies and International Law » (2016), 102 Va. L. Rev. 67, Ottawa Faculty of Law Working Paper No. 2016-29, aux pages 71 à 72). Je suis d'accord. La légalité en droit international de telles activités doit être déterminée à la lumière des faits de l'espèce.

[187] Au vu des faits de l'affaire, et à défaut de preuve contraire, je suis d'avis qu'aucun principe de droit international n'interdit les usages plus que minimalement envahissants de la technologie proposés par le SCRS sans mandat à l'égard de ressortissants étrangers dépourvus de lien avec le Canada à l'extérieur du Canada. Contrairement à ce qu'affirme l'*amicus*, cette interprétation ne revient pas à donner au SCRS « carte blanche en matière de fouille et de perquisition à l'égard de ressortissants étrangers ». Entre autres, le SCRS serait toujours assujetti aux balises énoncées à l'article 12, dont les critères des « motifs raisonnables de soupçonner » et de « la mesure strictement nécessaire ». En outre, la Loi sur le SCRS prévoit des mesures de surveillance des activités du SCRS sous le régime de l'article 12 (voir généralement *IMSI*, aux paragraphes 230 à 235).

[188] Qui plus est, comme le reconnaît le PGC, le SCRS n'est pas autorisé à recueillir des renseignements à l'extérieur du Canada d'une manière qui contreviendrait aux obligations juridiques qui lui sont imposées par la *Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères*, L.C. 2019, ch. 13, **art.** 49.1 et les *Instructions visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères (Directeur du Service canadien du renseignement de sécurité)*, 2019-1302 (Instructions).

[189] De manière générale, tout renseignement recueilli par le SCRS à l'extérieur du Canada devant servir dans des poursuites pénales est assujetti aux règles d'admissibilité de la preuve prévues à la Charte.

[190] Je conviens également avec l'*amicus* pour dire que, pour les besoins de la cause, l'article 12 de la Loi sur le SCRS est présumé conforme au droit international (*Canada (Ministre de la Citoyenneté et de l'Immigration) c. Vavilov*, 2019 CSC 65, [2019] 4 R.C.S. 653, aux paragraphes 114 et 182). En effet, cette disposition est dépourvue des termes qui figurent au paragraphe 21(3) et à l'article 24 (« par dérogation à toute autre règle de droit ») et aux paragraphes 21(3.1) et 21.1(4) (« sans égard à toute autre règle de droit »).

[191] Enfin, l'*amicus* et le PGC s'entendent pour dire que le principe de la conformité au droit international empêcherait toute interprétation de l'article 12 autorisant la torture ou d'autres infractions au droit humanitaire international. En outre, signalons que l'*amicus* ne souhaitait pas faire de conjectures sur les restrictions possibles imposées par le droit international aux pouvoirs conférés par l'article 12 de la Loi sur le SCRS.

[192] En résumé, pour les besoins de la cause, à défaut de tout élément de preuve ou d'argument convaincant démontrant le contraire, j'estime que les usages proposés par le SCRS de la technologie à l'extérieur du Canada ne contreviendraient pas aux principes de droit international. Par conséquent, la réponse à la troisième question énoncée au paragraphe 150 est non.

[193] Signalons que je suis rassuré par le fait que la Cour d'appel fédérale rejette la thèse suivant laquelle « les activités d'enquête comportant intrusion menées à l'étranger contreviendraient nécessairement au droit international ou au principe de courtoisie entre nations » (arrêt *X (Re)*, au paragraphe 80). La Cour d'appel conclut que le SCRS doit obtenir un mandat chaque fois qu'il opte pour des méthodes d'enquêtes envahissantes, mais ajoute comme précision importante que cette obligation s'applique aux méthodes qui « constitueraient autrement un acte criminel ou une violation du droit

à la protection contre les fouilles et les saisies [abusives] garanti par la Charte » (aux paragraphes 81 à 82). J'ajoute simplement que les objets des enquêtes dans cette affaire étaient des citoyens canadiens et non, comme en l'espèce, des ressortissants étrangers dépourvus de lien avec le Canada (voir l'arrêt *X (Re)*, aux paragraphes 9 et 11).

VI. Conclusion

[194] Pour les motifs énoncés aux rubriques IV.C. 3 (a) à (d), je conclus que les quatre usages proposés par le SCRS de la technologie au Canada ne nécessitent pas l'obtention d'un mandat.

[195] Il faut souligner que j'arrive à cette conclusion — quant à la légalité des usages proposés de la technologie sans mandat — en tenant pour acquis que les principes opérationnels et les mesures dont traitent les paragraphes 62, 88, 116 à 117, 126 à 127 et 141 des présents motifs sont suivis. Ma conclusion tient également compte des affirmations du PGC selon lesquelles seules les données [***] dont l'évaluation révèle une menace seraient téléversées dans les fonds de renseignements du SCRS et que ce dernier n'utilisera pas la technologie [***] a un lien reconnu avec le Canada sans mandat.

[196] Pour les motifs énoncés à la partie V des présents motifs, je suis d'avis que les usages proposés par le SCRS de la technologie à l'extérieur du Canada à l'égard de ressortissants étrangers dépourvus de lien avec le Canada ne nécessiteraient pas l'obtention de mandats.

JUGEMENT dans le dossier SCRS-1-21

LA COUR ORDONNE QUE :

1. La technologie peut être utilisée au Canada aux quatre fins précises proposées par le SCRS, sans mandat, à condition que ces usages soient conformes aux motifs énoncés plus haut, tout particulièrement les paragraphes 62, 88, 116 à 117, 126 à 127 et 141.

2. La technologie peut être utilisée à l'extérieur du Canada à l'égard de ressortissants étrangers dépourvus de lien avec le Canada, sans mandat, dans les deux situations décrites aux paragraphes 142 et 143 des motifs énoncés plus haut.

Annexe confidentielle I — la technologie

L'Annexe I, auquel il est référé au paragraphe 7 de ce Jugement et Motifs, comprend 16 pages et est entièrement caviardée.

Annexe II — Législation applicable

Loi sur le Service canadien du renseignement de sécurité, L.R.C. (1985), ch. C-23

Informations et renseignements

12 (1) Le Service recueille, au moyen d'enquêtes ou autrement, dans la mesure strictement nécessaire, et analyse et conserve les informations et renseignements sur les activités dont il existe des motifs raisonnables de soupçonner qu'elles constituent des menaces envers la sécurité du Canada; il en fait rapport au gouvernement du Canada et le conseille à cet égard.

Aucune limite territoriale

(2) Il est entendu que le Service peut exercer les fonctions que le paragraphe (1) lui confère même à l'extérieur du Canada. L.R. (1985), ch. C-23, art. 12; 2015, ch. 9, art. 3.

Mesures pour réduire les menaces envers la sécurité du Canada

12.1 (1) S'il existe des motifs raisonnables de croire qu'une activité donnée constitue une menace envers la sécurité du Canada, le Service peut prendre des mesures, même à l'extérieur du Canada, pour réduire la menace.

Limites

(2) Les mesures doivent être justes et adaptées aux circonstances, compte tenu de la nature de la menace et des mesures, des solutions de rechange acceptables pour réduire la menace et des conséquences raisonnablement prévisibles sur les tierces parties, notamment sur leur droit à la vie privée.

Autres options

(3) Avant de prendre des mesures en vertu du paragraphe (1), le Service consulte, au besoin, d'autres ministères ou organismes fédéraux afin d'établir s'ils sont en mesure de réduire la menace.

Charte canadienne des droits et libertés

(3.1) La *Charte canadienne des droits et libertés* fait partie de la loi suprême du Canada et toutes les mesures prises par le Service en vertu du paragraphe (1) s'y conforment.

Mandat — *Charte canadienne des droits et libertés*

(3.2) Le Service ne peut, en vertu du paragraphe (1), prendre des mesures qui limiteraient un droit ou une liberté garanti par la *Charte canadienne des droits et libertés* que si, sur demande présentée au titre de l'article 21.1, un juge décerne un mandat autorisant la prise de ces mesures.

Condition

(3.3) Le juge ne peut décerner le mandat visé au paragraphe (3.2) que s'il est convaincu que les mesures, telles qu'autorisées par le mandat, sont conformes à la *Charte canadienne des droits et libertés*.

Mandat — droit canadien

(3.4) Le Service ne peut, en vertu du paragraphe (1), prendre des mesures qui seraient par ailleurs contraires au droit canadien que si ces mesures ont été autorisées par un mandat décerné au titre de l'article 21.1.

Avis à l'Office de surveillance

(3.5) Dans les plus brefs délais possible après la prise de mesures en vertu du paragraphe (1), le Service avise l'Office de surveillance de ces mesures.

Précision

(4) Il est entendu que le paragraphe (1) ne confère au Service aucun pouvoir de contrôle d'application de la loi. 2015, ch. 20, art. 42; 2019, ch. 13, art. 23; 2019, ch. 13, art. 98.

Interdictions

12.2 (1) Dans le cadre des mesures qu'il prend pour réduire une menace envers la sécurité du Canada, le Service ne peut :

a) causer, volontairement ou par négligence criminelle, des lésions corporelles à un individu ou la mort de celui-ci;

b) tenter volontairement de quelque manière d'entraver, de détourner ou de contrecarrer le cours de la justice;

c) porter atteinte à l'intégrité sexuelle d'un individu;

d) soumettre un individu à la torture ou à d'autres peines ou traitements cruels, inhumains ou dégradants, au sens de la Convention contre la torture;

e) détenir un individu;

f) causer la perte de biens ou des dommages importants à ceux-ci si cela porterait atteinte à la sécurité d'un individu.

(2) [Abrogé, 2019, ch. 13, art. 99] 2015, ch. 20, art. 42, 2019; ch. 13, art. 99.

Charte canadienne des droits et libertés, partie I de la *Loi constitutionnelle de 1982*, édictée comme l'annexe B de la *Loi de 1982 sur le Canada*, 1982, c 11 (R.-U.)

Fouilles, perquisitions ou saisies

8 Chacun a droit à la protection contre les fouilles, les perquisitions ou les saisies abusives.