Federal Court  Cour fédérale

Date : 20091005

Dossier : CSIS-30-08

Référence : 2009 CF 1058

Ottawa (Ontario), le 5 octobre 2009

En présence de monsieur le juge Mosley

ENTRE :

AFFAIRE INTÉRESSANT une demande présentée par [redacted] visant la délivrance d'un mandat 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 [redacted]

MOTIFS PUBLICS DE L'ORDONNANCE MODIFIÉE ET EXPURGÉE

Le juge Mosley

[1] Le 27 novembre 2008, la Cour a décerné 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 (la Loi), lesquels portaient sur les activités de deux citoyens canadiens au sujet desquels il y avait des motifs raisonnables de croire qu'ils constituaient des menaces envers la sécurité du Canada. Les mandats, valides pendant un an, autorisaient l'utilisation de techniques d'enquête intrusives et la collecte de renseignements au Canada.

[2] Le 24 janvier 2009, une demande a été présentée en urgence, dans laquelle on sollicitait la délivrance d'un mandat supplémentaire visant les deux mêmes personnes et portant sur des activités qui s'étaient récemment révélées susceptibles de constituer des menaces. La demande était appuyée par l'affidavit du demandeur, un agent du Service canadien du renseignement de sécurité (le SCRS ou le Service), et par celui d'un expert employé par le Centre de la sécurité des télécommunications (le CST). Une audience a eu lieu le samedi 26 janvier 2009, lors de laquelle des observations ont été présentées par l'avocat du procureur général du Canada au nom du demandeur et des témoignages ont été entendus. Des observations écrites ainsi que des autorités ont également été déposées auprès de la Cour.

[3] La demande susmentionnée était différente de celle tranchée en novembre 2008 : elle portait sur des activités susceptibles de constituer des menaces qui, croyait-on, seraient entreprises alors que les deux personnes se trouveraient à l'extérieur du Canada. À cet égard, la demande était semblable à celle entendue, puis rejetée, par le juge Edmond Blanchard dans une décision rendue le 22 octobre 2007 (SCRS-10-07) et publiée dans une version expurgée : *Loi sur le service canadien du renseignement de sécurité (RE)*, 2008 CF 301. Dans cette décision, le juge Blanchard a conclu que la Loi n'accordait pas à la Cour compétence pour autoriser des employés du SCRS à mèner, à l'extérieur du Canada, des enquêtes comportant intrusion.

[4] En l'espèce, le demandeur a demandé à la Cour de se pencher de nouveau sur la question de la compétence et de faire une différence entre l'espèce et le raisonnement tenu par le juge Blanchard dans la décision de 2007, et ce, sur le fondement :

a) d'une description plus exhaustive des faits portant sur les activités – laquelle est nécessaire pour obtenir l'autorisation d'intercepter des communications – ainsi que des procédures qui seront utilisées afin d'obtenir les renseignements recherchés;

b) d'un argument juridique différent expliquant comment la méthode d'interception fait en sorte que la Cour a compétence en l'espèce.

[5] Après avoir lu les documents dont disposait la Cour et avoir entendu les témoignages du témoin du CST et les observations de l'avocat, j'ai été convaincu que les faits et le droit justifiaient que la présente demande soit considérée comme différente de la demande dont avait été saisi le juge Blanchard, et j'ai décerné le mandat, qui était valide pour trois mois. Le 6 avril 2009, j'ai entendu d'autres observations présentées par l'avocat et, le 16 avril 2009, j'ai prolongé le mandat de neuf autres mois. J'estime qu'il convient aujourd'hui de fournir les motifs écrits portant sur la délivrance du mandat qui a fait suite à la demande dont j'ai été saisi.

Le contexte

[6] Les questions tranchées par le juge Blanchard dans la demande de 2007 ont d'abord été soumises au juge Simon Noël dans le cadre d'une demande déposée en juin 2005 (CSIS -18-05). Dans cette instance, le juge Noël avait nommé M. Ronald Atkey, c.r., afin qu'il agisse en qualité d'*amicus curiae*. Une question préliminaire s'était imposée : les questions de droit soulevées dans la demande devaient-elles être tranchées dans le cadre d'une audience publique? Après avoir reçu les observations écrites et orales, le juge Noël a conclu que la demande devait être entendue à huis clos. Les motifs exhaustifs donnés par le juge Noël ont été rendus publics : *Loi sur le service canadien du renseignement de sécurité (Re)*, 2008 CF 300. Le 23 août 2006, l'avocat du sous-procureur général du Canada a déposé un avis de désistement avant que n'aient pu être tranchées les questions de droit portant sur l'étendue de la compétence de la Cour.

[7] La question de la compétence extraterritoriale a de nouveau été soulevée dans une demande de mandat dont a été saisi le juge Blanchard en avril 2007. Compte tenu de la preuve par affidavit, le juge Blanchard a été convaincu que les conditions préalables prévues aux alinéas 21(2)*a*) et *b*) de la Loi avaient été remplies, c'est-à-dire que l'affidavit mentionnait les faits sur lesquels le déposant s'était appuyé afin d'étayer ses motifs raisonnables de croire que les mandats étaient nécessaires pour permettre au Service de mener une enquête sur des menaces envers la sécurité du Canada; que d'autres méthodes d'enquêtes avaient été essayées en vain ou qu'elles avaient peu de chance de succès et que, sans mandat, des renseignements importants concernant les menaces ne pourraient pas être obtenus. Des mandats ont donc été décernés par le juge Blanchard à cette époque afin qu'ils soient exécutés au Canada.

[8] Au moment où il a décerné les mandats initiaux dans le cadre de la demande SCRS-10-07, le juge Blanchard n'était pas disposé à autoriser, sans autre considération, le Service à effectuer des enquêtes à l'extérieur du Canada comme le demandeur le lui avait demandé. Par conséquent, M. Atkey a de nouveau été nommé afin qu'il agisse en qualité d'*amicus curiae*, et le juge Blanchard a reçu les observations écrites et orales de M. Atkey et de l'avocat du sous-procureur général du Canada. Ces observations ont initialement mis l'accent sur deux questions formulées par la Cour : d'une part, le SCRS a-t-il pour mission d'entreprendre des enquêtes, à l'extérieur du Canada, sur des activités susceptibles de constituer des menaces et, d'autre part, la Cour fédérale a-t-elle compétence pour décerner des mandats autorisant de telles enquêtes?

[9] Des questions supplémentaires ont été formulées par le juge Blanchard à la suite de l'arrêt *R. c. Hape*, 2007 CSC 26, rendu par la Cour suprême du Canada, lequel portait sur l'application de la *Charte canadienne des droits et libertés* – qui constitue l'annexe B de la *Loi de 1982 sur le Canada*, 1982, ch. 11 (R.-U.), qui est entrée en vigueur le 17 avril 1982 (la Charte) – aux enquêtes menées à l'étranger par les autorités canadiennes. Des observations supplémentaires ont été déposées par l'*amicus curiae* sur ces questions.

[10] Dans l'arrêt *Hape*, la Cour suprême du Canada a confirmé le principe que, sauf mention expresse contraire à ce sujet dans la loi, la loi est présumée respecter le droit international et que le droit international coutumier interdit de s'immiscer dans les affaires intérieures des autres États. Le paragraphe 65 de l'arrêt *Hape* est très instructif à ce sujet :

> Dans l'*Affaire du « Lotus »*, la Cour permanente de justice internationale a conclu que la compétence « ne pourrait être exercée hors du territoire, sinon en vertu d'une règle permissive découlant du droit international coutumier ou d'une convention » […] Cette

> décision confirme que la compétence extraterritoriale est régie par le droit international et ne relève donc pas de la seule volonté des États individuels. S'il est vrai que le droit international reconnaît la compétence extraterritoriale – normative, d'exécution ou juridictionnelle –, il lui impose des limites strictes fondées sur les principes de l'égalité souveraine, de la non-intervention et de la territorialité. Le principe de non-intervention veut qu'un État s'abstienne d'invoquer sa compétence d'exécution extraterritoriale dans un domaine où, suivant le principe de la souveraineté territoriale, l'autre État peut exercer son pouvoir décisionnel en toute liberté et autonomie (voir l'avis de la Cour internationale de justice dans l'*Affaire des activités militaires et paramilitaires au Nicaragua et contre celui-ci*, p. 108). Par conséquent, il est bien établi qu'un État peut faire appliquer ses lois à l'étranger seulement s'il obtient le consentement de l'État en cause ou, à titre exceptionnel, si le droit international l'y autorise par ailleurs. […] Le principe du consentement se révèle fondamental pour toute revendication de la compétence d'exécution extraterritoriale. [Non souligné dans l'original; renvois omis.]

[11] Comme l'a mentionné le juge Blanchard aux paragraphes 29 à 31 de ses motifs, le Service a adopté la position que le régime légal établi par la Loi donne à la Cour le pouvoir nécessaire de décerner des mandats ayant effet à l'étranger. Le Service ne demandait pas l'autorisation de contrevenir aux lois d'un pays étranger, mais il reconnaissait que les activités visées par la demande d'autorisation y contreviendraient vraisemblablement. L'*amicus curiae* souscrit à la prétention de l'avocat du Service, selon laquelle il n'existe aucune limite territoriale concernant les activités du SCRS en ce qui a trait à la collecte, à l'analyse et à la conservation de renseignements au sujet des menaces envers la sécurité du Canada, tel que cela est énoncé à l'article 12 de la Loi. Toute demande de mandat en vertu de l'article 21 de la Loi peut s'étendre aux enquêtes du SCRS à l'extérieur du Canada. Toutefois, selon *l'amicus curiae*, le Service ne pourrait pas exécuter un mandat obtenu en vertu de l'article 21 de la Loi et exercer ses pouvoirs de collecte de renseignements dans un autre pays, à moins qu'il ait obtenu la permission du pays où les cibles des mandats résident

ou qu'il ait été partie à un traité ou à une entente englobant l'exercice de ses pouvoirs dans cet autre pays.

[12] À la suite d'un examen de la Loi et des principes de droit international traités par la Cour suprême du Canada dans l'arrêt *Hape*, le juge Blanchard a conclu qu'il n'était pas en mesure de donner aux dispositions applicables de la Loi une interprétation qui habiliterait la Cour à décerner un mandat pouvant être exécuté à l'étranger.

[13] Suivant le principe moderne d'interprétation des lois adoptée par la Cour suprême du Canada dans l'arrêt *Rizzo & Rizzo Shoes Ltd.*, [1998] 1 R.C.S. 27, au paragraphe 41, le juge Blanchard a conclu que les pouvoirs d'enquête sollicités dans la demande dont il était saisi n'étaient pas expressément autorisés par la Loi. Parmi les facteurs dont a tenu compte le juge Blanchard au paragraphe 39 de ses motifs, il y avait l'absence de limite territoriale expresse dans les articles 12 et 21 de la Loi. Le juge Blanchard a noté que, même s'il peut être inféré de la Loi que le Service à la mission de mener certaines activités à l'extérieur du territoire national, cette inférence n'est pas suffisamment manifeste pour que l'on puisse conclure que le Service a clairement la mission de mener les activités qu'il vise à faire autoriser dans le mandat, et ce, dans d'autres pays que le Canada, et que la Cour a compétence pour autoriser ce genre d'activités.

[14] Compte tenu de sa conclusion – selon laquelle il a été incapable de donner un sens évident, ou suffisamment clair, aux dispositions applicables de façon à permettre leur application à l'étranger –, le juge Blanchard a par la suite examiné d'autres facteurs afin de l'aider à interpréter l'objet de la Loi. En définitive, il a conclu que la preuve ne permettait pas de conclure que le législateur avait l'intention d'attribuer au Service une mission

consistant à faire utiliser des méthodes d'enquêtes s'apparentant à celles que l'on cherchait à faire autoriser dans le mandat.

[15] Le juge Blanchard a par la suite examiné les principes de droit international. Il a conclu que les méthodes d'enquêtes dont on sollicitait l'autorisation violeraient vraisemblablement les lois du ressort où le mandat serait exécuté. Sans le consentement des États étrangers à ce que le Canada applique ses lois à l'intérieur de leurs frontières, les méthodes d'enquêtes envisagées constitueraient une violation de la souveraineté territoriale et du droit international coutumier.

[16] Le juge Blanchard s'est penché sur la question de savoir si le *Code criminel*, L.R.C. 1985, ch. C-46, et la Charte s'appliquent aux activités des agents du SCRS qui mènent des enquêtes sur de possibles menaces à l'étranger. Cette partie des motifs n'était pas absolument nécessaire parce que le juge Blanchard avait tranché la question de la compétence en interprétant la Loi et en se fondant sur les principes du droit international.

[17] La principale allégation du Service dans sa demande présentée au juge Blanchard était que le mandat demandé était nécessaire afin de garantir le respect, par les agents canadiens enquêtant à l'étranger, du droit canadien, car les méthodes d'enquêtes contestées pouvaient, en l'absence du mandat, violer la Charte et le *Code criminel*. L'article 26 de la Loi dispose que la partie VI du *Code criminel* ne s'applique pas à une interception de communication autorisée par un mandat décerné en vertu de l'article 21 de la Loi. En l'absence de la protection offerte par le mandat, la partie VI s'appliquerait à l'interception de toute « communication privée » au sens de l'article 183 du *Code criminel*, c'est-à-dire toute communication privée lors de laquelle l'auteur ou le destinataire se trouve au Canada.

[18] Le juge Blanchard a conclu que les principes établis dans l'arrêt *Hape* concernant la compétence d'enquête dans le cadre d'une affaire criminelle s'appliquaient également à la collecte de renseignements dans le contexte des services de renseignement. Il a conclu que la Charte ne s'appliquait pas aux activités des agents du renseignement qui font la collecte de renseignements à l'étranger sans le consentement de l'État concerné.

[19] Je note que la juge Anne MacTavish, dans la décision *Amnistie internationale Canada c. Canada (Chef d'état-major de la Défense)*, 2008 CF 336, confirmée par 2008 CAF 401, s'est penchée sur l'application de la Charte dans le contexte distinct de la participation du Canada à l'opération militaire multinationale qui se déroule actuellement en Afghanistan. Compte tenu des critères de l'arrêt *Hape* et l'absence de consentement du gouvernement de l'Afghanistan quant à l'application du droit canadien sur son territoire, la juge MacTavish a conclu que la Charte ne s'appliquait pas aux non-Canadiens détenus par les Forces canadiennes en Afghanistan et transférés aux autorités afghanes. La juge MacTavish, au paragraphe 344 de ses motifs, a par contre fait remarquer que les membres du personnel militaire canadien pouvaient faire l'objet de poursuites pénales intentées suivant le droit canadien pour leurs actions en Afghanistan.

[20] En l'espèce, je suis convaincu que le mandat était justifié et qu'il y avait des circonstances impérieuses liées à la nature des menaces, circonstances faisant en sorte que le mandat devait être décerné de toute urgence. Lorsque j'ai tranché la demande le 26 janvier 2009, je me suis demandé si, à l'instar des juges Noël et Blanchard, il serait approprié de nommer un *amicus curiae* afin d'aider la Cour à trancher la question de la compétence. Étant donné l'urgence de la situation dont j'étais saisi et les observations quant aux faits et au droit présentées au nom du demandeur, j'ai conclu qu'il ne serait pas

judicieux de retarder la délivrance du mandat. En outre, la question de savoir si l'exécution d'un mandat d'application extraterritoriale pouvait être autorisée avait été examinée de façon exhaustive par le juge Blanchard dans sa décision.

Le cadre législatif

[21] Les dispositions pertinentes sont jointes dans l'annexe A des présents motifs. En résumé, l'article 12 de la Loi mentionne le mandat du Service et dispose que le Service recueille, au moyen d'enquêtes ou autrement, analyse et conserve l'information et les renseignements sur les activités dont il existe des motifs raisonnables de soupçonner qu'elles constituent des menaces envers la sécurité du Canada; il doit faire rapport au gouvernement du Canada et le conseiller au sujet de ces activités.

[22] En vertu de l'article 21, un juge a le pouvoir d'autoriser que le SCRS intercepte des communications et obtienne des renseignements et qu'il exerce des activités afin d'arriver à ces objectifs. Les exigences préalables sont les suivantes : le SCRS doit enquêter sur des « menaces envers la sécurité du Canada »; il y a des motifs raisonnables de croire qu'un mandat est nécessaire et, sans mandat, d'importants renseignements ne seront pas obtenus.

[23] Les « menaces envers la sécurité du Canada » sont définies à l'article 2 de la Loi comme étant notamment « les activités qui touchent le Canada ou s'y déroulent et visent à favoriser l'usage […] de menaces ». [Je souligne]

[24] Selon l'alinéa 21(2)*f*) de la Loi, une demande de mandat doit également renfermer, si possible, une description générale du lieu où le mandat demandé doit être exécuté.

[25] La Loi définit « intercepter » à l'article 2 comme ayant le sens qui lui est donné à l'article 183 du *Code criminel*, soit, notamment, le « fait d'écouter, d'enregistrer ou de prendre volontairement connaissance d'une communication ou de sa substance, son sens ou son objet ». Suivant l'article 26 de la Loi, la partie VI du *Code criminel* ne s'applique pas aux interceptions autorisées par un mandat décerné en vertu de la Loi.

La question en litige

[26] Le demandeur soutient essentiellement que la Cour a compétence, en vertu de l'article 21 de la Loi, pour décerner des mandats visant l'autorisation judiciaire des activités des représentants du gouvernement au Canada en lien avec une enquête qui s'étendra au-delà des frontières du Canada. Le demandeur admet que, s'ils n'étaient pas approuvés par la Cour, les actes pour lesquels il demande autorisation pourraient violer le *Code criminel* ou les droits constitutionnels de certaines personnes.

[27] La Cour doit trancher la question de savoir si elle a compétence pour autoriser des actes posés par le SCRS au Canada, lesquels nécessitent l'écoute de communications et la collecte de renseignements provenant de l'étranger.

Les prétentions du demandeur

[28] En l'espèce, le demandeur sollicitait l'autorisation pour exercer deux types d'activités : l'interception de communications et la collecte de renseignements [redacted]. Si l'autorisation était accordée, le SCRS envisageait de demander l'assistance du CST en vertu de l'alinéa 24*b*) de la Loi, qui dispose que le mandat décerné en vertu de l'article 21 autorise quiconque à prêter assistance à une personne habilitée par le

mandat. Grâce à cette assistance, le SCRS envisage d'intercepter les types de communications suivantes :

a) des communications ayant lieu [redacted];

b) des communications qui [redacted];

c) des communications qui [redacted];

[29] En plus des communications susmentionnées, le demandeur veut, au moyen de l'autorisation, obtenir des renseignements [redacted].

[30] Le demandeur soutient que les activités nécessaires à l'interception des communications et la collecte de renseignements [redacted], effectuée avec l'assistance du CST, se fera uniquement au Canada. Les communications ne seront écoutées et les renseignements [redacted] ne seront lus qu'au Canada.

[31] Le mandat du CST est établi dans la *Loi sur la défense nationale*, L.R.C. 1985, ch. N-5, telle que modifiée par la *Loi antiterroriste*, L.C. 2001, ch. 41. Suivant l'alinéa 273.64(1)*a*) de cette loi, le CST a l'autorisation d'acquérir et d'utiliser l'information provenant de l'infrastructure mondiale d'information (c'est-à-dire les systèmes de

télécommunication ainsi que les systèmes et les réseaux de technologie de l'information) dans le but de fournir des renseignements étrangers au gouvernement du Canada. Selon l'alinéa 273.64(2)*a*), les activités du CST ne peuvent pas viser des citoyens canadiens ni les résidents permanents, et ce, peu importe où ils se trouvent (les Canadiens), ni toute personne présente au Canada sans égard à sa nationalité.

[32] La restriction concernant les Canadiens ou les personnes se trouvant au Canada ne s'applique pas à l'assistance technique ou opérationnelle que le CST peut fournir, selon l'alinéa 273.64(1)*c*) de la *Loi sur la défense nationale*, aux organismes fédéraux chargés de l'application de la loi ou de la sécurité dans l'exercice des fonctions que la loi leur confère. Le paragraphe 273.64(3) de cette loi dispose que l'assistance offerte est assujettie aux limites que la loi impose à l'exercice des fonctions des organismes fédéraux en question.

[33] Par conséquent, en l'espèce, le CST pourra porter assistance au SCRS dans l'interception des communications et la collecte des renseignements seulement si la Cour autorise le mandat sollicité par le SRSC en vertu de l'article 21 de la Loi.

[34] Le témoignage du témoin du CST entendu le 26 janvier 2009 faisait état des capacités d'interception du CST [redacted]. Le témoignage révélait que les interceptions envisagées seraient contrôlées de l'intérieur du Canada [redacted].

[35] Les communications qui peuvent être interceptées ou obtenues par le CST de l'intérieur du Canada [redacted]

[redacted]

[36] [redacted] chaque activité qui modifie la capacité d'intercepter des communications aura lieu au Canada. Dans ces circonstances, selon l'avocat du sous-procureur général, la compétence de la Cour de décerner le mandat n'est pas remise en question.

[37] [redacted]. Le demandeur avance que [redacted]

les communications seraient interceptées, au sens de la Loi, seulement où elles seraient écoutées, c'est-à-dire au Canada.

[38] [redacted]. Les renseignements trouvés [redacted] seraient « saisis » seulement là où ils seraient lus pour la première fois, au Canada.

[39] [redacted]

[40] Le demandeur soutient que la question de savoir où le mandat serait exécutés dépend de l'endroit où seraient interceptées les communications et obtenus les renseignements. Il plaide que, ce qui est demandé à la Cour en l'espèce, ce n'est pas la délivrance d'un mandat qui autoriserait des activités à l'étranger, mais plutôt un mandat qui autoriserait la tenue d'enquêtes au Canada ainsi que l'interception de communications et la collecte de renseignements depuis le Canada.

[41] [redacted]

Analyse

Interception des communications

[42] Dans le cadre de l'examen de la présente demande, j'ai eu l'avantage de lire, en plus des témoignages et des observations reçus, la décision du juge Blanchard, tant dans sa forme expurgée que dans sa forme intégrale, de même que le contenu de la demande dont il était saisi. Du paragraphe 14 au paragraphe 16 de ses motifs, le juge Blanchard décrit la nature des pouvoirs qu'aurait conféré le mandat demandé. On sollicitait l'autorisation d'intercepter des communications, afin d'obtenir toute information ou tout document concernant les cibles [redacted].

[43] Dans la demande de mandat présentée en 2007 dont était saisi le juge Blanchard, on sollicitait l'autorisation d'installer, d'entretenir ou d'enlever tout objet nécessaire

[redacted]. Il ressort clairement de la demande de mandat en tant que telle et des motifs du juge Blanchard que le mandat devait inclure l'autorisation de [redacted] à l'étranger afin d'installer les objets par lesquels les communications, les renseignements et les dossiers [redacted].

[44] La proposition de mandat qu'on me demande d'approuver diffère de celle qui a été présentée au juge Blanchard en plusieurs aspects. [redacted] L'autorisation demandée d'intercepter la communication depuis n'importe quel endroit à l'extérieur du Canada où la communication pouvait être interceptée n'a pas été accordée. L'autorisation d'installer, d'entretenir ou d'enlever tout objet nécessaire pour intercepter ou obtenir des renseignements et pour obtenir l'accès aux renseignements, les rechercher, les examiner et les enregistrer a été limitée à [TRADUCTION] « depuis le Canada ».

[45] À mon sens, toutes les activités pour lesquelles l'autorisation d'intercepter des communications est demandée seraient comprises dans le terme « intercepter » défini dans la Loi par renvoi à la définition du *Code criminel*. Le SCRS cherche également à écouter ou enregistrer des communications ou à en prendre volontairement connaissance entre leur lieu d'origine et leur destination. Ces activités constituent des « interceptions » au sens donné à

ce terme par la jurisprudence dans des arrêts portant sur la définition du *Code criminel* : *R. c. McQueen* (1975), 25 C.C.C. (2d) 262 (Alta C.A.); *R. c. Giles*, 2007 BCSC 1147.

[46] La demande visant à faire autoriser l'interception de communications [redacted] pose peu de difficultés, à mon avis, parce que le mandat serait exécuté [redacted] au Canada. La Loi ne limite pas géographiquement l'interception de communications à celles qui proviennent du Canada ou qui doivent être reçues au Canada, contrairement à ce que prévoit la partie VI du *Code criminel*. En l'absence d'une exigence géographique de ce genre, il semble qu'il n'y ait aucun obstacle légal à l'interception de communications effectuée en vertu de la Loi et, d'ailleurs, la Cour a décerné auparavant des mandats à cet effet. Encore une fois, je fais observer que la partie VI du *Code criminel* ne s'applique pas aux interceptions autorisées en vertu de la Loi ni à toute communication ainsi interceptée.

[47] L'interception de communications qui sont transmises [redacted] semble également présenter peu de difficultés du point de vue de la compétence, dans la mesure où les signaux sont interceptés depuis le Canada. [redacted]

[48] Posent plus de difficultés les pouvoirs d'intercepter et [redacted] d'obtenir des renseignements susceptibles d'avoir des répercussions à l'étranger. [Les mots soulignés sont ajoutés pour faciliter la compréhension de la version expurgée.]

[49] [redacted]. Cela soulève la question de savoir si la communication est interceptée au sens de la loi. Si le lieu de l'interception doit être considéré comme se situant à l'étranger, la Cour, si elle applique les principes énoncés dans la décision du juge Blanchard, n'aurait pas compétence pour décerner un mandat autorisant de telles activités.

[50] Dans le contexte des autorisations accordées en vertu de la partie VI du *Code criminel*, le lieu d'interception des communications par ligne terrestre, et par conséquent le ressort d'où peut être autorisée l'interception, est généralement synonyme du lieu où le téléphone de la personne concernée se situe, même si l'interception en tant que telle se fait au poste de commutation de la compagnie de téléphone à quelque distance de là. Avec l'avènement de la technologie sans fil, des problèmes ont surgi du fait que la communication change constamment de cellule de transmission à mesure que le téléphone est amené d'un endroit à l'autre.

[51] Dans *R c. Taylor*, [1997] B.C.J. n^{o} 346, la Cour d'appel de la Colombie-Britannique a infirmé la décision du juge de première instance selon laquelle la communication cellulaire avait été interceptée illégalement au bureau d'un avocat, contrairement aux modalités de l'autorisation. La Cour d'appel a conclu que, correctement interprétée, l'interception avait eu lieu non pas dans le bureau de l'avocat, mais au centre de distribution des appels sans fil où les appels avaient été enregistrés et où il avait été pris connaissance de leur contenu.

[52] Dans le contexte en l'espèce, les interceptions autorisées se feront au Canada où les appels seront écoutés et enregistrés et où il sera pris connaissance de leur contenu.

[53] Bien qu'il semble qu'il n'y ait pas de jurisprudence canadienne à ce sujet, l'avocat du sous-procureur général du Canada a porté à mon attention un certain nombre de décisions américaines dans lesquelles des cours d'appel des États-Unis ont statué qu'un juge a le pouvoir d'autoriser l'interception de communications lorsque le premier endroit où la communication sera écoutée se situe dans le ressort du juge : *U.S. c. Denman*, 100 F 3d 399 (5th Cir., 1996); *U.S. c. Rodriguez*, 968 F 2d 130 (2d Cir., 1992); *U.S. c. Luong*, 471 F 3d 1007 (9th Cir., 2006); *U.S. c. Ramirez*, 112 F 3d 849 (7th Cir., 1997); *U.S. c. Jackson*, 471 F 3d 910 (7th Cir., 2000); *U.S. c. Tavarez*, 40 F 3d 1136 (10th Cir., 1994); *People c. Perez*, 848 N.Y.S. 2d 525 (N.Y. Supreme Ct.) contra, *Castillo c. Texas*, 810 S.W. 2d 180 (Texas Ct. Crim. App. 1990).

[54] Le Congrès américain régit la surveillance électronique par la section III de l'*Omnibus Crime Control and Safe Streets Act*, 18 U.S.C. 2510. Dans cette loi, la définition

du terme « intercepter » est très semblable à celle figurant dans la partie VI du *Code criminel* du Canada. L'interception désigne [TRADUCTION] « la prise de connaissance auditive ou autre d'une communication transmise par câble, par voie électronique ou oralement au moyen d'un objet électronique, mécanique ou autre ». Selon la législation fédérale américaine, l'interception ne peut être autorisée que dans le ressort du tribunal où siège le juge (18 U.S.C. 2518 (3)). Les États américains ont adopté des exigences de compétence semblables.

[55] Les Cours d'appel des États-Unis, qui se sont penchées sur la question, ont interprété le terme [TRADUCTION] « interception » tel qu'il est mentionné dans la section III comme incluant à la fois le lieu où les téléphones visés par les mandats judiciaires sont situés et l'endroit où les communications sont écoutées pour la première fois par les agents chargés de l'application de la loi.

[56] [redacted] l'interception doit également être considérée comme ayant lieu à l'endroit où le contenu [redacted] est entendu pour la première fois. Dans l'arrêt *Denman*, précité, une cour d'appel américaine a conclu que l'interception avait lieu à deux endroits, soit là où le signal est capté et là où la communication est écoutée pour la première fois, et que les juges des deux endroits ont compétence.

[57] La Cour d'appel en matière de droit criminel du Texas en est venue à une conclusion différente dans l'arrêt *Castillo*. Dans cet arrêt, la majorité de la Cour d'appel en matière de droit criminel s'inquiétait du risque de [TRADUCTION] « magasinage de juge » si on reconnaissait une définition plus large. Elle a conclu que l'assemblée législative de l'État avait délibérément et expressément adopté une [TRADUCTION] « restriction territoriale » limitant la compétence d'autoriser les interceptions au district précis où le dispositif d'écoute était situé. Dans l'arrêt *Perez*, la Cour suprême de New-York a estimé que le risque de « magasinage » de tribunal n'était pas important et a suivi la jurisprudence fédérale.

[58] Le raisonnement dans [redacted] les [redacted] décisions des cours d'appel des États-Unis est convaincant. L'interception de communications personnelles en droit canadien nécessite plus que le fait de capter techniquement le signal transmettant la communication. Il faut qu'il y ait écoute ou une autre forme de prise de connaissance du contenu de la communication. Le fait que la communication puisse être [redacted] n'empêche pas que soit accordée l'autorisation d'intercepter la communication depuis le Canada.

[59] En autorisant le SCRS, avec le soutien technique du CST, à obtenir des renseignements [redacted] interceptés au Canada, je n'autorise pas le CST à outrepasser le mandat légal que lui confie la *Loi sur la défense nationale*. [redacted] les activités du CST ne viseront pas des citoyens canadiens et n'auront pas pour but d'obtenir des renseignements pour le CST, elles serviront plutôt à aider le SCRS. La question dont je suis saisi est de savoir si la Cour peut autoriser le SCRS à écouter et à

enregistrer des communications depuis le Canada [redacted]. Après m'être penché sur la question, je suis convaincu que la Cour a compétence pour décerner un tel mandat.

[60] Le demandeur soutient que, [redacted], les exigences relatives à la compétence de décerner un mandat en vertu de l'article 21 sont remplies lorsque l'autorisation demandée vise à pouvoir obtenir des renseignements depuis le Canada. Je suis d'accord. Cependant, la question de savoir si la Cour peut autoriser le SCRS à [redacted] fait entrer en ligne de compte d'autres considérations.

[61] L'article 21 de la Loi confère au juge désigné le pouvoir d'autoriser le SCRS à intercepter toute communication ou à obtenir tout renseignement, dossier, document ou objet. [redacted].

[62] [redacted]

[63]

[64] La saisie, depuis le Canada, de renseignements que le détenteur considère raisonnablement comme étant privés soulève la question de l'application de l'article 8 de la Charte. En l'espèce, il y a de nombreux motifs justifiant que l'on s'immisce dans la vie privée des individus concernés et il n'est pas prétendu que la collecte de renseignements contreviendrait aux droits garantis par la Charte les protégeant contre les perquisitions, les fouilles et les saisies abusives. La question est de savoir si la Cour peut autoriser ces actions au Canada en sachant que la collecte de ces renseignements dans un pays étranger pourrait violer la souveraineté territoriale de cet État.

[65] Au paragraphe 54 de la décision *Loi sur le Service canadien du renseignement de sécurité (Re)*, précitée, le juge Blanchard a conclu qu'on ne lui avait présenté « aucun fondement dans le droit international » qui supplanterait les principes de l'égalité souveraine, de la non-intervention et de la territorialité. Le SCRS avait fait valoir que la pratique internationale coutumière pour ce qui est des opérations de collecte de renseignements dans un État étranger constituait une exception aux principes de la souveraineté territoriale. Je ferai encore une fois observer que la demande dont était saisi le juge Blanchard sollicitait l'autorisation de procéder à des activités comportant intrusion dans des ressorts étrangers [redacted], ce qui n'est pas le cas dans la présente demande. À la suite de la décision du juge Blanchard, la Cour d'appel fédérale a fait observer que l'information peut en théorie se trouver à plus d'un endroit : voir *eBay Canada Limited c. Ministre du Revenu national*, 2008 CAF 348.

[66] Je suis convaincu que le fait et le droit justifient que la présente demande soit considérée comme différente de la demande dont a été saisi le juge Blanchard. À mon avis, ce qui est proposé dans le mandat en l'espèce n'est pas l'application de lois canadiennes à l'étranger, mais plutôt l'exercice au Canada d'une compétence relative à la protection de la sécurité du pays.

[67] La question de savoir si la courtoisie internationale interdit l'utilisation de mesures d'enquête ayant des répercussions extraterritoriales se pose plus souvent en droit criminel. C'est dans ce domaine que la plupart des litiges à cet égard sont survenus, car il touche le cœur de la compétence territoriale inhérente à la souveraineté de l'État : John H. Currie,

Public International Law, Toronto, Irwin Law, 2008, aux pages 332 et suivantes. C'est dans le contexte d'une enquête criminelle que la Cour suprême a affirmé au paragraphe 65 de l'arrêt *Hape*, précité, que « […] un État peut faire appliquer ses lois à l'étranger seulement s'il obtient le consentement de l'État en cause ou, à titre exceptionnel, si le droit international l'y autorise par ailleurs ».

[68] Un exemple de courtoisie internationale en matière de droit criminel se trouve dans l'élaboration de la *Convention sur la cybercriminalité*, S.T.E. n^{o} 185, ouverte à la signature par le Conseil de l'Europe le 23 novembre 2001 et entrée en vigueur le 1er juillet 2004. Le Canada a participé à l'élaboration de la Convention et l'a signée, sans toutefois l'avoir ratifiée.

[69] La Convention est une réaction à de nouvelles formes de comportement criminel issues de la croissance d'Internet. Les services de police se butaient constamment à l'impossibilité d'enquêter sur des attaques provenant de l'étranger contre des systèmes informatiques locaux. Dans certains cas, la police a eu recours à des perquisitions informatiques transfrontalières pour obtenir des éléments de preuve à l'appui d'une poursuite au pays ou d'une demande d'extradition. Ces actes sont considérés comme une violation de la souveraineté territoriale du pays où les données sont situées, en l'absence du consentement de cet État : voir Stephan Wilskie, *International Jurisdiction in Cyberspace : Which States may Regulate the Internet?*, 50 Fed Commun L J 117.

[70] L'objectif de la Convention est de développer des outils efficaces pour lutter contre la cybercriminalité. Elle prévoit la criminalisation de certaines infractions relatives à

l'informatique, des pouvoirs de procédure permettant de faire enquête sur ce type de crime et de déposer des accusations, la conservation et la communication rapides de données stockées et l'entraide sur le plan juridique. L'accès transfrontière à des données stockées est autorisé avec consentement ou lorsque les données sont accessibles au public (article 32).

[71] Le Canada n'a pas encore ratifié la Convention, notamment parce que les lois nécessaires pour la mise en œuvre au pays des mesures sur la conservation et la divulgation des données n'ont pas été adoptées en raison des préoccupations à propos de leurs répercussions possibles sur la vie privée : voir par exemple http://www.cippic.ca/projects-cases-lawful-access/.

[72] Il ressort clairement du Rapport explicatif adopté en même temps que la Convention (se trouvant à l'adresse http://conventions.coe.int/Treaty/FR/Reports/Html/185.htm) que l'entente multilatérale n'a pas pour but de nuire aux mesures prises par les parties signataires afin de protéger la sécurité de leur nation (aux paragraphes 38 et 58). Cependant, la Convention ne prévoit pas de moyen par lequel des renseignements pourraient être collectés à l'étranger afin de protéger la sécurité nationale. Elle a pour objet principal l'utilisation à des fins criminelles des systèmes informatiques.

[73] Comme le montrent les faits en l'espèce, les individus représentant une menace à la sécurité du Canada peuvent se déplacer facilement et rapidement d'un pays à l'autre, sans couper les lignes de communication avec d'autres personnes se réclamant des mêmes idées. Il se peut que de l'information pouvant être cruciale pour prévenir les menaces ou y mettre

fin échappe aux agences de sécurité du pays si elles n'ont pas les moyens de suivre ces lignes de communication.

[74] Le principe de la souveraineté territoriale n'empêche pas une nation de collecter des renseignements dans le territoire d'une autre nation, bien qu'il l'empêche d'exercer sa compétence de faire appliquer ses lois. Comme le soutient M. Jack Goldsmith dans *The Internet and the Legitimacy of Remote Cross-Border Searches*, 2001 U. Chi. Legal F. 103, les nouvelles technologies ont simplement rendu plus facile la collecte de renseignements à l'étranger sans qu'il soit nécessaire de traverser concrètement la frontière.

[75] Le Canada a donné au CST le mandat de collecter des renseignements étrangers y compris des renseignements tirés de communications ainsi que de systèmes et de réseaux de technologie de l'information à l'étranger. La loi lui interdit de diriger ses activités contre des Canadiens ou contre toute personne se trouvant au Canada, mais elle ne l'empêche pas d'aider des organismes de sécurité et d'application de la loi agissant conformément à des délégations de pouvoirs légales comme des mandats décernés par des tribunaux. Le SCRS a le pouvoir de collecter des renseignements concernant des menaces potentielles à propos de Canadiens et d'autres personnes et, comme il en a été question précédemment, il n'est pas assujetti à des limites territoriales.

[76] Lorsque les conditions préalables à la délivrance d'un mandat sont remplies, y compris le contrôle judiciaire préalable, les motifs raisonnables et des cibles bien précises, la collecte de renseignements par le SCRS avec l'assistance du CST, comme le propose le

mandat, respecte le régime législatif approuvé par le législateur et ne contrevient pas à la Charte.

[77] En conclusion, je ferai observer que les tribunaux américains ont statué que la collecte de renseignements concernant les communications de citoyens américains voyageant à l'étranger n'étaient pas protégées par le quatrième amendement de la constitution américaine, qui exige le mandat : *In Re Sealed Case* (2002), 310 F.3d 717 (FISC); *In Re Directives [Redacted Text] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*; 22 août 2008, publiée dans sa version expurgée le 16 janvier 2009 (FISCR). Compte tenu des inquiétudes relatives à la vie privée des Canadiens exprimées par le législateur, il serait préférable que de telles activités soient autorisées après examen de la question par un tribunal, comme en l'espèce.

« Richard G. Mosley »
Juge

Traduction certifiée conforme
Jean-François Martin, LL.B., M.A.Trad.jur.

ANNEXE « A »

Loi sur le service canadien du renseignement de sécurité	***Canadian Security Intelligence Service Act***
Définitions	**Definitions**
2. Les définitions qui suivent s'appliquent à la présente loi.	**2.** In this Act,
« intercepter » "intercept"	"intercept" « intercepter »
« intercepter » S'entend au sens de l'article 183 du Code criminel.	"intercept" has the same meaning as in section 183 of the Criminal Code;
« menaces envers la sécurité du Canada » "threats to the security of Canada"	"threats to the security of Canada" « menaces envers la sécurité du Canada »
« menaces envers la sécurité du Canada » Constituent des menaces envers la sécurité du Canada les activités suivantes :	"threats to the security of Canada" means
a) l'espionnage ou le sabotage visant le Canada ou préjudiciables à ses intérêts, ainsi que les activités tendant à favoriser ce genre d'espionnage ou de sabotage;	(a) espionage or sabotage that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage,
b) les activités influencées par l'étranger qui touchent le Canada ou s'y déroulent et sont préjudiciables à ses intérêts, et qui sont d'une nature clandestine ou trompeuse ou comportent des menaces envers quiconque;	(b) foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person,
c) les activités qui touchent le Canada ou s'y déroulent 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;	(c) activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political, religious or ideological objective within Canada or a foreign state, and
	(d) activities directed toward undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of, the constitutionally

d) les activités qui, par des actions cachées et illicites, visent à saper le régime de gouvernement constitutionnellement établi au Canada ou dont le but immédiat ou ultime est sa destruction ou son renversement, par la violence.

La présente définition ne vise toutefois pas les activités licites de défense d'une cause, de protestation ou de manifestation d'un désaccord qui n'ont aucun lien avec les activités mentionnées aux alinéas a) à d).

established system of government in Canada,

but does not include lawful advocacy, protest or dissent, unless carried on in conjunction with any of the activities referred to in paragraphs (a) to (d).

Informations et renseignements

12. 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.

Collection, analysis and retention

12. The Service shall collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and, in relation thereto, shall report to and advise the Government of Canada.

Demande de mandat

21. (1) Le directeur ou un employé désigné à cette fin par le ministre peut, après avoir obtenu l'approbation du ministre, demander à un juge de décerner un mandat en conformité avec le présent article s'il a des motifs raisonnables de croire que le mandat est nécessaire pour permettre au Service de faire enquête sur des menaces envers la sécurité du Canada ou d'exercer les fonctions qui lui sont conférées en vertu de l'article 16.

Application for warrant

21. (1) Where the Director or any employee designated by the Minister for the purpose believes, on reasonable grounds, that a warrant under this section is required to enable the Service to investigate a threat to the security of Canada or to perform its duties and functions under section 16, the Director or employee may, after having obtained the approval of the Minister, make an application in accordance with subsection (2) to a judge for a warrant under this section.

Contenu de la demande

(2) La demande visée au paragraphe (1) est présentée par écrit et accompagnée de

Matters to be specified in application for warrant

(2) An application to a judge under subsection (1) shall be made in writing and be

l'affidavit du demandeur portant sur les points suivants :

a) les faits sur lesquels le demandeur s'appuie pour avoir des motifs raisonnables de croire que le mandat est nécessaire aux fins visées au paragraphe (1);

b) le fait que d'autres méthodes d'enquête ont été essayées en vain, ou la raison pour laquelle elles semblent avoir peu de chances de succès, le fait que l'urgence de l'affaire est telle qu'il serait très difficile de mener l'enquête sans mandat ou le fait que, sans mandat, il est probable que des informations importantes concernant les menaces ou les fonctions visées au paragraphe (1) ne pourraient être acquises;

c) les catégories de communications dont l'interception, les catégories d'informations, de documents ou d'objets dont l'acquisition, ou les pouvoirs visés aux alinéas (3)a) à c) dont l'exercice, sont à autoriser;

d) l'identité de la personne, si elle est connue, dont les communications sont à intercepter ou qui est en possession des informations, documents ou objets à acquérir;

e) les personnes ou catégories de personnes destinataires du mandat demandé;

f) si possible, une description générale du lieu où le mandat demandé est à exécuter;

g) la durée de validité applicable en vertu du paragraphe (5), de soixante jours ou d'un an au maximum, selon le cas, demandée pour le mandat;

h) la mention des demandes antérieures touchant des personnes visées à l'alinéa d), la date de chacune de ces demandes, le

accompanied by an affidavit of the applicant deposing to the following matters, namely,

(a) the facts relied on to justify the belief, on reasonable grounds, that a warrant under this section is required to enable the Service to investigate a threat to the security of Canada or to perform its duties and functions under section 16;

(b) that other investigative procedures have been tried and have failed or why it appears that they are unlikely to succeed, that the urgency of the matter is such that it would be impractical to carry out the investigation using only other investigative procedures or that without a warrant under this section it is likely that information of importance with respect to the threat to the security of Canada or the performance of the duties and functions under section 16 referred to in paragraph (a) would not be obtained;

(c) the type of communication proposed to be intercepted, the type of information, records, documents or things proposed to be obtained and the powers referred to in paragraphs (3)(a) to (c) proposed to be exercised for that purpose;

(d) the identity of the person, if known, whose communication is proposed to be intercepted or who has possession of the information, record, document or thing proposed to be obtained;

(e) the persons or classes of persons to whom the warrant is proposed to be directed;

(f) a general description of the place where the warrant is proposed to be executed, if a general description of that place can be given;

(g) the period, not exceeding sixty days or one year, as the case may be, for which the warrant is requested to be in force that is applicable by

nom du juge à qui elles ont été présentées et la décision de celui-ci dans chaque cas.

Délivrance du mandat

(3) Par dérogation à toute autre règle de droit mais sous réserve de la Loi sur la statistique, le juge à qui est présentée la demande visée au paragraphe (1) peut décerner le mandat s'il est convaincu de l'existence des faits mentionnés aux alinéas (2)a) et b) et dans l'affidavit qui accompagne la demande; le mandat autorise ses destinataires à intercepter des communications ou à acquérir des informations, documents ou objets. À cette fin, il peut autoriser aussi, de leur part :

a) l'accès à un lieu ou un objet ou l'ouverture d'un objet;

b) la recherche, l'enlèvement ou la remise en place de tout document ou objet, leur examen, le prélèvement des informations qui s'y trouvent, ainsi que leur enregistrement et l'établissement de copies ou d'extraits par tout procédé;

c) l'installation, l'entretien et l'enlèvement d'objets.

Contenu du mandat

(4) Le mandat décerné en vertu du paragraphe (3) porte les indications suivantes :

a) les catégories de communications dont l'interception, les catégories d'informations, de documents ou d'objets dont l'acquisition, ou les pouvoirs visés aux alinéas (3)a) à c) dont l'exercice, sont

virtue of subsection (5); and

(h) any previous application made in relation to a person identified in the affidavit pursuant to paragraph (d), the date on which the application was made, the name of the judge to whom each application was made and the decision of the judge thereon.

Issuance of warrant

(3) Notwithstanding any other law but subject to the Statistics Act, where the judge to whom an application under subsection (1) is made is satisfied of the matters referred to in paragraphs (2)(a) and (b) set out in the affidavit accompanying the application, the judge may issue a warrant authorizing the persons to whom it is directed to intercept any communication or obtain any information, record, document or thing and, for that purpose,

(a) to enter any place or open or obtain access to any thing;

(b) to search for, remove or return, or examine, take extracts from or make copies of or record in any other manner the information, record, document or thing; or

(c) to install, maintain or remove any thing.

Matters to be specified in warrant

(4) There shall be specified in a warrant issued under subsection (3)

(a) the type of communication authorized to be intercepted, the type of information, records, documents or things authorized to be obtained and the powers referred to in paragraphs (3)(a)

autorisés;

b) l'identité de la personne, si elle est connue, dont les communications sont à intercepter ou qui est en possession des informations, documents ou objets à acquérir;

c) les personnes ou catégories de personnes destinataires du mandat;

d) si possible, une description générale du lieu où le mandat peut être exécuté;

e) la durée de validité du mandat;

f) les conditions que le juge estime indiquées dans l'intérêt public.

Durée maximale

(5) Il ne peut être décerné de mandat en vertu du paragraphe (3) que pour une période maximale :

a) de soixante jours, lorsque le mandat est décerné pour permettre au Service de faire enquête sur des menaces envers la sécurité du Canada au sens de l'alinéa d) de la définition de telles menaces contenue à l'article 2;

b) d'un an, dans tout autre cas.

Primauté des mandats

24. Par dérogation à toute autre règle de droit, le mandat décerné en vertu des articles 21 ou 23 :

a) autorise ses destinataires, en tant que tels ou au titre de leur appartenance à une catégorie donnée :

(i) dans le cas d'un mandat décerné

to (c) authorized to be exercised for that purpose;

(b) the identity of the person, if known, whose communication is to be intercepted or who has possession of the information, record, document or thing to be obtained;

(c) the persons or classes of persons to whom the warrant is directed;

(d) a general description of the place where the warrant may be executed, if a general description of that place can be given;

(e) the period for which the warrant is in force; and

(f) such terms and conditions as the judge considers advisable in the public interest.

Maximum duration of warrant

(5) A warrant shall not be issued under subsection (3) for a period exceeding

(a) sixty days where the warrant is issued to enable the Service to investigate a threat to the security of Canada within the meaning of paragraph (d) of the definition of that expression in section 2; or

(b) one year in any other case.

Warrant to have effect notwithstanding other laws

24. Notwithstanding any other law, a warrant issued under section 21 or 23

(a) authorizes every person or person included in a class of persons to whom the warrant is directed,

(i) in the case of a warrant issued under section 21, to exercise the powers

en vertu de l'article 21, à employer les moyens qui y sont indiqués pour effectuer l'interception ou l'acquisition qui y est indiquée,

(ii) dans le cas d'un mandat décerné en vertu de l'article 23, à exécuter le mandat;

specified in the warrant for the purpose of intercepting communications of the type specified therein or obtaining information, records, documents or things of the type specified therein, or

(ii) in the case of a warrant issued under section 23, to execute the warrant; and

b) autorise quiconque à prêter assistance à une personne qu'il a des motifs raisonnables de croire habilitée par le mandat.

(b) authorizes any other person to assist a person who that other person believes on reasonable grounds is acting in accordance with such a warrant.

Code criminel du Canada

Définitions

183. Les définitions qui suivent s'appliquent à la présente partie.

« intercepter »
"intercept"

« intercepter »S'entend notamment du fait d'écouter, d'enregistrer ou de prendre volontairement connaissance d'une communication ou de sa substance, son sens ou son objet.

« communication privée »
"private communication"

« communication privée » Communication orale ou télécommunication dont l'auteur se trouve au Canada, ou destinée par celui ci à une personne qui s'y trouve, et qui est faite dans des circonstances telles que son auteur peut raisonnablement s'attendre à ce qu'elle ne soit pas interceptée par un tiers. La présente définition vise également la communication radiotéléphonique traitée électroniquement ou autrement en vue d'empêcher sa réception en clair par une personne autre que celle à laquelle son

Criminal Code of Canada

Definitions

183. In this Part,

"intercept"
« intercepter »

"intercept" includes listen to, record or acquire a communication or acquire the substance, meaning or purport thereof;

"private communication"
« communication privée »

"private communication" means any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing

auteur la destine.

intelligible reception by any person other than the person intended by the originator to receive it;

Loi sur la défense nationale

Mandat

273.64 (1) Le mandat du Centre de la sécurité des télécommunications est le suivant :

a) acquérir et utiliser l'information provenant de l'infrastructure mondiale d'information dans le but de fournir des renseignements étrangers, en conformité avec les priorités du gouvernement du Canada en matière de renseignement;

b) fournir des avis, des conseils et des services pour aider à protéger les renseignements électroniques et les infrastructures d'information importantes pour le gouvernement du Canada;

c) fournir une assistance technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité, dans l'exercice des fonctions que la loi leur confère.

National Defence Act

Mandate

273.64 (1) The mandate of the Communications Security Establishment is

(a) to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities;

(b) to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada; and

(c) to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.

Protection des Canadiens

(2) Les activités mentionnées aux alinéas (1)a) ou b) :

a) ne peuvent viser des Canadiens ou toute personne au Canada;

b) doivent être soumises à des mesures de protection de la vie privée des Canadiens lors de l'utilisation et de la conservation des renseignements interceptés.

Protection of Canadians

(2) Activities carried out under paragraphs (1)(a) and (b)

(a) shall not be directed at Canadians or any person in Canada; and

(b) shall be subject to measures to protect the privacy of Canadians in the use and retention of intercepted information.

Limites

Limitations imposed by law

(3) Les activités mentionnées à l'alinéa (1)c) sont assujetties aux limites que la loi impose à l'exercice des fonctions des organismes fédéraux en question.

(3) Activities carried out under paragraph (1)(c) are subject to any limitations imposed by law on federal law enforcement and security agencies in the performance of their duties.

Convention sur la cybercriminalité

Préambule

Les Etats membres du Conseil de l'Europe et les autres Etats signataires,

Considérant que le but du Conseil de l'Europe est de réaliser une union plus étroite entre ses membres;

Reconnaissant l'intérêt d'intensifier la coopération avec les autres Etats parties à la Convention;

Convaincus de la nécessité de mener, en priorité, une politique pénale commune destinée à protéger la société de la criminalité dans le cyberespace, notamment par l'adoption d'une législation appropriée et par l'amélioration de la coopération internationale;

Conscients des profonds changements engendrés par la numérisation, la convergence et la mondialisation permanente des réseaux informatiques;

Préoccupés par le risque que les réseaux informatiques et l'information électronique soient utilisés également pour commettre des infractions pénales et que les preuves de ces infractions soient stockées et transmises par le biais de ces réseaux;

Reconnaissant la nécessité d'une coopération entre les Etats et l'industrie privée dans la lutte contre la

Convention on Cybercrime

Preamble

The member States of the Council of Europe and the other States signatory hereto,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recognising the value of fostering co operation with the other States parties to this Convention;

Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation;

Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;

Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

Recognising the need for co-operation between States and private industry in

cybercriminalité, et le besoin de protéger les intérêts légitimes dans l'utilisation et le développement des technologies de l'information;

Estimant qu'une lutte bien menée contre la cybercriminalité requiert une coopération internationale en matière pénale accrue, rapide et efficace;

(…)

Chapitre II – Mesures à prendre au niveau national

Section 1 – Droit pénal matériel

Titre 1 – Infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques

Article 2 – Accès illégal

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique.

Article 3 – Interception illégale

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de

combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;

Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters;

(…)

Chapter II – Measures to be taken at the national level

Section 1 – Substantive criminal law

Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems

Article 2 – Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3 – Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by

données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques. Une Partie peut exiger que l'infraction soit commise dans une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique.

technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4 – Atteinte à l'intégrité des données

Article 4 – Data interference

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques.

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2 Une Partie peut se réserver le droit d'exiger que le comportement décrit au paragraphe 1 entraîne des dommages sérieux.

2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5 – Atteinte à l'intégrité du système

Article 5 – System interference

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'entrave grave, intentionnelle et sans droit, au fonctionnement d'un système informatique, par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération ou la suppression de données informatiques.

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 32 – Accès transfrontière à des données stockées, avec consentement ou

Article 32 – Trans-border access to stored

lorsqu'elles sont accessibles au public

Une Partie peut, sans l'autorisation d'une autre Partie :

a accéder à des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données; ou

b accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre Etat, si la Partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique.

"Omnibus Crime Control and Safe Streets Act"

computer data with consent or where publicly available

A Party may, without the authorisation of another Party:

a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

Omnibus Crime Control and Safe Streets Act

2510. Definitions

(…)

(4) 'intercept' means the aural acquisition of the contents of any wire or oral communication through the use of any electronic, mechanical, or other device.

COUR FÉDÉRALE

AVOCATS INSCRITS AU DOSSIER

DOSSIER :	SCRS-30-08
INTITULÉ :	AFFAIRE INTÉRESSANT une demande présentée par [ ] visant la délivrance d'un mandat 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 [ ]
LIEU DE L'AUDIENCE À HUIS CLOS :	Ottawa (Ontario)
DATES DE L'AUDIENCE À HUIS CLOS :	LE 24 JANVIER 2009, ET LE 6 AVRIL, 2009
MOTIFS PUBLICS DE L'ORDONNANCE MODIFIÉE ET EXPURGÉE :	MOSLEY, J.
DATE DES MOTIFS :	OCTOBER 5, 2009

COMPARUTIONS:

M. Robert Frater Mme Isabelle Chartier M. Andrew Cameron	POUR LE DEMANDEUR Sous-procureur général du Canada
M. Gordon Cameron	AMICUS CURIAE

AVOCATS INSCRITS AU DOSSIER:

William F. Pentney Sous-procureur général du Canada Ottawa, Ontario	POUR LE DEMANDEUR
Blakes Law Firm Ottawa, Ontario	AMICUS CURIAE