

**COUR SUPRÊME DU CANADA**

|  |  |
| --- | --- |
| **Référence :** R. *c.* Société TELUS Communications, 2013 CSC 16, [2013] 2 R.C.S. 3 | **Date :** 20130327  **Dossier :** 34252 |

Entre :

Société TELUS Communications

Appelante

et

Sa Majesté la Reine

Intimée

- et -

Procureur général de l’Ontario, Association canadienne des libertés civiles et Clinique d’intérêt public et de politique d’Internet du Canada Samuelson-Glushko

Intervenants

**Traduction française officielle**

**Coram :** La juge en chef McLachlin et les juges LeBel, Fish, Abella, Cromwell, Moldaver et Karakatsanis

|  |  |
| --- | --- |
| **Motifs de jugement :**  (par. 1 à 46)  **Motifs concordants en partie et quant au résultat :**  (par. 47 à 108)  **Motifs dissidents :**  (par. 109 à 196) | La juge Abella (avec l’accord des juges LeBel et Fish)  Le juge Moldaver (avec l’accord de la juge Karakatsanis)  Le juge Cromwell (avec l’accord de la juge en chef McLachlin) |

R. *c.* Société TELUS Communications, 2013 CSC 16, [2013] 2 R.C.S. 3

Société TELUS Communications Appelante

c.

Sa Majesté la Reine Intimée

et

Procureur général de l’Ontario, Association canadienne

des libertés civiles et Clinique d’intérêt public et de

politique d’Internet du Canada Samuelson‑Glushko Intervenants

**Répertorié : R. *c.* Société** TELUS Communications

2013 CSC 16

No du greffe : 34252.

2012 : 15 octobre; 2013 : 27 mars.

Présents : La juge en chef McLachlin et les juges LeBel, Fish, Abella, Cromwell, Moldaver et Karakatsanis.

en appel de la cour supérieure de justice de l’ontario

*Droit criminel — Interception de communications — Mandat général — Messages textes stockés brièvement dans la base de données informatique d’une société de télécommunications par suite de la procédure particulière qu’elle applique pour les transmettre — Mandat général obligeant la société de télécommunications à communiquer prospectivement, sur une base quotidienne, tous les messages textes envoyés et reçus par deux abonnés — Le mandat général prévu à l’art. 487.01 du Code criminel peut‑il autoriser la communication prospective de futurs messages textes se trouvant dans l’ordinateur d’un fournisseur de services? — La technique d’enquête autorisée par le mandat général délivré en l’espèce constitue‑t‑elle une interception qui doit être autorisée en vertu de la partie VI du Code criminel? — Un mandat général peut‑il être délivré à bon droit lorsqu’une disposition législative en vigueur traite du contenu de la technique d’enquête, sinon de sa forme précise? — Code criminel, L.R.C. 1985, ch. C‑46, art. 487.01.*

Contrairement à la plupart des fournisseurs de services de télécommunications, la Société TELUS Communications a pour pratique de copier électroniquement tous les messages textes envoyés ou reçus par ses abonnés et de les conserver brièvement dans une base de données. En l’espèce, les policiers ont obtenu, en vertu des art. 487.01 et 487.02 respectivement du *Code criminel*, un mandat général et une ordonnance d’assistance connexe obligeant Telus à fournir aux policiers copie de tous les messages textes envoyés ou reçus par deux de ses abonnés et se trouvant dans sa base de données. L’extrait pertinent du mandat obligeait Telus à produire pendant deux semaines, sur une base quotidienne, tous les messages envoyés ou reçus. Telus a demandé l’annulation du mandat général, soutenant que la prise de connaissance prospective, sur une base quotidienne, de messages textes se trouvant dans sa base de données constitue une interception de communications privées et doit, en conséquence, être autorisée en vertu des dispositions de la partie VI du *Code* relatives à l’autorisation d’écoute électronique. La demande a été rejetée. Le pourvoi soulève la question de savoir si la communication prospective de futurs messages textes se trouvant dans l’ordinateur d’un fournisseur de services peut être autorisée en vertu du mandat général.

*Arrêt* (la juge en chef McLachlin et le juge Cromwell sont dissidents) : Le pourvoi est accueilli et le mandat général ainsi que l’ordonnance d’assistance connexe sont annulés.

*Les* juges LeBel, Fish et Abella : La partie VI du *Code criminel* instaure un régime complet d’« autorisation d’écoute électronique » en vue de l’interception de communications privées. La partie VI a pour objet de restreindre la capacité des policiers d’obtenir et de divulguer des communications privées.

Telus applique pour transmettre des messages textes une procédure particulière qui fait que ces messages sont stockés brièvement dans sa base de données informatique. Pour décider si la partie VI s’applique à la communication prospective, sur une base quotidienne, de futurs messages textes stockés dans l’ordinateur de Telus, il nous faut tenir compte de l’objectif général de cette partie VI.

La messagerie texte est, essentiellement, une conversation électronique. Les différences techniques intrinsèques des nouvelles technologies ne devraient pas déterminer l’étendue de la protection accordée aux communications privées. La seule distinction entre la messagerie texte et les communications orales traditionnelles réside dans le processus de transmission. Cette distinction ne devrait pas avoir pour effet de priver les messages textes des mesures de protection des communications privées auxquelles ces messages ont droit sous le régime de la partie VI.

L’article 487.01 du *Code*, qui prévoit le mandat général, a été édicté en 1993 dans le cadre d’une série de modifications apportées au *Code* par le projet de loi C‑109, L.C. 1993, ch. 40. Il habilite un juge à décerner un mandat général autorisant un agent de la paix à « utiliser un dispositif ou une technique ou une méthode d’enquête, ou à accomplir tout acte qui y est mentionné, qui constituerait sans cette autorisation une fouille, une perquisition ou une saisie abusive ». L’alinéa 487.01(1)*c*) prévoit notamment que le pouvoir d’accorder un mandat général a un caractère résiduel et que son utilisation est interdite dans le cas où une autre disposition du *Code* ou d’une autre loi fédérale permet à un juge d’autoriser l’utilisation du dispositif, de la technique ou de la méthode proposé ou encore l’accomplissement de l’acte envisagé.

L’alinéa 487.01(1)*c*) doit être interprété largement de sorte que le mandat général ne soit pas utilisé comme mesure de premier recours, afin d’éviter que les autorités se soustraient aux exigences plus spécifiques ou rigoureuses en matière d’autorisation préalable, comme celles que l’on trouve à la partie VI. Il est nécessaire d’interpréter le terme « intercepter » à la partie VI afin de déterminer si l’al. 487.01(1)*c*) s’applique, c’est‑à‑dire si une autre disposition prévoit l’autorisation demandée. Le mot « intercepter » est utilisé dans toute la partie VI et se rapporte à l’interception de *communications privées*. Il faut par conséquent interpréter l’expression « intercepter une communication privée » en tenant compte de la vaste portée de la partie VI, du fait qu’elle s’applique à différentes plateformes technologiques, ainsi que de son objectif, à savoir la protection du droit individuel à la vie privée en matière de communication au moyen de garanties particulièrement strictes. Cette interprétation ne doit pas être dictée par le moyen technologique qui est employé pour transmettre de telles communications, par exemple l’ordinateur utilisé en l’espèce, mais plutôt par les aspects que le législateur a voulu protéger au moyen des dispositions de la partie VI. Cette interprétation doit se fonder aussi sur les droits garantis par l’art. 8 de la *Charte*, lesquels doivent progresser au rythme de la technologie.

Le fait d’interpréter de manière formaliste le mot « intercepter » aurait essentiellement pour effet de rendre la partie VI inutile en matière de protection du droit à la vie privée dans le cas des nouveaux moyens technologiques de communication textuelle électronique qui génèrent et sauvegardent des copies des communications privées dans le cadre du processus de transmission. Une interprétation étroite est en outre incompatible avec la formulation et l’objet de la partie VI qui accorde une protection étendue aux communications privées contre les ingérences non autorisées de l’État.

Il faut par conséquent interpréter les mots « intercepter une communication privée » en s’attachant à la prise de connaissance du contenu informationnel de la communication et aux attentes qu’avaient les interlocuteurs en matière de respect de la vie privée au moment de cette communication. Dans la mesure où le sens formaliste du mot « intercepter » pourrait comporter intrinsèquement un aspect temporel, cela ne devrait pas faire obstacle à l’intention du législateur de protéger, dans l’application de la partie VI, le droit des gens au respect de leur vie privée en matière de communications. L’emploi du mot « intercepter » implique que la prise de connaissance de la communication privée se fait au cours du processus de transmission. Ce processus englobe toutes les activités du fournisseur de services qui sont nécessaires ou accessoires à la fourniture du service de communication. La prise de connaissance de la substance d’une communication privée se trouvant dans un ordinateur exploité par un fournisseur de services de télécommunications ferait, en conséquence, partie de ce processus.

Les messages textes constituent des communications privées et, même s’ils sont stockés dans l’ordinateur d’un fournisseur de services, la communication prospective de futurs messages de cette nature doit être autorisée en vertu de la partie VI du *Code*. Si Telus n’exploitait pas une base de données informatique, il ne fait aucun doute que les policiers seraient tenus d’obtenir une autorisation en vertu de la partie VI afin de recevoir prospectivement communication de messages textes, et ce, sur une base continue en l’espèce. La plupart des fournisseurs de services de transmission ne copient pas systématiquement les messages textes dans une base de données. Par conséquent, si la personne ciblée par les policiers était desservie par un fournisseur différent, ces derniers devraient nécessairement obtenir des autorisations d’écoute électronique sous le régime de la partie VI pour contraindre ce fournisseur à leur communiquer de façon prospective et continue les messages textes. Cette situation crée une injustice flagrante pour les personnes qui ne réalisent vraisemblablement pas que le choix de leur fournisseur de services de télécommunications peut avoir de sérieuses répercussions sur leur vie privée. Les différences techniques inhérentes à la procédure de transmission des messages textes propre à Telus ne devraient pas priver les abonnés de cette dernière des mesures de protection prévues par le *Code* et auxquelles ont droit tous les autres Canadiens.

Le mandat général en l’espèce était invalide parce que les policiers n’avaient pas respecté la condition prévue par l’al. 487.01(1)*c*) du *Code*, à savoir qu’un mandat général ne peut être décerné si une autre disposition du *Code* permet d’autoriser la technique utilisée par les policiers. Comme le mandat entend autoriser l’interception de communications privées et que les interceptions de ce genre sont régies par le régime de la partie VI, un mandat général ne pouvait être délivré.

*Les* juges Moldaver et Karakatsanis : Il y a accord avec la juge Abella pour dire que la police n’a droit d’obtenir un mandat général que si elle est à même de démontrer qu’« aucune disposition » du *Code criminel* ou d’une autre loi fédérale n’autorise le recours à la technique, ou à un procédé équivalent en substance à la technique, pour laquelle l’autorisation est demandée. La technique d’enquête en l’espèce était équivalente sur le plan du fond à une interception. Par conséquent, le mandat général est invalide. Il n’est pas nécessaire de déterminer si ce qui s’est produit en l’espèce était ou non, à proprement parler, une « interception » au sens de l’art. 183 du *Code criminel*. Un motif de décision plus restreint nous met à l’abri des conséquences imprévues et incalculables dans ce domaine complexe du droit.

L’issue de l’espèce repose sur le défaut des autorités d’établir la condition prévue à l’al. 487.01(1)*c*) qu’il n’y ait « aucune disposition » permettant la fouille ou la perquisition. Cette disposition fait en sorte que le mandat général est utilisé avec modération et de façon limitée. En créant le mandat général, le législateur n’a pas supprimé les autres autorisations de fouille et de perquisition du *Code criminel* pour laisser aux juges le soin de concevoir les mandats généraux de façon ponctuelle comme ils l’entendent. Par conséquent, les tribunaux doivent veiller à combler le vide législatif uniquement lorsque le législateur n’a pas prévu une autorisation de fouille ou de perquisition en particulier. La condition qu’il n’y ait « aucune disposition » doit être interprétée de façon à accorder à la police la souplesse envisagée par le législateur lorsqu’il a créé le mandat général, tout en empêchant son utilisation abusive. Il est nécessaire de resserrer l’examen judiciaire lorsque le législateur a prévu une autorisation pour une technique d’enquête qui correspond, sur le plan du fond, à ce que la police cherche à obtenir, mais qui requiert des conditions préalables plus strictes. Par conséquent, le critère fondé sur l’al. 487.01(1)*c*) exige la prise en compte de la technique d’enquête que la police cherche à utiliser en fonction de son fond réel et non simplement de sa forme.

L’approche à l’égard de la condition qu’il n’y ait « aucune disposition » accepte un certain degré d’incertitude en chargeant les juges d’examiner au fond les techniques d’enquête censément « nouvelles ». En cas d’incertitude, la police ferait bien de pécher par excès de prudence. Le mandat général ne peut être utilisé pour contourner d’autres dispositions applicables en matière d’autorisation, mais qui comportent des conditions préalables plus exigeantes. Les juges saisis d’une demande relative à une technique d’enquête qui, bien que non identique, s’apparente du point de vue du fond à une technique d’enquête prévue par une autre disposition pour laquelle des normes plus rigoureuses s’appliquent devraient redoubler de prudence. Si un examen minutieux établit qu’une technique d’enquête proposée, bien que similaire, est différente, sur le plan du fond,d’une technique existante, les juges peuvent accorder le mandat général en tenant compte de l’obligation que leur impose le par. 487.01(3) de fixer des modalités qui reflètent la nature du droit à la protection de la vie privée en jeu.

L’interprétation littérale de l’al. 487.01(1)*c*) doit être rejetée. Une telle interprétation vide la disposition de tout sens et lui fait perdre pratiquement toute valeur. L’historique législatif confirme que les mandats généraux devaient jouer un rôle modeste, en offrant à la police une voie constitutionnelle pour recourir à des techniques d’enquête que le législateur n’avait pas abordées. Veiller à ce que le recours aux mandats généraux soit limité constitue le véritable objet de l’al. 487.01(1)*c*). Bien que l’exigence que le mandat serve « au mieux » l’administration de la justice prévue à l’al. 487.01(1)*b*) vise à empêcher le recours abusif au mandat général, cette disposition ne devrait pas être interprétée comme englobant la question analytique distincte que pose le critère exigeant qu’il n’y ait « aucune disposition ». Une interprétation téléologique de l’al. 487.01(1)*c*) n’a rien à voir avec une nécessité pour l’enquête. Suivant la condition qu’il n’y ait « aucune disposition », la police n’est pas tenue de démontrer pourquoi une autre autorisation ne serait pas praticable au regard des faits d’une affaire en particulier, mais plutôt pourquoi elle est différente sur le plan du fond des autorisations déjà prévues par le législateur.

En l’espèce, le mandat général est invalide parce que la technique d’enquête qu’il autorisait était équivalente sur le fond à une interception. Ce que la police a fait — obtenir l’autorisation prospective de se faire transmettre des communications privées futures de façon continue, sinon constante, pendant une période prolongée — équivalait au fond à ce qu’elle aurait fait conformément à une autorisation visée à la partie VI. Cette transmission équivalait donc, à tout le moins, à une interception. Même si aucun élément de preuve ne laisse entendre que la police a agi autrement que de bonne foi, elle ne s’est pas acquittée de son fardeau de démontrer que la technique contestée était différente sur le plan du fond d’une interception. D’après les faits de l’espèce, le mandat général n’a servi qu’à éviter la rigidité de la partie VI. La police aurait pu et aurait dû demander une autorisation sous le régime de la partie VI.

*La* juge en chef McLachlin et le juge Cromwell (dissidents) : La question de savoir si ce que la police a fait en vertu du mandat général constitue l’interception de communications privées relève de l’interprétation de la loi. À la lecture des dispositions législatives dans leur contexte intégral, il est clair que le mandat général ne permet pas une interception nécessitant une autorisation sous le régime de la partie VI. Si un message texte est incontestablement une communication privée et s’il est tout aussi incontestable que Telus a intercepté des messages textes au moyen d’un dispositif électromagnétique, acoustique, mécanique ou autre, la police, en l’espèce, n’a pas intercepté ces messages lorsque Telus lui a remis copie des messages envoyés et reçus qu’elle avait préalablement interceptés et stockés dans ses bases de données. Par conséquent, la technique d’enquête autorisée en l’espèce par le mandat général n’est pas une interception de communications privées.

La distinction entre *l’interception* de communications privées et *la divulgation, l’utilisation ou la conservation* de communications privées qui ont été interceptées est fondamentale pour ce qui est de l’objet des dispositions relatives à l’écoute électronique et du régime qu’elles établissent. L’objet, le texte et le régime de la partie VI montrent que la divulgation, l’utilisation ou la conservation de communications privées interceptées sont distinctes de l’interception elle‑même. En effet, si la divulgation ou l’utilisation d’une communication privée en constituait l’interception, il n’aurait pas été nécessaire de les ériger en infraction distincte. De la même façon, les exonérations de responsabilité criminelle prévues par le législateur indiquent qu’il a établi une distinction entre l’interception, d’une part, et la conservation, l’utilisation et la divulgation, d’autre part.

En l’espèce, nul ne conteste que Telus interceptait les messages textes lorsqu’elle les copiait pour les besoins de gestion de ses propres systèmes. Cela dit, il est pareillement reconnu que Telus a licitement intercepté des communications privées. En vertu du mandat général, la police a demandé à Telus la divulgation de renseignements que Telus avait déjà légalement interceptés. Le mandat général n’obligeait pas Telus à intercepter des communications, mais à fournir copie de communications qu’elle avait déjà interceptées à des fins licites qui lui étaient propres. Comme l’indique clairement le régime législatif, la divulgation ou l’utilisation de communications interceptées légitimement ne constituent pas une interception. La conclusion que la police interceptait des communications privées en recevant de Telus des copies de messages textes déjà interceptés et stockés est incompatible avec la distinction fondamentale qu’établit le texte de loi. La distinction que fait la loi entre l’interception et la divulgation ne peut pas être qualifiée de simple « différence technique ». Elle constitue un élément fondamental du régime créé par les dispositions en cause. Lorsque Telus remet à la police les copies de communications déjà interceptées, elle les divulgue, elle ne les intercepte pas à nouveau. Cette divulgation par Telus de données stockées dans ses bases de données ne peut pas constituer une interception par la police.

On n’intercepte pas des communications déjà interceptées et stockées en en prenant connaissance, parce qu’une telle interprétation large est incompatible avec la nette distinction que font les dispositions législatives entre interception et divulgation. L’application générale de cette interprétation de « prendre volontairement connaissance » élargirait bien au‑delà de tout ce qui a déjà pu être envisagé le champ des techniques d’enquête nécessitant une autorisation d’écoute électronique. En outre, introduire un aspect temporel à la notion d’interception confond l’acte d’intercepter et la nature de son autorisation. L’interception est une technique, une façon de prendre connaissance de la substance d’une communication privée. La même technique, donnant connaissance de l’information sous la même forme, ne peut pas constituer soit une saisie de renseignements stockés, soit une interception, selon le moment où elle est autorisée.

Le mandat général n’est pas une autorisation qu’il faut utiliser de façon limitée et avec modération. Au contraire, cette disposition est formulée en termes larges, ainsi que le signalent de nombreux auteurs. Par conséquent, la prémisse voulant que cet article doive être interprété de façon à en restreindre sévèrement l’utilisation est rejetée. L’examen porte sur deux points (outre, bien sûr, les motifs raisonnables de croire qu’une infraction a été commise et que l’autorisation demandée permettra d’obtenir des renseignements la concernant) : l’autorisation porte‑t‑elle sur l’utilisation d’« un dispositif ou une technique ou une méthode d’enquête » ou « l’accomplissement d’un acte » prévu par une autre disposition législative fédérale, et sert‑elle au mieux l’administration de la justice? L’alinéa 487.01(1)*c*) prévoit qu’un mandat général peut être décerné « s’il n’y a aucune disposition [. . .] qui prévoie un mandat, une autorisation ou une ordonnance permettant une telle utilisation [d’un dispositif, d’une technique ou d’une méthode d’enquête] ou l’accomplissement d’un tel acte ». Les mots « une telle utilisation [d’un dispositif, d’une technique ou d’une méthode d’enquête] » et « l’accomplissement d’un tel acte » renvoient tous à *ce que* la police veut faire, non aux *raisons* motivant ce choix. Cet alinéa n’exige pas que le juge saisi examine s’il existe des techniques analogues et si elles permettent d’obtenir les mêmes éléments de preuve, mais simplement si *une telle utilisation* peut être autorisée par une autre disposition. Il ne s’agit pas simplement d’une interprétation étroite et littérale de l’art. 487.01. Il s’agit plutôt d’une interprétation qui rend compte de son objet : l’octroi au juge du vaste pouvoir discrétionnaire d’autoriser la police « à utiliser un dispositif ou une technique ou une méthode d’enquête, ou à accomplir tout acte », pourvu, naturellement, que le juge soit convaincu que l’autorisation sert au mieux l’administration de la justice après avoir accordé l’importance voulue à la protection constitutionnelle contre les fouilles, perquisitions et saisies abusives. Un juge ne devrait toutefois pas autoriser tout ce que la police cherche à faire simplement parce que l’autorisation n’est pas prévue par un autre texte législatif. Son pouvoir discrétionnaire de décerner le mandat doit s’exercer en donnant pleinement effet à la protection des attentes raisonnables en matière de vie privée, comme l’établit l’art. 8 de la *Charte*.

L’inclusion à l’al. 487.01(1)*c*) d’un critère de « l’équivalent sur le plan du fond » n’est étayée ni par le texte de cette disposition, ni par son objet, ni par la jurisprudence. La question posée par cet alinéa est simple : Est‑ce qu’une loi fédérale prévoit « un mandat, une autorisation ou une ordonnance permettant une telle utilisation ou l’accomplissement d’un tel acte »? Lorsque cette condition préalable est respectée, le juge peut envisager d’accorder l’autorisation demandée. La question de savoir *s’il y a lieu* d’accorder l’autorisation demandée ne relève pas de cet alinéa. Pour déterminer s’il y a lieu de décerner un mandat général, il faut plutôt se tourner vers l’al. 487.01(1)*b*), lequel pose la question de savoir si la délivrance du mandat général servirait au mieux l’administration de la justice. Non seulement le texte et l’objet de la disposition de même que la jurisprudence étayent‑ils une telle approche, mais l’application d’un critère de « l’équivalent sur le plan du fond » engendre une incertitude inutile et détourne le juge de la question de la compatibilité de la technique visée par la demande d’autorisation avec le droit à la protection contre les fouilles, perquisitions et saisies abusives. La prévisibilité et la clarté du droit revêtent une importance particulière en matière d’autorisation judiciaire préalable de fouilles et de perquisitions. L’autorisation préalable n’a pas pour but premier de détecter après le fait des fouilles ou perquisitions abusives, mais d’en prévenir l’existence. Les exigences en matière d’autorisation préalable doivent être aussi claires que possible pour assurer l’entière protection du droit garanti par la *Charte*.

La technique visée par la demande d’autorisation en l’espèce n’équivaut pas fondamentalement à l’autorisation de l’écoute électronique. Vu les faits de la présente espèce, l’autorisation d’écoute électronique seule ne permettrait pas à la police d’obtenir les renseignements que Telus devait fournir en exécution du mandat général. Il faudrait trois autorisations distinctes pour que la police ait accès à l’information qu’elle recevrait grâce au mandat général.  Ainsi, même si l’on acceptait l’ajout par interprétation, à l’al. 487.01(1)*c*), d’un critère de « l’équivalent sur le plan du fond », ni les faits ni le droit n’étayent son application en l’espèce.

La demande de la police visant à obtenir un mandat général en l’espèce n’était pas une façon de contourner les exigences de la partie VI. Le mandat général permettait l’atteinte des objectifs légitimes de l’enquête policière de façon beaucoup plus pratique et économique que ce qui aurait pu être autorisé en vertu de toute autre disposition. Il n’y a aucune preuve de « recours abusif » à l’art. 487.01. Un service de police municipal de taille plutôt réduite a mené une enquête de façon efficace et pratique, en respectant pleinement le droit à la vie privée des personnes visées par l’enquête ainsi que des autres abonnés de Telus.

**Jurisprudence**

Citée par la juge Abella

**Arrêts mentionnés :** *R. c. Ha*, 2009 ONCA 340, 96 O.R. (3d) 751; *R. c. Brand*, 2008 BCCA 94, 229 C.C.C. (3d) 443 (*sub nom. R. c. Ford*); *R. c. Welsh and Iannuzzi (No. 6)* (1977), 32 C.C.C. (2d) 363; *Lyons c. La Reine*, [1984] 2 R.C.S. 633; *R. c. Araujo*, 2000 CSC 65, [2000] 2 R.C.S. 992; *R. c. Tse*, 2012 CSC 16, [2012] 1 R.C.S. 531; *R. c. Wong*, [1990] 3 R.C.S. 36; *Société canadienne des auteurs, compositeurs et éditeurs de musique c. Assoc. canadienne des fournisseurs Internet*, 2004 CSC 45, [2004] 2 R.C.S. 427.

Citée par le juge Moldaver

**Arrêts mentionnés :** *R. c. Wong*, [1990] 3 R.C.S. 36; *R. c. Ha*, 2009 ONCA 340, 96 O.R. (3d) 751; *Lyons c. La Reine*, [1984] 2 R.C.S. 633; *R. c. Brand*, 2008 BCCA 94, 229 C.C.C. (3d) 443 (*sub nom. R. c. Ford*); *Schreiber c. Canada (Procureur général)*, [1997] 2 C.F. 176, inf. par [1998] 1 R.C.S. 841; *R. c. Araujo*, 2000 CSC 65, [2000] 2 R.C.S. 992.

Citée par le juge Cromwell (dissident)

*Société Télé‑Mobile c. Ontario*, 2008 CSC 12, [2008] 1 R.C.S. 305; *R. c. Cole*, 2012 CSC 53, [2012] 3 R.C.S. 34; *R. c. Jones*, 2011 ONCA 632, 107 O.R. (3d) 241; *R. c. Bahr*, 2006 ABPC 360, 434 A.R. 1; *R. c. Cross*, 2007 CanLII 64141; *R. c. Little*,2009 CanLII 41212; *R. c. Tse*, 2008 BCSC 906 (CanLII); *R. c. Weir*, 2001 ABCA 181, 281 A.R. 333; *R. c. Ha*, 2009 ONCA 340, 96 O.R. (3d) 751, autorisation d’appel refusée, [2009] 3 R.C.S. vii; *R. c. Lauda* (1998), 37 O.R. (3d) 513, conf. par [1998] 2 R.C.S. 683; *R. c. Noseworthy* (1997), 33 O.R. (3d) 641; *R. c. Brand*, 2008 BCCA 94, 229 C.C.C. (3d) 443 (*sub nom. R. c. Ford*); *R. c. Araujo*, 2000 CSC 65, [2000] 2 R.C.S. 992.

**Lois et règlements cités**

*Charte canadienne des droits et libertés*, art. 8, 24(2).

*Code criminel*, L.R.C. 1985, ch. C‑46, partie VI, art. 183 « communication privée », « intercepter », 184, 184.4, 185, 186, 189, 193, 195, 196, 487, 487.01 [aj. 1993, ch. 40, art. 15], 487.012, 487.02, 492.2(1), (2).

*Loi d’interprétation*, L.R.C. 1985, ch. I‑21, art. 35 « télécommunication » [mod. 1993, ch. 38, art. 87].

*Loi modifiant le Code criminel, la Loi sur la responsabilité civile de l’État et le contentieux administratif et la Loi sur la radiocommunication*, L.C. 1993, ch. 40 (projet de loi C-109).

*Loi sur la protection de la vie privée*, S.C. 1973‑74, ch. 50.

Projet de loi C‑30, *Loi sur la protection des enfants contre les cyberprédateurs*, 1re sess., 41e lég., 2011-2012 (Première lecture le 14 février 2012).

Projet de loi C‑55, *Loi donnant suite à la décision de la Cour suprême du Canada dans l’affaire R. c. Tse*, 1re sess., 41e lég., 2011-2012-2013 (Première lecture le 11 février 2013).

Projet de loi C‑176, *Loi sur la protection de la vie privée*, 1re sess., 29e lég., 1973, Notes explicatives.

**Doctrine et autres documents cités**

Coughlan, Steve. « *R. v. Ha* : Upholding General Warrants without Asking the Right Questions » (2009), 65 C.R. (6th) 41.

Fontana, James A., and David Keeshan. *The Law of Search and Seizure in Canada*, 8th ed. Markham, Ont. : LexisNexis, 2010.

Hutchison, Scott C. *Hutchison’s Canadian Search Warrant Manual 2005 : A Guide to Legal and Practical Issues Associated with Judicial Pre‑Authorization of Investigative Techniques*, 2nd ed. Toronto : Thomson Carswell, 2004.

Hutchison, Scott C., et al.  *Search and Seizure Law in Canada*, vol. 1. Toronto : Carswell, 2005 (loose‑leaf updated 2012, release 7).

Sullivan, Ruth. *Sullivan on the Construction of Statutes*, 5th ed. Markham, Ont. : LexisNexis, 2008.

Watt, David. *Law of Electronic Surveillance in Canada*. Toronto : Carswell, 1979.

POURVOI contre une décision de la Cour supérieure de justice de l’Ontario (le juge Sproat), 2011 ONSC 1143, 105 O.R. (3d) 411, [2011] O.J. No. 974 (QL), 2011 CarswellOnt 1331, qui a confirmé la validité d’un mandat général et d’une ordonnance d’assistance connexe. Pourvoi accueilli, la juge en chef McLachlin et le juge Cromwell sont dissidents.

Scott C. Hutchison, Michael Sobkin et *Fredrick Schumann*, pour l’appelante.

Croft Michaelson et Lisa Matthews, pour l’intimée.

Michal Fairburn, pour l’intervenant le procureur général de l’Ontario.

Wendy Matheson et Rebecca Wise, pour l’intervenante l’Association canadienne des libertés civiles.

Argumentation écrite seulement par Tamir Israel, pour l’intervenante la Clinique d’intérêt public et de politique d’Internet du Canada Samuelson‑Glushko.

Version française du jugement des juges LeBel, Fish et Abella rendu par

1. La juge Abella — Pour bon nombre de Canadiennes et de Canadiens, la messagerie texte est devenue une forme de communication de plus en plus populaire. Malgré certaines différences technologiques, elle présente plusieurs caractéristiques de la communication orale traditionnelle : elle se veut un moyen de conversation, la transmission du message est généralement instantanée et l’on s’attend à ce que la communication demeure privée. La question en litige dans le présent pourvoi consiste à déterminer la procédure qui doit être appliquée par les tribunaux, en vertu du *Code criminel*, L.R.C. 1985, ch. C‑46, pour autoriser la communication prospective, sur une base quotidienne, de tels messages se trouvant dans une base de données informatique exploitée par un fournisseur de services de télécommunications.
2. En l’espèce, le fournisseur de services concerné est la Société TELUS Communications. Cette dernière invite la Cour à conclure que la prise de connaissance volontaire prospective, sur une base quotidienne, de messages textes se trouvant dans sa base de données constitue une interception de communications privées et doit, en conséquence, être autorisée en vertu de la partie VI du *Code*, laquelle instaure un régime complet d’« autorisation d’écoute électronique » en vue de l’interception de communications privées. Le ministère public soutient pour sa part que l’extraction de messages d’un ordinateur exploité par un fournisseur de services ne relève pas de la partie VI, parce que la production de messages stockés sur ordinateur ne constitue pas une « interception », et que les policiers peuvent par conséquent invoquer le mandat général prévu à l’art. 487.01 du *Code* pour être autorisés à obtenir copie de messages textes.
3. La partie VI du *Code* établit un régime de protection des communications privées. Par suite de la procédure particulière que Telus applique pour transmettre des messages textes, ces messages sont stockés brièvement dans sa base de données informatique. La question qui se pose en l’espèce consiste à décider si, en raison des différences techniques inhérentes à la procédure de transmission des messages textes propre à Telus, les abonnés de cette dernière devraient être privés des mesures de protection prévues par le *Code* et auxquelles ont droit tous les autres Canadiens.
4. Le nœud du présent pourvoi réside donc dans l’interprétation du mot « intercepter » utilisé à la partie VI. Dans toute cette partie, ce mot se rapporte à l’interception de *communications privées*. Il faut par conséquent interpréter l’expression « intercepter une communication privée » en tenant compte de la vaste portée de la partie VI, du fait qu’elle s’applique à différentes plateformes technologiques ainsi que de son objectif, à savoir la protection du droit individuel à la vie privée en matière de communication au moyen de garanties particulièrement strictes. Cette interprétation ne doit pas être dictée par le moyen technologique qui est employé pour transmettre de telles communications, par exemple l’ordinateur utilisé en l’espèce, mais plutôt par les aspects que le législateur a voulu protéger au moyen des dispositions de la partie VI.
5. La messagerie texte est, essentiellement, une conversation électronique. La seule distinction entre la messagerie texte et les communications orales traditionnelles réside dans le processus de transmission. Cette distinction ne devrait pas avoir pour effet de priver les messages textes des mesures de protection des communications privées auxquelles ces messages ont droit sous le régime de la partie VI. Les différences techniques intrinsèques des nouvelles technologies ne devraient pas déterminer l’étendue de la protection accordée aux communications privées.

Contexte

1. Lorsqu’un abonné de Telus envoie un message texte, la transmission de ce message se déroule suivant la séquence d’opérations suivante : le message est d’abord transmis à la tour de transmission la plus proche, qui le relaie à l’infrastructure de transmission de Telus, d’où il est ensuite acheminé à la tour de transmission la plus proche du destinataire puis, enfin, au téléphone de ce dernier. Si l’appareil du destinataire est éteint ou hors de portée d’une tour de transmission, le message demeure temporairement dans l’infrastructure de transmission de Telus pendant une période maximale de cinq jours, après quoi Telus met fin aux tentatives de transmission et supprime le message sans en informer l’expéditeur.
2. Contrairement à la plupart des fournisseurs de services de télécommunications, Telus a pour pratique de copier électroniquement les messages textes envoyés ou reçus par ses abonnés et de les conserver dans une base de données pendant une période de 30 jours. Les messages textes envoyés par un abonné sont copiés dans la base de données à l’étape du processus de transmission où ils entrent dans l’infrastructure de transmission de Telus. Les messages textes que reçoit un abonné sont copiés lorsqu’ils parviennent à l’appareil de ce dernier. En raison de ce système, il arrive dans bien des cas que le message texte soit copié dans la base de données avant de parvenir à l’appareil du destinataire ou avant que ce dernier ne l’ait lu, ou les deux.
3. Le 27 mars 2010, le service de police d’Owen Sound a obtenu un mandat général en vertu de l’art. 487.01, ainsi qu’une ordonnance d’assistance connexe en vertu de l’art. 487.02 du *Code*. Le mandat désignait deux abonnés des services mobiles de Telus et obligeait cette entreprise à fournir aux policiers copie de tous les messages textes envoyés ou reçus par ces abonnés qui étaient conservés dans la base de données de Telus. Le mandat exigeait en outre la production de renseignements relatifs aux abonnés permettant d’identifier toute personne ayant envoyé des messages textes aux deux personnes visées par le mandat ou ayant reçu de tels messages de ces personnes.
4. Le mandat visait une période subséquente de deux semaines allant du 30 mars au 16 avril 2010, période pendant laquelle Telus devait observer un calendrier de communication précis. Le 30 mars 2010, Telus devait produire les renseignements se rapportant à la période du 18 au 30 mars 2010. Au cours de chacun des 13 jours suivants, elle devait produire, sur une base quotidienne, les messages textes envoyés ou reçus pendant les 24 heures précédentes, ainsi que tout renseignement connexe relatif aux abonnés.
5. Telus a soutenu que le mandat était invalide parce que les policiers n’avaient pas respecté la condition prévue par l’al. 487.01(1)*c*) du *Code*, à savoir qu’un mandat général ne peut être décerné si une autre disposition du *Code* permet d’autoriser la technique utilisée par les policiers. Comme le mandat entendait autoriser l’interception de communications privées et que les interceptions de ce genre sont régies par le régime de la partie VI, un mandat général ne pouvait être délivré. Pour sa part, le ministère public a plaidé que l’extraction de messages de cette base de données de Telus ne relevait pas de la partie VI, puisque les copies emmagasinées dans la base de données n’étaient pas des communications en temps réel et que, de ce fait, les policiers pouvaient demander un mandat général autorisant la production de futurs messages textes stockés dans la base de données d’un fournisseur.
6. Le juge saisi de la demande a débouté Telus (2011 ONSC 1143, 105 O.R. (3d) 411). La partie du mandat visant la communication d’anciens messages antérieurs à la délivrance du mandat a été annulée, étant donné que tant le ministère public que Telus ont reconnu qu’il était possible de demander une ordonnance de communication afin d’obtenir ces messages.
7. À mon avis, les messages textes constituent des communications privées et, même s’ils sont stockés dans l’ordinateur d’un fournisseur de services, la communication prospective de futurs messages de cette nature doit être autorisée en vertu de la partie VI du *Code*.
8. Si Telus n’exploitait pas une base de données informatique, il ne fait aucun doute que les policiers seraient tenus d’obtenir une autorisation en vertu de la partie VI afin de recevoir prospectivement communication de messages textes, et ce, sur une base continue en l’espèce. En fait, la plupart des fournisseurs de services de transmission ne copient pas systématiquement les messages textes dans une base de données. Par conséquent, si la personne ciblée par les policiers était desservie par un fournisseur différent, ces derniers devraient nécessairement obtenir des autorisations d’écoute électronique sous le régime de la partie VI pour contraindre ce fournisseur à leur communiquer de façon prospective et continue de futurs messages textes. Cette situation crée une injustice flagrante pour les personnes qui ne réalisent vraisemblablement pas que le choix de leur fournisseur de services de télécommunications peut avoir de sérieuses répercussions sur leur vie privée.
9. Je suis donc d’avis d’accueillir le pourvoi et d’annuler le mandat général et l’ordonnance d’assistance connexe.

Analyse

1. Il ne nous a pas été demandé de décider si un mandat général peut autoriser la communication de messages textes existants ou encore d’examiner l’application et la validité de la disposition régissant les ordonnances de communication en ce qui concerne les communications privées. Le présent pourvoi soulève plutôt la question de savoir si la communication *prospective* de futurs messages textes se trouvant dans l’ordinateur d’un fournisseur de services peut être autorisée en vertu du mandat général prévu à l’art. 487.01 du *Code*. Cela signifie que nous n’avons pas besoin de décider si la saisie de ces messages textes constituerait une interception si elle était autorisée après leur stockage.
2. Édicté en 1993, l’art. 487.01 faisait partie d’une série de modifications apportées au *Code* par le projet de loi C‑109, L.C. 1993, ch. 40. Ce projet de loi a instauré plusieurs nouvelles dispositions en matière d’autorisation judiciaire. L’article 487.01 a pour objectif de permettre l’obtention de mandats de perquisition à l’égard de techniques ou méthodes non précisées dans le *Code*. Il habilite un juge à décerner un mandat général autorisant un agent de la paix à « utiliser un dispositif ou une technique ou une méthode d’enquête, ou à accomplir tout acte qui y est mentionné, qui constituerait sans cette autorisation une fouille, une perquisition ou une saisie abusive » :

**487.01**(1)  Un juge de la cour provinciale, un juge de la cour supérieure de juridiction criminelle ou un juge au sens de l’article 552 peut décerner un mandat par écrit autorisant un agent de la paix, sous réserve du présent article, à utiliser un dispositif ou une technique ou une méthode d’enquête, ou à accomplir tout acte qui y est mentionné, qui constituerait sans cette autorisation une fouille, une perquisition ou une saisie abusive à l’égard d’une personne ou d’un bien :

*a*)  si le juge est convaincu, à la suite d’une dénonciation par écrit faite sous serment, qu’il existe des motifs raisonnables de croire qu’une infraction à la présente loi ou à toute autre loi fédérale a été ou sera commise et que des renseignements relatifs à l’infraction seront obtenus grâce à une telle utilisation ou à l’accomplissement d’un tel acte;

*b*)  s’il est convaincu que la délivrance du mandat servirait au mieux l’administration de la justice;

*c*)  *s’il n’y a aucune disposition dans la présente loi ou toute autre loi fédérale qui prévoie un mandat, une autorisation ou une ordonnance permettant une telle utilisation ou l’accomplissement d’un tel acte.*

1. La solution du présent pourvoi dépend de la question de savoir si l’al. 487.01(1)*c*) s’applique à la présente situation, en d’autres mots s’il existe une autre disposition permettant d’obtenir l’autorisation qui est sollicitée en l’espèce. Dans *R. c. Ha*, 2009 ONCA 340, 96 O.R. (3d) 751, le juge MacPherson a fait remarquer que l’analyse fondée sur l’al. 487.01(1)*c*) s’attache à [traduction] « la technique ou méthode d’enquête particulière que la police veut utiliser et à la question de savoir si cette technique ou méthode peut être autorisée par une autre disposition du Code ou d’une autre loi fédérale » (par. 43; voir aussi *R. c. Brand*, 2008 BCCA 94, 229 C.C.C. (3d) 443 (*sub nom.* *R. c. Ford*), par. 50).
2. Par conséquent, il ressort d’un examen contextuel de l’al. 487.01(1)*c*) que le pouvoir d’accorder un mandat général a un caractère résiduel et que son utilisation est *interdite* dans le cas où une autre disposition du *Code* ou d’une autre loi fédérale permet à un juge d’autoriser l’utilisation du dispositif, de la technique ou de la méthode proposé ou encore l’accomplissement de l’acte envisagé.
3. Autrement dit, l’al. 487.01(1)*c*) doit être interprété largement de sorte que le mandat général ne soit pas utilisé comme mesure de premier recours. Il a pour but d’éviter que les autorités se soustraient aux exigences plus spécifiques ou rigoureuses en matière d’autorisation préalable (S. C. Hutchison et autres, *Search and Seizure Law in Canada* (feuilles mobiles), p. 16‑40.3).
4. Cela signifie que le ministère public a droit à un mandat général uniquement lorsqu’il est en mesure de prouver qu’aucune autre disposition ne prévoit un mandat, une autorisation ou une ordonnance permettant le recours à la technique en question, y compris, comme le souligne le juge Moldaver, quelque disposition autorisant des techniques équivalentes, sur le plan du fond, à celle proposée par les policiers dans une affaire donnée. La technique d’enquête autorisée par le mandat général délivré en l’espèce a permis à la police d’obtenir directement d’un fournisseur de services, et ce, chaque jour pendant une période de deux semaines, la communication prospective de futurs messages textes. L’argument du ministère public consiste essentiellement à dire qu’il était impossible de recourir à une autre disposition, étant donné que l’extraction de messages stockés ne constituait pas une interception. Si le ministère public a raison, il a droit à la délivrance d’un mandat général. S’il a tort, le mandat général qui a été délivré doit être annulé. D’une manière ou d’une autre, il est essentiel de déterminer si la technique que la police voulait employer devait être autorisée sous le régime de la partie VI.
5. Le ministère public n’a à aucun moment concédé que les circonstances de la présente espèce donnaient ouverture soit à un mandat général soit à une autorisation fondée sur la partie VI. Il a plutôt affirmé que la condition prévue à l’al. 487.01(1)*c*) était respectée, vu l’absence d’autre disposition permettant d’obtenir la communication prospective de futurs messages textes stockés dans l’ordinateur d’un fournisseur de services, la partie VI n’étant pas selon lui applicable du fait que l’extraction de messages stockés dans un ordinateur ne constitue pas une « interception ». Il s’agit là de la question centrale à trancher en l’espèce.
6. La Cour doit donc décider si la partie VI s’applique à la communication prospective — et, en l’espèce, continue — des messages textes demandés par la police ou si, du fait que ces messages sont stockés dans l’ordinateur de Telus, leur extraction ne constitue pas une « interception ». Si la partie VI s’applique, un mandat général ne peut alors être décerné, conformément à l’al. 487.01(1)*c*).
7. Aux termes du par. 184(1), constitue un acte criminel le fait d’« intercept[er] volontairement une communication privée » au moyen d’un dispositif. La partie VI établit un régime exhaustif pourvoyant à l’autorisation de telles interceptions. Ces dispositions ont été édictées en 1974 par la *Loi sur la protection de la vie privée*, S.C. 1973‑74, ch. 50, qui a modifié le *Code* en y ajoutant la partie IV.1 (aujourd’hui la partie VI) intitulée « Atteintes à la vie privée ». Le juge Zuber a expliqué ainsi l’objet de ces dispositions dans *R. c. Welsh and Iannuzzi (No. 6)* (1977), 32 C.C.C. (2d) 363 (C.A. Ont.) :

[traduction] Il est évident qu’en édictant la *Loi sur la protection de la vie privée*, 1973-74 (Can.), ch. 50, [. . .] le Parlement visait deux objectifs. Le premier était de protéger les communications privées en interdisant leur interception et en rendant inadmissible la preuve obtenue en violation de cette loi. Le second objectif, qui fait contrepoids au premier, était de reconnaître la nécessité de permettre aux autorités compétentes, sous réserve de certaines restrictions précises, d’intercepter des communications privées dans le cadre d’une enquête sur un crime grave et de produire la preuve ainsi obtenue. [p. 369]

1. Parce qu’elle a pour objet de restreindre la capacité des policiers d’obtenir et de divulguer des communications privées, la partie VI est rédigée en termes généraux afin d’assurer la protection nécessaire. Dans l’arrêt *Lyons c. La Reine*,[1984] 2 R.C.S. 633, la Cour a expliqué ainsi la portée de ces dispositions :

Il s’agit d’un texte législatif général qui vise, par ces dispositions étendues, l’utilisation de toute une gamme de dispositifs radioélectriques, téléphoniques, optiques et acoustiques pour écouter et enregistrer les communications privées dont une définition générale est donnée. Il ne s’agit ni d’un texte législatif portant sur le branchement clandestin de lignes téléphoniques ou sur l’écoute clandestine, ni d’un règlement sur la radio. Il s’agit d’une réglementation de toutes ces choses et de « tout autre dispositif » qui peut servir à intercepter des renseignements dont l’auteur peut raisonnablement s’attendre à ce qu’ils ne soient pas interceptés par une personne autre que celle à laquelle il les destine. [p. 664]

1. Suivant la définition qui en est donnée à l’art. 183, le mot « 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 ». Il s’agit là d’une définition non exhaustive, qui cadre avec la portée large de la partie VI et met l’accent sur la prise de connaissance par l’État du contenu informationnel — substance, sens ou objet — de la communication privée. Ce n’est pas seulement la communication elle‑même qui est protégée, mais aussi toute information connexe à cette communication qui permet d’en dégager la substance ou le sens. L’expression « communication privée » est définie ainsi à l’art. 183 :

*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 auteur la destine.

1. Cette définition souligne les attentes raisonnables de l’auteur de la communication en matière de respect de sa vie privée à cet égard. Le mot « télécommunication » figurant dans la définition est lui‑même défini en ces termes dans la *Loi d’interprétation*, L.R.C. 1985, ch. I‑21, art. 35, modifié en 1993 (L.C. 1993, ch. 38, art. 87) : « La transmission, l’émission ou la réception de signes, signaux, écrits, images, sons ou renseignements de toute nature soit par système électromagnétique, notamment par fil, câble ou système radio ou optique, soit par tout procédé technique semblable ».
2. Les articles 185 et 186 du *Code* énoncent les exigences générales applicables aux demandes d’autorisation présentées en vertu de la partie VI. En comparaison des conditions prévues par d’autres dispositions du *Code* se rapportant aux fouilles, saisies, perquisitions et mandats, ces articles comportent des exigences plus strictes au titre de la protection de la vie privée. Avant d’accorder une autorisation fondée sur la partie VI, le juge doit être convaincu que cette mesure sert au mieux l’administration de la justice.
3. Le juge doit également être convaincu, conformément à l’al. 186(1)*b*), que « d’autres méthodes d’enquête ont été essayées et ont échoué, ou ont peu de chance de succès, ou que l’urgence de l’affaire est telle qu’il ne serait pas pratique de mener l’enquête relative à l’infraction en n’utilisant que les autres méthodes d’enquête ». Dans *R. c. Araujo*,2000 CSC 65, [2000] 2 R.C.S. 992, la Cour a précisé que cette exigence obligeait la police à démontrer qu’il n’existait « aucune autre méthode d’enquête raisonnable dans les circonstances de l’enquête criminelle considérée » (par. 29).
4. Les autorisations décernées en vertu de la partie VI doivent aussi indiquer l’identité des personnes dont les communications privées seront interceptées, le lieu où les communications seront interceptées et la façon dont elles le seront. Les autorisations doivent également préciser les modalités que le juge estime opportunes, et elles ne sont valides que pour une période maximale de 60 jours. Enfin, la demande doit être présentée par écrit par le procureur général, le ministre de la Sécurité publique ou un mandataire spécialement désigné.
5. Outre ces conditions préalables d’autorisation, la partie VI énonce un certain nombre d’exigences en matière d’avis. L’article 196 requiert que soient « avisées », dans un certain délai, les personnes ayant fait l’objet d’interceptions autorisées en vertu de l’art. 186. Suivant l’art. 189, l’accusé doit être avisé de toute interception dont on entend présenter les fruits en preuve. De plus, l’art. 195 oblige le ministre de la Sécurité publique et de la Protection civile ou le procureur général de chaque province à établir chaque année un rapport sur l’utilisation des autorisations visées à la partie VI. Dans *R. c. Tse*,2012 CSC 16, [2012] 1 R.C.S. 531, la Cour a jugé que l’obligation de notification assure la transparence du processus et constitue une mesure de contrôle supplémentaire à l’égard du pouvoir de la police d’exécuter des interceptions très attentatoires en matière de communications privées. Elle a en conséquence conclu qu’une disposition de notification était nécessaire au respect des normes constitutionnelles minimales établies par l’art. 8 de la *Charte canadienne des droits et libertés*.
6. Ces garanties font bien ressortir l’intention du législateur d’accorder une protection plus grande aux communications privées. La partie VI s’applique largement à divers moyens technologiques et prévoit des garanties plus strictes que d’autres dispositions du *Code* en matière de mandat. Il nous faut donc tenir compte de cet objectif général pour décider si la partie VI s’applique à la communication prospective, sur une base quotidienne, de futurs messages textes stockés dans l’ordinateur de Telus.
7. Comme l’ont reconnu les parties, les messages textes sont clairement visés par la définition de « télécommunication » figurant dans la *Loi d’interprétation*.Les parties ont également reconnu que, tout comme les communications orales, ces messages surviennent dans des circonstances faisant naître une attente raisonnable en matière de respect de la vie privée et constituent, de ce fait, des « communication[s] privée[s] » au sens de l’art. 183. En outre, il ne fait pas de doute que l’ordinateur utilisé par Telus est visé par les mots « [t]out dispositif » à l’art. 183.
8. La question consiste donc à interpréter le mot « intercepter » à la partie VI. L’interprétation de ce mot doit se fonder non seulement sur les objectifs de la partie VI, mais aussi sur les droits garantis par l’art. 8 de la *Charte*, lesquels doivent progresser au rythme de la technologie. Dans *R. c. Wong*,[1990] 3 R.C.S. 36, la Cour a conclu que « le droit général à la protection contre les fouilles, les perquisitions ou les saisies abusives garanti par l’art. 8 [de la *Charte*] doit évoluer au rythme du progrès technologique et, par conséquent, nous assurer une protection constante contre les atteintes non autorisées à la vie privée par les agents de l’État, peu importe la forme technique que peuvent revêtir les divers moyens employés » (p. 44). Le fait d’interpréter de manière formaliste le mot « intercepter » aurait essentiellement pour effet de rendre la partie VI inutile en matière de protection du droit à la vie privée dans le cas des nouveaux moyens technologiques de communication textuelle électronique qui génèrent et sauvegardent des copies des communications privées dans le cadre du processus de transmission.
9. Il est vrai que, contrairement aux communications orales traditionnelles, un message texte n’est pas toujours communiqué à son destinataire au moment où il est créé. La réception d’un tel message texte suppose que le téléphone soit ouvert et se trouve à la portée d’une tour de transmission, et que le destinataire consulte le message. Si Telus ne parvient pas à transmettre un message, celui‑ci demeure dans son infrastructure de transmission pendant cinq jours, après quoi Telus met fin à ses tentatives de transmission. En outre, contrairement aux communications orales, les communications textuelles — qui sont, de par leur nature, des écrits — génèrent un document qui peut facilement être copié et conservé. Une interprétation étroite ou formaliste du mot « intercepter », qui exigerait que l’interception ait lieu en même temps que la communication elle‑même, est donc dépourvue d’utilité pour étudier les nouvelles communications textuelles électroniques.
10. Une interprétation étroite est en outre incompatible avec l’objet de la partie VI et les termes généraux qui y sont utilisés. La définition française d’« intercepter » à l’art. 183 comporte trois aspects distincts : « écouter », « enregistrer » et « prendre [. . .] connaissance ». La définition législative élargit la notion d’« intercepter » au lieu de la limiter à son sens étroit et technique. La définition de ce mot dans le *Code* n’exige aucunement que l’interception d’une communication privée s’effectue simultanément à la communication elle‑même ou sensiblement au même moment. Si le législateur avait voulu établir une telle exigence, il l’aurait fait dans la définition d’« intercepter ». Il a plutôt choisi d’adopter une définition plus générale, conforme à l’objet de la partie VI, qui consiste à accorder une protection étendue aux communications privées contre les ingérences non autorisées de l’État.
11. Il faut par conséquent interpréter les mots « intercepter une communication privée » en s’attachant à la prise de connaissance du contenu informationnel de la communication et aux attentes qu’avaient les interlocuteurs en matière de respect de la vie privée au moment de cette communication. À mon avis, dans la mesure où le sens formaliste du mot « intercepter » pourrait comporter intrinsèquement un aspect temporel, cela ne devrait pas faire obstacle à l’intention du législateur de protéger, dans l’application de la partie VI, le droit des gens au respect de leur vie privée en matière de communications.
12. L’emploi du mot « intercepter » implique que la prise de connaissance de la communication privée se fait au cours du processus de transmission. À mon avis, ce processus englobe toutes les activités du fournisseur de services qui sont nécessaires ou accessoires à la fourniture du service de communication. La prise de connaissance de la substance d’une communication privée se trouvant dans un ordinateur exploité par un fournisseur de services de télécommunications ferait, en conséquence, partie de ce processus.
13. Mettre l’accent sur le fait que le *Code* établit une distinction entre l’interception de communications privées et leur divulgation ne permet pas d’offrir la protection qu’est censée accorder la partie VI. Au contraire, cela fait en sorte que les différences d’ordre technologique du processus de transmission employé par Telus font échec à la protection qu’entendait accorder le législateur aux communications privées contre les atteintes étatiques.
14. La réalité des technologies modernes de communication fait en sorte que des communications privées électroniques, par exemple des messages textes, sont souvent à la fois en cours de transmission *et* simultanément stockées sur ordinateur, sous une certaine forme, par le fournisseur de services. Par conséquent, la même communication privée se trouve à plus d’un endroit, ce qui permet à l’État d’en prendre connaissance à partir du canal de transmission et de l’ordinateur où elle est stockée. Autrement dit, la même communication privée peut être « interceptée » par la police plus d’une fois à partir de sources différentes.
15. Quand Telus copie des messages dans sa base de données informatique, plusieurs étapes du processus de transmission n’ont pas encore été réalisées. Il découle du calendrier de communication fixé par le mandat général en l’espèce que les policiers ont vraisemblablement obtenu des copies stockées de certains messages textes avant même leur réception par la personne à laquelle ils étaient destinés. Le ministère public concède que, si les policiers avaient pris connaissance de ces mêmes communications privées directement à partir du canal de transmission plutôt que des copies stockées, l’autorisation prévue à la partie VI aurait été nécessaire. Le degré de protection accordé ne devrait pas dépendre du fait que l’État prend connaissance soit d’une copie de la communication privée en cours de transmission soit d’une copie stockée par un fournisseur de services dans le cadre du processus de communication. Le législateur a rédigé la partie VI en termes larges, de façon à ce que les communications privées soient protégées sur plusieurs plateformes technologiques (voir *Lyons*).
16. Le processus de communication qu’emploie un tiers fournisseur de services ne devrait pas faire échec à la protection que le législateur entend accorder aux communications privées. Comme l’ont souligné dans leur mémoire les intervenantes l’Association canadienne des libertés civiles et la Clinique d’intérêt public et de politique d’Internet du Canada Samuelson‑Glushko, la Cour a reconnu dans d’autres contextes que les fournisseurs de services de télécommunications ne sont que des tiers qui transmettent des communications privées à titre d’« agents » et qu’ils devraient pouvoir fournir leurs services sans que cela n’entraîne d’effets juridiques sur la nature (ou, en l’espèce, sur la protection) de ces communications (*Société canadienne des auteurs, compositeurs et éditeurs de musique c. Assoc. canadienne des fournisseurs Internet*, 2004 CSC 45, [2004] 2 R.C.S. 427, par. 100‑101).
17. La partie VI reconnaît les dangers inhérents au fait de permettre l’accès aux futures communications privées d’un nombre potentiellement illimité de personnes pendant une longue période. Il s’agit là exactement des risques que soulève intrinsèquement la technique d’enquête utilisée en l’espèce. Une autorisation permettant à la police d’obtenir la communication *prospective* de *futurs* messages textes pendant une période de deux semaines, directement à partir du processus de communication employé par le fournisseur de services, constitue précisément le genre de situations auxquelles la protection de la partie VI est censée s’appliquer. À mon avis, la technique d’enquête en cause est une « interception de communications privées » visée à la partie VI.
18. La définition d’« intercepter » à l’art. 183 appuie une interprétation des mots « intercepter une communication privée » qui englobe la technique d’enquête utilisée par la police en l’espèce. Cette définition inclut la simple prise de connaissance d’une communication. Elle n’exige pas qu’il soit pris connaissance de la communication elle‑même; la prise de connaissance « de sa substance, son sens ou son objet » suffit. En outre, cette interprétation s’harmonise avec l’esprit et l’objet de la partie VI, laquelle est rédigée en termes larges de manière à régir et à encadrer une grande variété d’atteintes technologiques à la vie privée. Enfin, elle établit l’équilibre voulu entre l’atteinte grave à la vie privée qui résulte de la prise de connaissance clandestine de communications privées, et l’évolution des besoins en matière d’application efficace de la loi.
19. Les policiers ont joui d’un avantage considérable en recourant au mandat général. Ils n’avaient pas besoin d’une demande d’autorisation présentée par le procureur général; ils n’étaient pas tenus de démontrer que d’autres méthodes d’enquête avaient été utilisées sans succès; ils n’avaient pas l’obligation d’aviser les personnes ciblées; ils n’avaient pas à préciser l’identité des autres personnes dont les communications privées risquaient d’être regardées au cours de l’enquête.
20. Le mandat général décerné en l’espèce visait à permettre une technique d’enquête déjà envisagée par la procédure d’autorisation d’écoute électronique prévue à la partie VI, c’est‑à‑dire permettre à la police d’obtenir la production *prospective* de *futures* communications privées à partir d’un ordinateur exploité par un fournisseur de services dans le cadre de son processus de transmission. Comme la partie VI s’appliquait, le mandat général prévu à l’art. 487.01 ne pouvait être décerné.
21. En conséquence, je suis d’avis d’accueillir le pourvoi et d’annuler le mandat général et l’ordonnance d’assistance connexe.

Version française des motifs des juges Moldaver et Karakatsanis rendus par

Le juge Moldaver —

I. Introduction

1. Lorsqu’une technique d’enquête policière va à l’encontre de l’attente raisonnable d’une personne en matière de vie privée, il revient au législateur d’autoriser spécifiquement la technique. Il s’agit là de la règle générale. La disposition du *Code criminel*, L.R.C. 1985, ch. C‑46, portant sur ce qu’on a appelé le « mandat général » fait exception à la règle et permet à la police de s’adresser au tribunal pour qu’il autorise une technique d’enquête proposée qui n’est pas expressément autorisée par la loi. Parmi les questions soulevées en l’espèce, à mon avis, la question décisive consiste à savoir si un mandat général peut être dûment décerné lorsque le fond d’une technique d’enquête, sinon sa forme précise, est déjà visé par une autre disposition législative en vigueur.
2. J’ai eu l’occasion de lire les motifs de ma collègue la juge Abella et, bien que nous abordons la question différemment, je suis d’accord avec elle pour conclure que le mandat général en l’espèce est invalide. Les motifs de ma collègue s’attachent principalement à la définition d’« intercepter » qui figure à l’art. 183 du *Code* et à la question de savoir si la fouille en l’espèce était visée par cette définition pour l’application de la partie VI. Je ne crois pas qu’il soit nécessaire de répondre à ces questions parce que, à mon sens, l’issue de l’espèce repose sur le défaut des autorités d’établir l’une des conditions d’autorisation nécessaires à l’obtention d’un mandat général.
3. Au vu des faits de l’espèce, si l’on se détache de la forme et qu’on examine sur le fond la fouille que la police désirait effectuer, on se retrouve avec ce qui équivaut à une interception au sens de la partie VI. À ce titre, la police aurait pu — et aurait dû, comme je vais l’expliquer — demander une autorisation sous le régime de la partie VI, ce qui empêche la délivrance d’un mandat général.  Par conséquent, je suis d’avis, comme ma collègue la juge Abella, d’accueillir le pourvoi et d’annuler le mandat général ainsi que l’ordonnance d’assistance connexe.

II. Aperçu des questions soulevées dans le présent pourvoi

1. Les arguments principaux des parties au pourvoi ont trait à la question de savoir si la technique d’enquête autorisée par le mandat général entre dans la définition d’« intercepter » à l’art. 183 du *Code*. Les parties conviennent que s’il y a eu interception en l’espèce, le mandat général ne pouvait être décerné, faute de respecter la condition, prévue à l’al. 487.01(1)*c*) du *Code*, qu’il n’y ait « aucune disposition » qui prévoie le mandat. Bien entendu, elles divergent d’opinion sur la question de savoir si cette technique constitue une interception.
2. Ma collègue la juge Abella et moi sommes d’avis que le ministère public n’a droit d’obtenir un mandat général que s’il est à même de démontrer qu’« aucune disposition » n’autorise le recours à la technique, ou à un procédé équivalent en substance à la technique, proposée par la police dans une affaire donnée. Nous partageons également le même avis sur l’issue de l’espèce, mais nous divergeons d’opinion sur la manière d’y parvenir.
3. Ma collègue estime que la technique d’enquête en l’espèce *constituait* une interception au sens de l’art. 183; elle est donc d’avis de déclarer invalide le mandat général.  Je préfère plutôt trancher la présente affaire en partant du principe que la technique d’enquête qui nous occupe *était équivalente, sur le plan du fond*,à une interception et, à la lumière de cette conclusion, je suis également d’avis de déclarer invalide le mandat général.
4. J’emprunte une voie différente parce que j’hésite à me servir de la présente affaire pour analyser ce qui constitue une interception pour l’application de la partie VI. En envisageant la question comme je le fais, je suis conscient de la nécessité d’écarter les menaces que présente l’ère numérique pour la vie privée. Adapter des lois édictées dans les années 1970 à un univers de téléphones intelligents et de réseaux sociaux est une tâche difficile et profondément importante. Mais il ne m’apparaît pas nécessaire de déterminer si ce qui s’est produit en l’espèce était ou non une interception à proprement parler parce qu’il existe un motif de décision plus restreint qui nous met à l’abri des conséquences imprévues et incalculables dans ce domaine complexe du droit.

III. Analyse

A. *La disposition relative au mandat général*

1. En 1993, le législateur a édicté la disposition relative au mandat général ainsi que plusieurs nouveaux pouvoirs en matière de fouille et de perquisition en réponse à une série de décisions de notre Cour concernant la surveillance électronique. L’article 487.01 a été adopté précisément pour répondre à l’arrêt *R. c. Wong*, [1990] 3 R.C.S. 36. Dans cet arrêt, la Cour a conclu que la surveillance vidéo par la police d’activités qui se déroulent dans une chambre d’hôtel va à l’encontre de l’attente raisonnable d’une personne en matière de vie privée et nécessite ainsi une autorisation judiciaire préalable conformément à une disposition législative valide. La réponse du législateur, qui a pris la forme de l’art. 487.01, allait au‑delà de l’autorisation de la surveillance vidéo. La disposition prévoit en partie ce qui suit :

**487.01** (1) [Dénonciation pour mandat général] Un juge de la cour provinciale, un juge de la cour supérieure de juridiction criminelle ou un juge au sens de l’article 552 peut décerner un mandat par écrit autorisant un agent de la paix, sous réserve du présent article, à utiliser un dispositif ou une technique ou une méthode d’enquête, ou à accomplir tout acte qui y est mentionné, qui constituerait sans cette autorisation une fouille, une perquisition ou une saisie abusive à l’égard d’une personne ou d’un bien :

*a*) si le juge est convaincu, à la suite d’une dénonciation par écrit faite sous serment, qu’il existe des motifs raisonnables de croire qu’une infraction à la présente loi ou à toute autre loi fédérale a été ou sera commise et que des renseignements relatifs à l’infraction seront obtenus grâce à une telle utilisation ou à l’accomplissement d’un tel acte;

*b*) s’il est convaincu que la délivrance du mandat servirait au mieux l’administration de la justice;

*c*) s’il n’y a aucune disposition dans la présente loi ou toute autre loi fédérale qui prévoie un mandat, une autorisation ou une ordonnance permettant une telle utilisation ou l’accomplissement d’un tel acte.

(2) [Limite] Le paragraphe (1) n’a pas pour effet de permettre de porter atteinte à l’intégrité physique d’une personne.

(3) [Fouilles, perquisitions ou saisies raisonnables] Le mandat doit énoncer les modalités que le juge estime opportunes pour que la fouille, la perquisition ou la saisie soit raisonnable dans les circonstances.

1. La portée du mandat général — soit l’autorisation judiciaire d’« utiliser un dispositif ou une technique ou une méthode d’enquête » ou d’« accomplir tout acte » qui constituerait sans cette autorisation une fouille, une perquisition ou une saisie abusive — est restreinte par de nombreuses conditions préalables à sa délivrance et par des modalités d’exécution. La principale de ces conditions, et celle qui, à mon sens, est au cœur du présent pourvoi, est celle, prévue à l’al. 487.01(1)*c*), qu’il n’y ait « aucune disposition dans la présente loi ou toute autre loi fédérale qui prévoie un mandat, une autorisation ou une ordonnance permettant une telle utilisation ou l’accomplissement d’un tel acte ».
2. La condition qu’il n’y ait « aucune disposition » autorisant la fouille ou la perquisition fait en sorte que le mandat général est utilisé avec modération et de façon limitée. Cette condition permet d’éviter que le mandat général ne devienne [traduction] « un moyen détourné de recourir facilement à d’autres techniques dont les conditions préalables à l’autorisation sont plus exigeantes » : S. C. Hutchison et autres, *Search and Seizure Law in Canada* (feuilles mobiles), p. 16‑40.3. Sans vouloir prêter à la police des intentions malveillantes, j’estime que c’est ce qui s’est produit en l’espèce.

B. *Le mandat général en l’espèce*

1. Dans un cas typique où la Société TELUS Communications (« Telus »), le fournisseur de services de télécommunications en l’espèce, reçoit signification d’une autorisation visée par la partie VI, elle installe un appareil qui copie automatiquement toutes les activités qui concernent le numéro de téléphone indiqué, y compris tous les messages textes, et transmet automatiquement ces données au service des télécommunications de la police. Le ministère public ne conteste pas que l’acquisition de cette façon de messages textes d’une personne constitue une interception au sens de la partie VI; il est admis également qu’un message texte peut constituer une « communication privée » au sens de la partie VI.
2. Comme pratique d’entreprise, toutefois, Telus conserve systématiquement pendant au moins 30 jours dans ses bases de données une copie des messages textes envoyés et reçus par ses abonnés. Bien que Telus soit la seule, parmi les principaux fournisseurs de services de télécommunications, à faire de telles copies, elle a légalement le droit de le faire conformément à l’exception prévue au par. 184(2) du *Code.* La société affirme qu’elle intercepte les messages de ses abonnés de cette façon pour aider à résoudre les problèmes techniques de ses clients.
3. Le fait que Telus conserve les messages textes de ses abonnés de cette façon est important — il constitue en fait le fondement du présent pourvoi — parce qu’il crée une ressource d’enquête pour les autorités. Comme l’a affirmé le sergent‑détective Prosser de la Police provinciale de l’Ontario dans son affidavit déposé à la Cour, la pratique de Telus [traduction] « permet aux enquêteurs d’accéder au contenu de ces messages par un autre moyen » (d.a., p. 115). Au moyen de mandats de perquisition ordinaires (art. 487) ou d’ordonnances de communication (art. 487.012), la police a déjà obtenu copie de messages conservés dans la base de données de Telus.
4. En somme, avant la présente affaire, toutes les fouilles policières qui exigeaient les copies de messages textes d’abonnés de Telus étaient autorisées, à quelques exceptions près, soit sous le régime de la partie VI, soit par un mandat de perquisition ou une ordonnance de communication. Dans son mémoire, le ministère public résume la question : à l’égard des abonnés de Telus, la police demande généralement [traduction] « des mandats de perquisition ou des ordonnances de communication (relativement aux messages existants) ou des autorisations d’écoute électronique (relativement aux messages futurs) » (m.i., par. 10 (je souligne)).
5. Le mandat général en l’espèce représente donc une troisième possibilité. Sur le plan de la forme, il ressemble à une ordonnance de communication, car il permet à la police d’avoir accès aux messages textes *déjà conservés dans la base de données de Telus*. Sur le plan du fond, il ressemble plutôt à l’autorisation visée par la partie VI, car il permet *prospectivement* à la police d’accéder à des communications privées *futures* de façon *continue* pendant une période prolongée.
6. Le caractère hybride inhérent au mandat général en l’espèce fait ressortir la nécessité, pour le juge, de déterminer si la condition qu’il n’y ait « aucune disposition » est respectée pour examiner au fond la technique d’enquête policière, et non simplement ses formalités. Mais ce n’est pas ce qui s’est produit en l’espèce.

C. *Le mandat général a‑t‑il été valablement décerné?*

1. Le juge siégeant en révision a examiné la jurisprudence de la Cour d’appel de l’Ontario. Dans *R. c. Ha*, 2009 ONCA 340, 96 O.R. (3d) 751, le juge MacPherson a indiqué ce qui suit :

[traduction] L’analyse relative à l’al. 487.01(1)*c*) ne porte pas sur l’existence d’autres techniques d’enquête qui pourraient répondre aux besoins ou aux objectifs d’enquête de la police; elle porte plutôt sur la technique ou méthode d’enquête particulière que la police cherche à utiliser et sur la possibilité que cette utilisation puisse être autorisée par une autre disposition du Code ou d’une autre loi fédérale. [Je souligne; par. 43.]

1. S’appuyant sur l’arrêt *Ha*, le juge siégeant en révision a conclu qu’aucune disposition, dans le *Code* ou dans une autre loi, n’autoriserait la technique d’enquête utilisée en l’espèce — à savoir la [traduction] « communication quotidienne de messages textes futurs » (2011 ONSC 1143, 105 O.R. (3d) 411, par. 75). Bien que la police « aurait pu s’adresser à un juge de paix tous les jours durant les 14 jours couverts par le mandat général et obtenir les mêmes enregistrements au moyen d’un mandat ordinaire », le mandat général pouvait être décerné précisément parce qu’il autorisait entièrement, à lui seul, la fouille que le législateur n’avait pas par ailleurs prévue (par. 70)[[1]](#footnote-1).
2. À mon humble avis, l’analyse est incomplète. Il va de soi que la police *aurait pu* demander une autorisation visée à la partie VI et atteindre ainsi l’objectif de son enquête. L’avocat du ministère public l’a d’ailleurs admis à l’audition du présent pourvoi :

[traduction] Je ne suis pas certain s’ils ont bien réfléchi en fin de compte à la question parce que si ce que la police fait constitue une interception au sens de la partie VI, elle pourrait probablement s’adresser de nouveau au juge qui a décerné le mandat, soit un juge de la Cour supérieure, et lui demander une autorisation visée à la partie VI. [Je souligne; transcription, p. 81.]

Au vu du dossier dont dispose la Cour, la police n’a pas expliqué pourquoi elle n’aurait pas pu demander une autorisation visée par la partie VI. Nous savons que, n’eût été la pratique de Telus de conserver systématiquement les messages de ses abonnés, la police n’aurait pas eu d’autres choix que d’obtenir une telle autorisation puisqu’elle demandait l’autorisation prospective d’obtenir la communication quotidienne de messages textes futurs. En effet, c’est ce qu’elle fait — apparemment sans problème — avec les autres principaux fournisseurs de services de télécommunications, comme Rogers et Bell, qui ne conservent pas les messages textes comme le fait Telus.

1. Quoi qu’il en soit, il reste à déterminer si, selon la loi, la police *aurait dû* demander une telle autorisation. À l’audience du présent pourvoi, l’avocat du ministère public a affirmé que l’arrêt *Ha* répond irréfutablement à la question par la négative :

[traduction] . . . comme l’a indiqué la Cour d’appel de l’Ontario dans l’arrêt *Ha*, le critère à appliquer pour déterminer si un mandat général peut être décerné porte principalement sur la nature de la technique d’enquête en question, et non sur la nature de l’objectif de l’enquête.

La fouille de la base de données de Telus visant à obtenir des enregistrements futurs est une technique qui est complètement distincte de la saisie d’une télécommunication. C'est‑à‑dire que du point de vue de la mécanique [. . .] les policiers ne faisaient pas la même chose. [. . .] [I]l s’agissait d’un processus complètement différent. [Je souligne; transcription, p. 94‑95.]

1. En toute déférence, je ne saurais être d’accord. Interpréter l’arrêt *Ha* de cette façon reviendrait à fermer les yeux sur le fond de la fouille — et sur le bon sens. Ce que la police a fait en l’espèce — obtenir l’autorisation *prospective* de se faire transmettre des communications privées *futures* de façon *continue*, sinon constante, pendant une période prolongée — équivalait au fond à ce qu’elle aurait fait conformément à une autorisation visée à la partie VI. Cette transmission équivalait donc, à tout le moins, à une interception.
2. J’accepte la prétention du ministère public selon laquelle, sur le plan de la forme, les événements survenus en l’espèce diffèrent de ce qui se produirait conformément à une autorisation visée à la partie VI. Toutefois, je n’accepte pas que ce fait soit déterminant eu égard aux intérêts identiques en matière de vie privée. Abstraction faite du délai de 24 heures, les techniques d’enquête étaient les mêmes. Si l’on accepte la logique du ministère public, un mandat général aurait été décerné si le délai avait été de 24 minutes ou, d’ailleurs, de 24 secondes[[2]](#footnote-2). Établir une distinction entre ce qui a été autorisé en l’espèce et une interception au sens de la partie VI sur le fondement d’une telle théorie revient à établir « une distinction artificielle et irréaliste » : *Lyons c. La Reine*, [1984] 2 R.C.S. 633, p. 643.
3. Par conséquent, il convient d’établir une distinction entre les faits de l’espèce et ceux de l’arrêt *Ha.* Tant l’arrêt *Ha* que l’arrêt *R. c. Brand*, 2008 BCCA 94, 229 C.C.C. (3d) 443 (*sub nom. R. c. Ford*), l’autre arrêt d’une cour d’appel qui interprète l’art. 487.01, concernent des tentatives infructueuses par la personne visée par la fouille d’invalider un mandat général au motif que la police aurait pu demander plusieurs mandats ordinaires. Dans l’arrêt *Ha*, la police enquêtait sur un présumé laboratoire de fabrication de drogues. Elle a demandé l’autorisation de pénétrer clandestinement dans la propriété en tout temps dans une période de deux mois et d’y mener une vaste gamme d’activités de collecte d’éléments de preuve, notamment de prendre des photos, des échantillons de produits chimiques et de prélever des empreintes digitales sur des objets. De même, dans l’arrêt *Brand*, la police enquêtait sur d’importantes activités liées à la culture de marijuana et avait besoin de pénétrer secrètement dans diverses propriétés pour vérifier la présence de drogues sans compromettre d’autres aspects de son enquête. Fondamentalement, dans chaque cas, la demande d’accès en secret et la souplesse des délais démontraient clairement que le *fond* des techniques d’enquête pour lesquelles une autorisation était demandée différait de ce qui pouvait être autorisé dans le cadre d’un mandat ordinaire.
4. Pour expliquer en quoi la fouille autorisée par le mandat général dans l’arrêt *Ha* était différente, sur le plan du fond, d’une fouille nécessitant plusieurs mandats ordinaires, le juge MacPherson a affirmé ce qui suit :

[traduction] En l’espèce, la police a demandé l’autorisation d’effectuer un nombre illimité d’entrées et de fouilles clandestines dans une propriété privée sur une période de deux mois. À part l’art. 487.01 du Code, il n’y a « aucune disposition dans [. . .] toute autre loi fédérale » qui pourrait potentiellement permettre à la police d’accomplir ces actes. [par. 43]

Les faits dont nous sommes saisis sont tout autres. Dans le cas qui nous occupe, la police cherchait à obtenir, comme l’a dit le juge siégeant en révision, l’autorisation pour [traduction] « la technique ou la procédure d’enquête visant la communication prospective et quotidienne de messages textes » (par. 75). Mais en réalité, il *existe* une disposition qui prévoit au fond cette technique. Il s’agit de la partie VI.

1. Pour souligner l’importance de regarder au‑delà de la forme d’une technique d’enquête pour découvrir son fond véritable, il convient d’observer un autre point. Dans les arrêts *Ha* et *Brand*, si la police voulait obtenir des éléments de preuve, elle pouvait choisir entre une série de mandats ordinaires ou un mandat général. Si la police demandait un mandat général, il aurait fallu qu’elle respecte les conditions de l’art. 487.01, lesquelles sont délibérément plus strictes que celles relatives au mandat ordinaire. Par exemple, les conditions prévoyant qu’un mandat général ne peut être décerné que par un juge, et non par un juge de paix, et que sa délivrance doit servir au mieux l’administration de la justice visent à faire en sorte que le mandat général demeure un mandat d’arrière‑garde auquel il faut limiter le recours.
2. Autrement dit, les exigences plus strictes du mandat général dissuadent les autorités d’y recourir quotidiennement. Dans les arrêts *Ha* et *Brand*, où la seule autre solution consistait en une série de mandats ordinaires, le fait que la police a eu recours à un mandat général ne lui a pas permis de se soustraire facilement aux exigences d’une autorisation législative plus stricte — le mandat général *constituait* l’autorisation législative plus stricte. Dans ces deux arrêts, il est donc plus difficile de voir comment les dispositions portant sur le mandat général auraient pu être utilisées abusivement.
3. En l’espèce, par contre, la police pouvait réellement choisir entre une autorisation visée à la partie VI et un mandat général[[3]](#footnote-3). Pour la police, les avantages étaient donc nettement différents de ceux dans l’arrêt *Ha*. Bien que le mandat général et les dispositions de la partie VI exigent que le juge soit convaincu que l’ordonnance sert au mieux l’administration de la justice, la partie VI à elle seule impose plusieurs autres exigences afin de protéger le droit au respect de la vie privée :

l’autorisation visée à la partie VI ne peut être obtenue que relativement à certaines infractions (art. 183);

seules les personnes désignées par le ministre de la Sécurité publique et de la Protection civile ou par le procureur général peuvent demander une autorisation visée à la partie VI (par. 185(1) et 186(6));

l’autorisation visée à la partie VI peut être obtenue uniquement lorsque « d’autres méthodes d’enquête ont été essayées et ont échoué, ou ont peu de chance de succès, ou que l’urgence de l’affaire est telle qu’il ne serait pas pratique de mener l’enquête relative à l’infraction en n’utilisant que les autres méthodes d’enquête » (al. 186(1)*b*));

l’autorisation visée à la partie VI doit indiquer l’identité des personnes dont les communications privées seront interceptées, le lieu où l’interception se fera et la façon dont on y procédera (al. 186(4)*c*));

le procureur général ou le ministre est tenu, dans un certain délai, d’aviser de l’autorisation la personne en cause (art. 196);

le ministre est tenu de présenter au Parlement un rapport annuel indiquant le nombre de demandes d’autorisation présentées sous le régime de la partie VI et les détails de ces demandes (art. 195).

1. Par conséquent, en l’espèce, le fait de s’en tenir uniquement au mécanisme de la fouille nous fait perdre de vue l’essentiel. Le mandat général doit être comparé à l’autorisation visée à la partie VI lorsque l’on analyse les avantages qu’il offre à la police. L’interprétation mécanique de la condition qu’il n’y ait « aucune disposition »ne saurait être retenue parce que, pour dire les choses sans détour, un mandat général peut s’avérer plus facile à obtenir qu’une autorisation visée à la partie VI. Pour cette raison, on peut difficilement reprocher à la police de demander un mandat général au lieu d’une autorisation visée à la partie VI. Elle avait peu à perdre (un retard dans la réception des données sollicitées, qui aurait probablement eu peu de conséquences) et beaucoup à gagner (aucune obligation de s’acquitter du lourd fardeau que le législateur a choisi d’imposer sous le régime de la partie VI).
2. Les faits portent à croire que c’est précisément ce qui s’est produit par suite du rejet de la contestation du mandat soulevée par Telus en l’espèce. Dans son affidavit, le sergent‑détective Prosser affirme que la police demande des mandats généraux uniquement dans ces [traduction] « rares circonstances » qui nécessitent l’accès aux messages textes « dans un délai plus court » (d.a., p. 116). Et pourtant, bien que Telus ait obtenu seulement six mandats généraux avant 2010, l’avocat de la société a informé la Cour à l’audience que le nombre a depuis augmenté à [traduction] « plusieurs centaines » depuis la décision de première instance (transcription, p. 42).
3. La logique qui a mené à ce résultat prévisible annule en fait la mesure de protection exigeant qu’il n’y ait « aucune disposition » en invitant la police à différencier une technique d’enquête d’une certaine façon — de quelque façon que ce soit, même si la distinction est sans importance du point de vue du fond — afin d’éviter la rigidité d’une autorisation législative plus exigeante comme celle visée à la partie VI. Si la police doit choisir entre demander une autorisation sous le régime de la partie VI et procéder par un moyen moins exigeant, elle choisira sans doute la dernière option — ce qui est compréhensible. Par conséquent, je suis d’avis qu’il faut renforcer le critère exigeant qu’il n’y ait « aucune disposition » afin qu’il puisse répondre à son objectif de veiller à ce que le mandat général ne devienne pas une façon d’éviter le recours aux autorisations de fouille qui comportent des conditions plus exigeantes.

D. *Résumé de la façon d’aborder la condition qu’il n’y ait « aucune disposition »*

1. Le critère fondé sur l’al. 487.01(1)*c*) exige la prise en compte de la technique d’enquête que la police cherche à utiliser en fonction de son fond réel et non simplement de sa forme. La disposition doit être interprétée de façon à accorder à la police la souplesse envisagée par le législateur lorsqu’il a créé le mandat général, tout en empêchant son utilisation abusive. Comme le démontrent les faits de l’espèce, il est nécessaire de resserrer l’examen judiciaire lorsque le législateur a prévu une autorisation pour une technique d’enquête qui correspond, sur le plan du fond, à ce que la police cherche à obtenir, mais qui requiert des conditions préalables plus strictes.
2. En concluant ainsi, je souligne qu’en créant le mandat général, le législateur n’a pas supprimé les autres autorisations de fouille du *Code* pour laisser aux juges le soin de concevoir les mandats généraux de façon ponctuelle comme ils l’entendent. Par conséquent, les tribunaux doivent veiller à combler le vide législatif uniquement lorsque le législateur n’a pas prévu une autorisation de fouille en particulier. Agir autrement éroderait le fondement qui encadre les rôles respectifs des tribunaux et du législateur dans notre système de justice criminelle lorsque les droits et libertés d’une personne sont en jeu.
3. Cela dit, je reconnais, comme je me dois de le faire, que cette approche accepte un certain degré d’incertitude en chargeant les juges d’examiner au fond les techniques d’enquête censément « nouvelles ». À mon avis, une interprétation qui demeure fidèle à l’objectif de la condition qu’il n’y ait « aucune disposition », prévue à l’al. 487.01(1)*c*), n’exige forcément pas moins. Toutefois, deux directives pratiques devraient servir à répondre aux questions qui peuvent être soulevées.
4. Premièrement, il importe pour la police de comprendre que le mandat général n’est pas un mandat d’application générale. Au contraire, il doit être utilisé avec modération, lorsque la technique d’enquête que la police désire utiliser est réellement différente, sur le plan du fond, d’une technique d’enquête prévue par une disposition législative. En cas d’incertitude, la police ferait bien de pécher par excès de prudence. Elle doit savoir — avec certitude — que le mandat général ne peut être utilisé pour contourner d’autres dispositions applicables en matière d’autorisation, mais qui comportent des conditions préalables plus exigeantes.
5. Deuxièmement, lorsque les juges sont saisis d’une demande en vue d’obtenir un mandat général et que la technique d’enquête, bien que non identique, s’apparente du point de vue du fond à une technique d’enquête prévue par une autre disposition pour laquelle des normes plus rigoureuses s’appliquent, ils devraient redoubler de prudence. À tout le moins, les juges devraient examiner attentivement les documents présentés et s’assurer que la demande en vue d’obtenir un mandat général est authentique et ne constitue pas seulement un moyen de contourner les exigences d’une autre disposition en matière d’autorisation. Si un examen minutieux établit qu’une technique d’enquête proposée, bien que similaire, est différente sur le plan du *fond* d’une technique existante — qui n’est pas simplement similaire du point de vue du fond, mais différente sur le plan de la forme — les juges peuvent accorder le mandat général, mais ils devraient tenir compte de l’obligation que leur impose le par. 487.01(3), c’est‑à‑dire qu’ils devraient fixer des modalités et conditions qui reflètent la nature du droit à la protection de la vie privée en jeu. Pour ce faire, ils peuvent s’inspirer des conditions que le législateur a choisi d’imposer à l’autorisation existante similaire sur le plan du fond.
6. À la lumière de ces deux considérations, et malgré les préoccupations du juge Cromwell à propos de la certitude, sur lesquelles je reviendrai, si la police a procédé de bonne foi et le juge fait preuve de prudence, il est peu probable qu’un mandat général décerné dans de telles circonstances soit jugé entaché d’un vice au procès — et encore moins que la preuve obtenue conformément à ce mandat soit exclue sur le fondement du par. 24(2) de la *Charte canadienne des droits et libertés*.

E. *La façon opposée de voir l’exigence qu’il n’y ait « aucune disposition »*

1. J’ai eu l’occasion de lire les motifs du juge Cromwell, qui est d’avis que la condition qu’il n’y ait « aucune disposition » a été respectée en l’espèce parce que la technique d’enquête ne cadre pas dans la définition d’une « interception » pour l’application de la partie VI. Par conséquent, il est d’avis de rejeter le pourvoi. En ce qui concerne la définition d’une interception, l’analyse de mon collègue repose sur la distinction entre l’interception d’une communication privée (art. 184) et la divulgation subséquente de la communication ainsi interceptée (art. 193). Comme je l’ai expliqué, je ne crois pas qu’il soit nécessaire de me pencher sur cette question dans le présent pourvoi et, pour cette raison, je ne ferai aucun commentaire sur cet aspect de ses motifs.
2. Toutefois, mon collègue conteste mon interprétation de l’al. 487.01(1)*c*) et son application au cas qui nous occupe. Il ne fait aucun doute que mon collègue et moi avons une vision fondamentalement différente non seulement de la condition qu’il n’y ait « aucune disposition », mais aussi du rôle des mandats généraux de manière plus générale. Il a fait une analyse minutieuse qui mérite une réponse.
3. Le juge Cromwell affirme que l’al. 487.01(1)*c*) devrait être interprété littéralement et rejette l’approche téléologique que j’ai adoptée, affirmant qu’elle « engendre [. . .] une incertitude inutile et détourne le juge de la question de la compatibilité de la technique visée par la demande d’autorisation avec le droit à la protection contre les fouilles, perquisitions et saisies abusives » (par. 171). Selon mon collègue, « la prévisibilité et la clarté du droit revêtent une importance particulière en matière d’autorisation judiciaire préalable de fouilles et de perquisitions » (par. 172).
4. Le juge Cromwell conteste aussi mon interprétation de l’al. 487.01(1)*c*) au motif qu’elle ajoute d’une manière inacceptable une « nécessité pour l’enquête » comme condition préalable supplémentaire à la délivrance d’un mandat général — à savoir que, pour obtenir un mandat général, la police doit être en mesure de démontrer qu’elle ne peut atteindre son objectif d’enquête par aucun autre moyen. Mon collègue affirme que le législateur n’a pas jugé bon d’ajouter une telle exigence et qu’il est inadmissible pour la Cour de le faire.
5. Je propose de répondre à chacune des préoccupations du juge Cromwell.
6. Premièrement, pour des raisons qui devraient ressortir clairement de ce qui précède, je ne saurais accepter l’interprétation littérale que donne mon collègue à l’al. 487.01(1)*c*). À mon humble avis, une telle interprétation vide la disposition de tout sens et lui fait perdre pratiquement toute valeur. En 1996, peu après l’introduction du mandat général, l’auteur d’un traité faisant autorité sur ce sujet a prédit ce qui suit :

[traduction] Des quatre conditions préalables [au mandat général], la plus difficile pour les enquêteurs sera [la condition qu’il n’y ait « aucune disposition »], une nouvelle disposition visant à empêcher que ce pouvoir résiduel de décerner un mandat ne devienne un moyen détourné de recourir facilement à d’autres techniques dont les conditions préalables à l’autorisation sont plus strictes. [Je souligne; Hutchison et autres, p. 16‑40.3.]

Toutefois, l’approche de mon collègue aurait pour effet de réduire cette disposition à un tigre de papier.

1. Selon l’interprétation littérale que mon collègue donne à l’al. 487.01(1)*c*), pour respecter la condition qu’il n’y ait « aucune disposition », il suffit d’une déviation — si légère ou insignifiante soit‑elle — faisant en sorte qu’une technique d’enquête excède le cadre d’application d’une autre disposition en matière d’autorisation du *Code* ou d’une loi fédérale. Par conséquent, en l’espèce, si la police avait sollicité un mandat général obligeant Telus à fournir des copies de tous les messages textes conservés dans un délai de 24 secondes (au lieu de 24 heures), j’ai l’impression que mon collègue aurait conclu que la condition qu’il n’y ait « aucune disposition » avait été respectée. De même, selon l’interprétation de mon collègue, si la police avait sollicité un mandat général nécessitant l’interception *simultanée* des messages textes *et* un mandat autorisant le placement sous enregistreur de numéro, il semblerait que cela aussi aurait suffi pour respecter la condition qu’il n’y ait « aucune disposition ».
2. Si, selon le raisonnement de mon collègue, le législateur avait vraiment voulu que la police puisse satisfaire à la condition qu’il n’y ait « aucune disposition » en trouvant un moyen détourné — n’importe lequel — qui ferait en sorte que la technique d’enquête excéderait le cadre d’application d’une autorisation existante, il nous faut alors conclure que le législateur a choisi d’édicter une disposition absurde. Je ne saurais accepter une telle conclusion.
3. Qui plus est, l’importance que mon collègue accorde à la grande portée de la disposition prévoyant le mandat général — une portée que je reconnais d’emblée — confond les questions distinctes de *ce* que le pouvoir permet de faire, à supposer qu’on puisse l’exercer, et *les moments* auxquels il peut être exercé. Comme je l’ai déjà indiqué, la disposition prévoyant le mandat général ne visait pas à effacer toutes les autres dispositions du *Code* en matière d’autorisation et à laisser aux juges le soin de concevoir les mandats généraux de façon ponctuelle. Au contraire, les mandats généraux ont été créés « pour combler toute “lacune” potentielle » (*Schreiber c. Canada (Procureur général)*, [1997] 2 C.F. 176 (C.A.), par. 86 (je souligne), inf. pour d’autres motifs par [1998] 1 R.C.S. 841), pour fournir une [traduction] « sécurité législative » qui « complète plutôt que remplace » (S. C. Hutchison, *Hutchison’s Canadian Search Warrant Manual 2005* (2e éd. 2004), p. 143 et 163 (je souligne)), pour [traduction] « combler une lacune de l’enquête » (J. A. Fontana et D. Keeshan, *The Law of Search and Seizure in Canada* (8e éd. 2010), p. 459 (je souligne)), et pour servir de [traduction] « pouvoir résiduel » (Hutchison et autres, p. 16‑36 (je souligne)).
4. Bien que peu de choses aient été dites sur les mandats généraux dans les débats ou les audiences du comité en 1993, nous savons que le législateur n’a pas mis un terme à son intervention dans le domaine des mandats après avoir édicté l’art. 487.01. De multiples autorisations ont été créées depuis lors, notamment des ordonnances de communication en 2004. Des autorisations existantes ont été modifiées, y compris les dispositions de la partie VI, pour répondre aux besoins d’enquête en constante évolution et aux préoccupations quant à la vie privée. Et même aujourd’hui, le législateur continue d’examiner des propositions en matière de mandat présentées — et parfois retirées — par le gouvernement. Voir, p. ex., le projet de loi C‑30, *Loi sur la protection des enfants contre les cyberprédateurs*, 1re sess., 41e lég. (Première lecture le 14 février 2012); le projet de loi C‑55, *Loi donnant suite à la décision de la Cour suprême du Canada dans l’affaire R. c. Tse*, 1re sess., 41e lég. (Première lecture le 11 février 2013).
5. Cet historique confirme que les mandats généraux devaient jouer un rôle modeste, en offrant à la police une voie constitutionnelle pour recourir à des techniques d’enquête que le législateur n’avait pas abordées. Ils constituaient donc des mandats d’arrière‑garde auxquels il faut limiter le recours, et non des mandats de première ligne d’application générale. Ils devaient permettre de combler des lacunes, non en créer.
6. Bref, veiller à ce que le recours aux mandats généraux soit limité constitue, à mon avis, le véritable objet de l’al. 487.01(1)*c*). L’interprétation littérale que donne le juge Cromwell à la disposition dénature cet objectif en invitant la police à demander aux tribunaux d’autoriser des techniques d’enquête censément « nouvelles » sur le fondement de distinctions dénuées de sens sur le plan du fond. De toute évidence, cette interprétation fait primer la forme aux dépens du fond.
7. Mon collègue invoque la condition de servir « au mieux » l’administration de la justice, dont fait état l’al. 487.01(1)*b*), qui serait une mesure de protection suffisante contre le recours abusif au mandat général. Il prétend que le législateur a édicté l’al. (1)*b*) pour remédier à lui seul aux « recours potentiellement abusifs au mandat général » (par. 190). Mais s’il en est ainsi, il faut se demander pourquoi alors le législateur a édicté l’al. 487.01(1)*c*).
8. Certes, l’exigence que le mandat serve « au mieux » l’administration de la justice vise à empêcher le recours abusif au mandat général. Mais cette disposition ne devrait pas être interprétée comme englobant la question analytique distincte que pose le critère exigeant qu’il n’y ait « aucune disposition ». Le rôle de chaque disposition doit être respecté. D’abord, suivant l’al. 487.01(1)*c*), il faut se demander s’il y a, dans le *Code* ou toute autre loi fédérale, une disposition qui prévoit en fait ou sur le fond la technique d’enquête que la police demande l’autorisation d’utiliser. Ensuite, suivant l’al. 487.01(1)*b*), ce n’est que si l’on répond par la négative à la première question qu’il faut se demander si la délivrance du mandat servirait au mieux l’administration de la justice.
9. Les deux exemples que j’ai évoqués plus tôt illustrent ce point. Je souhaiterais qu’un délai de 24 secondes et un mandat autorisant l’utilisation d’un enregistreur de numéro combiné à une autorisation pour l’interception simultanée de messages textes répondraient à la définition de recours abusif que propose mon collègue. Pourquoi? Parce que l’on constaterait probablement la vraie nature des deux techniques d’enquête — l’équivalent, sur le plan du fond, d’une autorisation visée à la partie VI. À la fin, tous les chemins mènent à Rome. Mais l’interprétation de l’al. 487.01(1)*c*) à laquelle je souscris donne un certain sens et une utilité à la disposition; l’interprétation de mon collègue la dépouille des deux.
10. En ce qui concerne l’al. 487.01(1)*b*), prenons, à titre d’exemple seulement, le fait que le recours à l’autorisation visée par la partie VI est limité à certaines infractions visées par la définition du terme « infraction » à l’art. 183. Si la police demande l’autorisation pour une fouille ou une perquisition concernant une infraction qui n’est pas visée par cette définition, bien que la condition qu’il n’y ait « aucune disposition » serait respectée, l’autorisation ferait l’objet d’une analyse fondée sur l’al. (1)*b*) pour prévenir la délivrance d’un mandat que le législateur a manifestement anticipé et délibérément exclu : S. Coughlan, « *R. v. Ha*: Upholding General Warrants without Asking the Right Questions » (2009), 65 C.R. (6th) 41, p. 41‑43.
11. Cela dit, mon collègue ne fournit aucune indication quant au genre de conduite qu’il qualifierait d’abusive, même s’il souligne que « le juge saisi d’une demande de mandat général doit veiller à ce que toute technique d’enquête autorisée respecte entièrement le droit à la protection contre les fouilles, perquisitions et saisies abusives » (par. 189). Vraisemblablement, il laisserait aux juges le soin de trancher la question de façon ponctuelle suivant l’al. 487.01(1)*b*), acceptant ainsi sa propre forme d’incertitude dans le processus. Je reconnais que l’approche fondée sur le fond à laquelle je souscris n’est pas hermétique — mais elle n’est pas plus perméable que l’approche fondée uniquement sur le recours au critère exigeant que le mandat serve « au mieux » l’administration de la justice auquel souscrit mon collègue.
12. Je me penche maintenant sur la deuxième préoccupation de mon collègue — selon laquelle j’ai introduit d’une manière inacceptable dans l’art. 487.01 une nécessité pour l’enquête, un concept propre à la partie VI. À mon humble avis, ma façon d’interpréter l’al. 487.01(1)*c*) n’a rien à voir avec une nécessité pour l’enquête.
13. L’exigence prévue à l’al. 186(1)*b*) selon laquelle l’autorisation visée à la partie VI est nécessaire porte sur une question *factuelle*. En exigeant que d’autres méthodes « ont été essayées et ont échoué », ou qu’elles ont « peu de chance de succès » ou que « l’urgence de l’affaire est telle qu’il ne serait pas pratique » de les utiliser, il appert que l’al. 186(1)*b*) porte sur la question de savoir si les circonstances factuelles d’une affaire en particulier nécessitent l’exercice des pouvoirs conférés par la partie VI. Le juge LeBel l’a expliqué au nom de la Cour dans *R. c. Araujo*, 2000 CSC 65, [2000] 2 R.C.S. 992 :

Le législateur et les tribunaux ont en effet reconnu que l’interception des communications privées est une mesure grave, qui ne doit être envisagée que pour des infractions graves, que s’il existe des motifs probables et que s’il est véritablement nécessaire de recourir à l’écoute électronique compte tenu de l’enquête en cause et de ses objectifs [. . .] Sur le plan pratique, il ne doit exister aucune autre méthode d’enquête raisonnable, dans les circonstances de l’enquête criminelle considérée. [Je souligne; soulignement dans l’original omis; par. 29.]

1. Par contre, la condition qu’il n’y ait « aucune disposition » soulève une question *juridique*. Il ne s’agit pas de savoir si d’autres techniques de fouille ont été épuisées, ou si elles ont peu de chance de succès, ou s’il y a urgence dans les circonstances. La question est plutôt de savoir si la technique d’enquête censément « nouvelle » est équivalente, en fait ou sur le fond, à une technique qui est déjà autorisée par la loi. Autrement dit, suivant la condition qu’il n’y ait « aucune disposition », la police n’est pas tenue de démontrer pourquoi une autre autorisation *ne serait pas praticable* au regard des faits d’une affaire en particulier, mais plutôt pourquoi elle est *différente sur le plan du fond* des autorisations déjà prévues par le législateur. Bien que le fait qu’une autre autorisation qui répondra à l’objectif d’enquête de la police puisse s’avérer un facteur utile pour démontrer son équivalence sur le plan du fond, l’examen suivant le critère exigeant qu’il n’y ait « aucune disposition » demeure axé sur ce dernier point, non sur le premier. Si la police réussit à démontrer pourquoi l’autorisation qu’elle demande est différente de celles déjà prévues, l’examen fondé sur l’al. 487.01(1)*c*) prend fin.
2. Enfin, deux questions soulevées par le juge Cromwell dans ses motifs méritent d’être clarifiées.
3. Premièrement, je ne conclus pas — et je ne voudrais pas non plus laisser entendre — que la police a agi sournoisement ou de mauvaise foi en sollicitant le mandat général en l’espèce. Aucune preuve en ce sens n’a été présentée, et je n’ai aucune raison de croire que la police a agi autrement que de bonne foi. Plus simplement, nous ne savons pas ce qui a motivé la police, et là n’est pas la question. La question de savoir si la police pouvait ou non obtenir une autorisation visée par la partie VI en l’espèce n’est pas pertinente dans la mesure où la condition qu’il n’y ait « aucune disposition » est concernée. Ce qui importe, c’est que nous ne disposons de rien qui puisse aider la police à s’acquitter de son fardeau de démontrer que la technique contestée était *différente sur le plan du fond* d’une interception.
4. Deuxièmement, l’approche à laquelle je souscris n’élimine pas la souplesse des enquêtes. Comme l’indiquent clairement les arrêts *Ha* et *Brand*, il s’agit d’un facteur qu’un juge peut examiner lorsqu’il décide si une technique d’enquête est différente sur le plan du fond de sorte qu’un mandat général devrait être décerné. Mais il ne s’agit pas du seul facteur à examiner, et ce facteur doit être abordé avec prudence, particulièrement dans des cas comme celui qui nous occupe, où la délivrance d’un mandat général peut constituer une façon commode pour la police d’éviter la rigidité d’une autre disposition en matière de fouille qui est équivalente sur le plan du fond.

IV. Conclusion

1. Pour ces motifs, je suis d’avis que la démarche adoptée par la police en l’espèce ne peut être approuvée. Le mandat général est invalide parce que la technique d’enquête qu’il autorisait était équivalente sur le fond à une interception. D’après les faits de l’espèce, le mandat général n’a servi qu’à éviter la rigidité de la partie VI. Comme l’a reconnu le ministère public, la police aurait pu demander une autorisation visée par la partie VI. Cela est suffisant pour trancher le pourvoi et pour conclure qu’elle aurait dû demander une telle autorisation.
2. Cela dit, bien que nous ne soyons pas en présence d’un tel scénario, je n’irais pas jusqu’à conclure qu’un mandat général ne peut *jamais* autoriser prospectivement la transmission de communications privées futures à la police de façon continue pendant une période prolongée. S’il est convaincu qu’une technique d’enquête précise est différente sur le plan du fond de sorte que les dispositions de la partie VI, ou de toute autre loi, ne prévoient pas la fouille, le juge pourrait décerner le mandat, en supposant que les autres exigences soient respectées. Bien entendu, le juge doit conclure que le mandat « servirait au mieux l’administration de la justice » (al. 487.01(1)*b*)) et « doit » imposer les modalités nécessaires pour que la fouille soit raisonnable dans les circonstances (par. 487.01(3)).
3. Je suis d’avis d’accueillir le pourvoi et d’annuler le mandat général et l’ordonnance d’assistance connexe.

Version française des motifs de la juge en chef McLachlin et du juge Cromwell rendus par

Le juge Cromwell (dissident) —

I. Aperçu

1. La Société TELUS Communications (« Telus ») conserve dans ses bases de données une copie de tous les messages textes envoyés ou reçus par ses abonnés. Il s’agit principalement de déterminer en l’espèce si la police doit obtenir une autorisation d’écoute électronique pour obtenir des copies des messages ainsi stockés. Mes collègues, la juge Abella et le juge Moldaver, concluent à la nécessité d’une telle autorisation, bien que pour des motifs très différents. Je ne suis pas de cet avis. Comme le juge de la Cour supérieure de l’Ontario qui a rendu la décision portée en appel, j’estime que l’autorisation d’écoute électronique n’était pas nécessaire. Je rejetterais donc le pourvoi.

II. Faits, historique judiciaire et questions litigieuses

1. La présente espèce concerne des techniques d’enquête particulières qui peuvent être autorisées sous le régime du *Code criminel*, L.R.C. 1985, ch. C‑46, lorsque la police souhaite avoir licitement accès au contenu de messages textes. Avant d’entreprendre l’analyse des questions juridiques précises auxquelles nous sommes confrontés, je donnerai quelques indications techniques au sujet de la messagerie texte et de l’éventail des techniques d’enquête que la police peut employer pour y avoir accès. Je résumerai ensuite brièvement les étapes judiciaires jusqu’au présent pourvoi ainsi que les questions que nous devons trancher.

A. *Le service de messagerie texte de Telus*

1. Le service de messages courts (« SMC »), communément appelé la messagerie texte, est un service de communication utilisant des protocoles de communication normalisés et des réseaux de téléphonie mobile pour la transmission de courts messages textes entre téléphones cellulaires.
2. Telus emploie le même système de transmission de messages textes que les autres fournisseurs de services de télécommunications. Lorsqu’un abonné de Telus envoie un message, celui‑ci est transmis à une station cellulaire Telus puis acheminé à un centre de commutation mobile, soit l’ordinateur central du réseau Telus. Ce centre de commutation comprend le centre de service de messages courts (« CSMC ») de Telus, qui tente de transmettre le message à son destinataire au moyen de moteurs de routage. Si le destinataire est lui‑même un abonné de Telus, le message est envoyé du CSMC à une station cellulaire qui le relaie au téléphone du destinataire; s’il n’est pas un abonné de Telus, le message est envoyé du CSMC de Telus au CSMC du fournisseur du destinataire puis il est relayé au téléphone du destinataire par une station cellulaire. Lorsque l’appareil du destinataire ne peut recevoir le message (par exemple, s’il est éteint ou s’il n’y a pas de réception), le message texte est conservé au CSMC de Telus pour une période maximale de cinq jours. Si, à l’expiration de cette période, le téléphone du destinataire n’a pu recevoir le message, ce message est effacé. Si un message n’est pas transmis, l’expéditeur n’en est pas informé.
3. Telus diffère toutefois de la plupart des autres fournisseurs en ce qu’elle conserve pendant au moins 30 jours, dans l’une de ses quatre bases de données, une copie électronique des messages textes passant par son système. Trois bases de données PSMS (la PSMS 1 (base de données principale), la PSMS 2 (base secondaire) et la PSMS 3 (base tertiaire)) reçoivent des messages dans les quinze minutes, environ, suivant leur envoi, et la capacité de chaque base de données détermine dans laquelle de ces bases un message est stocké. Tous les messages textes que reçoit un client de Telus sont copiés, et la copie est expédiée aux bases de données au moment où le téléphone de l’abonné les reçoit du CSMC de Telus. Lorsqu’un abonné de Telus envoie un message texte, le message est copié lorsqu’il arrive au CSMC de Telus, et la copie est stockée dans une base de données. Telus possède en outre une quatrième base de données, appelée PECSMS, qui reçoit des messages dans un délai de deux à huit heures après leur envoi. Au moment de l’instruction de la présente affaire en première instance, Telus prévoyait qu’en avril 2011 la base PECSMS serait l’unique base de stockage des messages textes et l’utilisation des bases PSMS cesserait.
4. Telus copie les messages textes pour faciliter le dépannage et le traitement des plaintes des clients. Comme je l’expliquerai plus loin, en procédant ainsi, Telus intercepte les messages, ce que le *Code* l’autorise à faire sans autorisation d’écoute électronique. Le but avoué par Telus, jumelé au fait que la plupart des autres fournisseurs de services en Ontario transmettent les messages textes sans en conserver une copie de cette façon, montre clairement, selon moi, que cette étape supplémentaire ne fait pas partie du processus de communication. Le type de stockage en cause ici n’est pas inhérent à la communication de messages textes, contrairement au stockage transitoire des courriels, nécessaire à leur transmission.

B. *Messages textes et techniques d’enquête*

1. Pour obtenir l’autorisation de prendre connaissance du contenu de messages textes stockés par Telus, la police dispose, en vertu du *Code*, d’au moins trois moyens potentiels : l’ordonnance de communication, le mandat général et l’autorisation d’interception, aussi appelée « autorisation d’écoute électronique ». En l’espèce, la police a demandé et obtenu un mandat général se voulant une sorte d’ordonnance de communication étoffée, mais Telus soutient que la police devait demander une autorisation d’écoute électronique. Les exigences de ces trois techniques d’enquête étant en quelque sorte interreliées, une brève description de chacune sera utile.

1. L’ordonnance de communication

1. La police peut obtenir le contenu de messages textes stockés en demandant l’ordonnance de communication prévue à l’art. 487.012 du *Code*, lequel énonce qu’un juge de paix ou un juge peut ordonner à une personne « de communiquer des documents — originaux ou copies [. . .] [ou] de préparer un document à partir de documents ou données existants et de le communiquer » (al. 487.012(1)*a*) et *b*)). Les conditions régissant la délivrance d’une ordonnance de communication sont essentiellement les mêmes que pour le mandat de perquisition. Une dénonciation sous serment doit convaincre le juge de paix ou le juge qu’une infraction a été ou est présumée avoir été commise, que les documents ou données fourniront une preuve touchant la perpétration de l’infraction et que ces documents ou données sont en la possession ou à la disposition de la personne visée par l’ordonnance (par. 487.012(3)). En outre, cette personne ne doit pas faire l’objet de l’enquête (par. 487.012(1)).
2. Lorsque Telus reçoit signification d’une ordonnance de communication, elle doit communiquer à la police les documents ou données qui sont déjà en sa possession ou des copies de ceux‑ci. La police obtient ainsi copie de messages textes qui ont déjà été envoyés ou reçus par les abonnés et stockés dans les bases de données de Telus. On a supposé, et je tiens pour acquis en l’espèce, qu’une ordonnance de communication ne peut viser des documents ou données qui n’existent pas encore (voir les al. 487.012(1)*b*) et 487.012(3)*c*)).
3. J’ajouterais qu’à première vue, l’art. 487.012 permet à un juge de paix ou un juge d’ordonner la communication de messages textes se trouvant dans les bases de données d’un fournisseur au moyen d’une série d’autorisations quotidiennes. Cet article établit relativement peu de restrictions pour la délivrance d’ordonnances de communication. Contrairement aux autres autorisations examinées en l’espèce, cet article n’exige pas du juge une conclusion que l’ordonnance est nécessaire à l’enquête policière et ne requiert pas que l’ordonnance serve au mieux l’administration de la justice. À l’instar du juge siégeant en révision, je considère que la police aurait pu avoir accès aux messages textes stockés dans les bases de données de Telus au moyen d’une série de telles ordonnances.

2. Le mandat général

1. Un juge peut décerner un mandat général autorisant un agent de la paix à « utiliser un dispositif ou une technique ou une méthode d’enquête, ou à accomplir tout acte qui y est mentionné, qui constituerait sans cette autorisation une fouille, une perquisition ou une saisie abusive » (art. 487.01). Le juge doit être convaincu, par la dénonciation faite sous serment, de l’existence de motifs raisonnables de croire qu’une infraction a été ou sera commise et que l’utilisation de la technique pour laquelle la police demande une autorisation permettra d’obtenir des renseignements au sujet de cette infraction.
2. Comme une vaste gamme de techniques peuvent être autorisées par un mandat général, le législateur a imposé des conditions supplémentaires rigoureuses. Premièrement, contrairement aux mandats de perquisition et aux ordonnances de communication qui peuvent émaner de juges ou de juges de paix, le mandat général ne peut être décerné que par un juge (par. 487.01(1)). Deuxièmement, le juge doit être « convaincu que la délivrance du mandat servirait au mieux l’administration de la justice » (al. 487.01(1)*b*)). Troisièmement, le mandat général « doit énoncer les modalités que le juge estime opportunes pour que la fouille, la perquisition ou la saisie soit raisonnable dans les circonstances » (par. 487.01(3)). Quatrièmement, le mandat général n’est décerné que « s’il n’y a aucune disposition [. . .] qui prévoie un mandat, une autorisation ou une ordonnance permettant une telle utilisation ou l’accomplissement d’un tel acte » (al. 487.01(1)*c*)). Autrement dit, on ne peut avoir recours au mandat général pour autoriser « une telle utilisation ou l’accomplissement d’un tel acte » si d’autres dispositions prévues au *Code* (ou ailleurs) pourraient les autoriser. (Ce que j’appellerai, dans ces motifs, la condition qu’il n’y ait « aucune disposition ».) Telus affirme que cette condition n’était pas respectée parce que les dispositions du *Code* en matière d’écoute électronique prévoient l’autorisation de la technique que la police souhaitait utiliser.

3. L’autorisation d’écoute électronique

1. L’autorisation d’intercepter des communications privées délivrée sous le régime de la partie VI du *Code* permet à la police de recevoir les messages au moment où ils sont envoyés ou reçus par les abonnés. Cette autorisation est assujettie à des conditions encore plus strictes que celles qui s’appliquent au mandat général.  Elle ne peut être délivrée que par un juge d’une cour supérieure de juridiction criminelle ou par un juge au sens de l’art. 552 du *Code*, et la demande d’autorisation doit être présentée par le procureur général, le ministre de la Sécurité publique et de la Protection civile ou un mandataire spécialement désigné (par. 185(1)). Des dispositions particulières détaillées prévoient ce qui doit être présenté au juge, lequel doit être convaincu non seulement que l’autorisation servirait au mieux l’administration de la justice, mais encore qu’il a été satisfait au critère dit de la « nécessité pour l’enquête » (par. 186(1)), ce qui signifie qu’il doit avoir la conviction que « d’autres méthodes d’enquête ont été essayées et ont échoué, ou ont peu de chance de succès, ou que l’urgence de l’affaire est telle qu’il ne serait pas pratique de mener l’enquête relative à l’infraction en n’utilisant que les autres méthodes d’enquête » (par. 186(1)). Généralement, la durée de validité de l’autorisation ne dépasse pas 60 jours (al. 186(4)*e*)), et des exigences en matière d’avis et de rapport s’appliquent (art. 196).
2. Lorsque l’interception de messages textes est autorisée, Telus installe un dispositif qui achemine automatiquement une copie de chaque message texte à la salle ou au poste d’écoute de la police. Lorsqu’un abonné de Telus envoie un message texte, le dispositif achemine une copie du message lorsque celui‑ci arrive au CSMC de Telus. Lorsque l’abonné de Telus reçoit un message texte, l’acheminement de la copie se fait lorsque le message parvient au téléphone de l’abonné. Ainsi, avec l’autorisation d’interception, la police a accès aux messages « en temps réel », dès leur envoi ou leur réception.

C. *Historique judiciaire*

1. En l’espèce, la police a demandé et obtenu un mandat général ordonnant à Telus de lui fournir copie de messages textes stockés, envoyés et reçus par deux de ses abonnés avant la délivrance du mandat et, aussi, de messages qui seraient envoyés et reçus après la délivrance du mandat, pendant une période d’environ deux semaines. Seule l’autorisation de communication des messages textes postérieurs à la délivrance du mandat est en cause. Relativement à ces derniers messages, Telus devait fournir, au plus tard à 14 h chaque jour, du mardi au vendredi, une copie de tous les messages envoyés ou reçus entre 11 h la veille et 11 h le jour même. Les lundis, elle devait fournir, au plus tard à 14 h, une copie de tous les messages envoyés ou reçus entre 11 h le vendredi précédent et 11 h le lundi. Le mandat général exigeait en outre que Telus fournisse à la police les renseignements relatifs aux abonnés à l’égard de tous les numéros de téléphone avec lesquels les deux abonnés en cause avaient échangé des messages textes. Le mandat général s’apparentait ainsi à une ordonnance de communication, puisqu’il exigeait la communication de copies de messages stockés et de renseignements relatifs aux abonnés s’y rapportant, mais il s’en distinguait du fait qu’il autorisait prospectivement la communication de ces copies.
2. Telus a demandé l’annulation du mandat général et le juge Sproat a essentiellement rejeté sa demande (2011 ONSC 1143, 105 O.R. (3d) 411). Selon le principal argument invoqué par Telus, le mandat général autorisait une interception, une technique qui pouvait être autorisée sous le régime de la partie VI du *Code*. On ne pouvait donc décerner un mandat général puisque la condition qu’il n’y ait « aucune disposition » permettant cette technique n’avait pas été respectée.
3. Le juge siégeant en révision a rejeté cet argument. À son avis, le mandat général n’autorisait pas une interception; la police demandait les copies de messages déjà stockés dans les bases de données de Telus; elle ne sollicitait pas l’autorisation d’« intercepter des communications privées ». Le mot « intercepter » exigeait, selon lui, l’obtention en temps réel de communications transitoires, ce qui ne couvrait pas l’obtention de copies de messages stockés dans une base de données. Les dispositions relatives à l’écoute électronique ne pouvaient autoriser que des interceptions et par conséquent, elles n’étaient pas applicables à la technique d’enquête employée par la police en l’espèce. De l’avis du juge siégeant en révision, un mandat général pouvait donc être décerné.
4. Telus a aussi invoqué d’autres arguments que le juge siégeant en révision a rejetés. Elle a fait valoir que la police aurait dû attendre la fin de la période de 14 jours visée par le mandat général et demander alors une ordonnance unique de communication. Le juge a rejeté cet argument et estimé que la police n’avait pas à attendre si longtemps pour obtenir les messages. Il a ajouté que, bien que la police eût pu demander au juge de paix 14 ordonnances distinctes de communication, cette solution n’était pas pratique dans les circonstances (par. 76). Il a énuméré divers inconvénients liés à l’obligation faite à la police de demander 14 autorisations, dont le fait de devoir répéter quotidiennement la demande, peut‑être devant des officiers de justice différents, et les inconvénients en résultant pour Telus, qui devrait donner suite à des mandats quotidiens exigeant une prompte réponse (par. 70). Le juge Sproat a conclu qu’un mandat général unique autorisant la police à recevoir des messages par courriel pendant environ deux semaines était acceptable parce qu’[traduction] « il n’aurait pas été pratique pour la police d’obtenir chaque jour un mandat pour parvenir au résultat visé par son enquête, soit obtenir pour examen quotidien des messages textes stockés » (par. 76).
5. Le juge siégeant en révision n’a pas retenu non plus l’argument de Telus voulant que la délivrance du mandat général ne serve pas au mieux l’administration de la justice (al. 487.01(1)*b*)). Il a conclu que la technique pour laquelle l’autorisation était demandée n’était pas une interception. Il a conclu qu’[traduction] « il n’appartient pas au tribunal de déterminer, pour des considérations d’intérêt public, que le régime législatif est inadéquat et de prendre prétexte de ce qui sert au mieux l’administration de la justice pour élargir en fait la portée de la partie VI du *Code criminel* » (par. 80). Le juge a aussi écarté l’argument de Telus fondé sur la lourdeur et le caractère impraticable du régime du mandat général et le fardeau excessif qu’il imposait, faisant observer que notre Cour avait écarté pareil argument dans *Société Télé‑Mobile c. Ontario*, 2008 CSC 12, [2008] 1 R.C.S. 305, par. 60.

D. *Les questions en litige*

1. Le principal argument avancé devant nous par Telus est que la technique d’enquête autorisée par le mandat général consistait, en fait, en l’interception de communications privées et qu’en vertu de la condition qu’il n’y ait « aucune disposition » prévue à l’al. 487.01(1)*c*), cette technique ne pouvait être autorisée que sous le régime de la partie VI du *Code*. Ma collègue la juge Abella accepte cet argument, mais je ne puis m’y rallier. Mon collègue le juge Moldaver estime pour sa part inutile d’examiner le principal argument de Telus. Selon lui, même si le mandat général ne constitue pas à strictement parler un mandat autorisant une interception, il autorise une technique qui y équivaut fondamentalement et qui, par conséquent, devrait être exclue de l’autorisation par mandat général en application de la condition qu’il n’y ait « aucune disposition » imposée par l’al. 487.01(1)*c*). Deux questions se posent en conséquence :

1. La technique d’enquête autorisée en l’espèce par le mandat général est‑elle une interception nécessitant une autorisation sous le régime de la partie VI du *Code*?

2. Si la saisie de messages textes stockés n’est pas une interception, la condition qu’il n’y ait « aucune disposition » énoncée à l’al. 487.01(1)*c*) interdit‑elle néanmoins la délivrance d’un mandat général du fait que la technique que l’on demande d’autoriser équivaut fondamentalement à de l’écoute électronique?

III. Analyse

A. *Première question : La technique d’enquête autorisée en l’espèce par le mandat général est‑elle une interception nécessitant une autorisation sous le régime de la partie VI du Code?*

1. Telus plaide qu’un mandat général ne pouvait être décerné en l’espèce car la technique d’enquête que la police cherchait à faire autoriser était l’interception de communications privées. Cette technique d’interception de communications privées peut être autorisée par un juge en vertu de l’art. 186, partie VI, du *Code*. Par conséquent, selon cet argument, le mandat général n’aurait pas dû être décerné parce que la condition qu’il n’y ait « aucune disposition » n’était pas respectée (al. 487.01(1)*c*)).
2. Ma collègue la juge Abella accepte en gros cet argument. Elle est d’avis que le mandat général était censé autoriser une interception, parce qu’il permettait « la communication *prospective* de futurs messages textes se trouvant dans l’ordinateur d’un fournisseur de services » (par. 15 (en italique dans l’original)). Je crois comprendre que « la communication *prospective* de futurs messages textes » signifie qu’au moment où le mandat est décerné, au moins certains des messages à divulguer n’existent pas encore. J’estime avec égards que ce mandat général n’a pas autorisé une interception.
3. La technique d’enquête autorisée en l’espèce par le mandat général n’est pas une interception de communications privées qui pourrait être autorisée en vertu de l’art. 186. Le mandat général procure à la police des copies de messages stockés, préalablement interceptés par Telus; la police n’obtient la divulgation des messages que lorsque Telus les récupère de sa base de données et les lui envoie par courriel. La distinction entre la divulgation d’une communication interceptée et l’interception d’une communication, loin d’être une différence « de forme », revêt une importance fondamentale pour ce qui est de l’objet des dispositions relatives à l’écoute électronique et du régime qu’elles établissent.

1. Texte, contexte et régime de la partie VI

1. La question de savoir si ce que la police a fait en vertu du mandat général constitue l’interception de communications privées relève de l’interprétation de la loi. À mon avis, à la lecture des dispositions législatives dans leur contexte intégral, il est clair que le mandat général ne permet pas une interception nécessitant une autorisation sous le régime de la partie VI.
2. En règle générale, la police doit obtenir une autorisation pour intercepter une communication privée au moyen d’un dispositif électromagnétique, acoustique, mécanique ou autre. Les mots clés sont donc « intercepter » et « communication privée ».
3. La définition du mot « intercepter » n’est pas exhaustive; le terme 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 » (art. 183). La définition de l’expression « communication privée » est liée à la notion d’interception. Si l’on réduit cette définition à l’essentiel, une communication privée est une communication faite « dans des circonstances telles que son auteur peut raisonnablement s’attendre à ce qu’elle ne soit pas interceptée par un tiers » (art. 183).
4. Un message texte est incontestablement une communication privée et, comme nous le verrons, il est tout aussi incontestable que Telus a intercepté des messages textes au moyen d’un dispositif électromagnétique, acoustique, mécanique ou autre. La question est de savoir si la police a elle aussi intercepté ces messages lorsque Telus lui a remis copie des messages envoyés et reçus qu’elle avait préalablement interceptés et stockés dans ses bases de données.
5. Cette question m’amène à un examen plus approfondi de l’objet et du texte des dispositions relatives à l’écoute électronique, ainsi que du régime qu’elles établissent. Cet examen permet le mieux, selon moi, de déterminer si le législateur voulait que la technique employée par la police en l’espèce constitue une interception. Les dispositions applicables sont reproduites en annexe.
6. La distinction entre *l’interception* de communications privées et *la divulgation, l’utilisation ou la conservation* de communications privées qui ont été interceptées est fondamentale pour ce qui est de l’objet des dispositions et du régime qu’elles établissent. L’objet, le texte et le régime de la partie VI montrent que la divulgation, l’utilisation ou la conservation de communications privées interceptées sont distinctes de l’interception elle‑même.
7. Lorsque les dispositions originales en matière d’écoute électronique ont été introduites en 1973, les notes explicatives du projet de loi indiquaient qu’il avait notamment pour but de créer trois types distincts d’infractions. Deux d’entre eux sont pertinents en l’espèce. La première infraction a trait à l’*interception* de communications privées au moyen d’un dispositif électromagnétique, acoustique, mécanique ou autre. La seconde a trait à la *divulgation* de communications privées interceptées de cette façon (Notes explicatives, projet de loi C‑176, *Loi sur la protection de la vie privée*, 1re sess., 29e lég. (S.C. 1973‑74, ch. 50)). Bien que les notes explicatives fassent moins autorité que l’énoncé des objets figurant dans le texte de loi même, elles peuvent néanmoins donner une idée de l’objectif législatif : R. Sullivan, *Sullivan on the Construction of Statutes* (5e éd. 2008), p. 272. Les notes explicatives indiquent ainsi que, dès le début, le texte de loi avait notamment pour objet de différencier l’interception de communications privées des actes subséquents et distincts que sont la divulgation ou l’utilisation des communications privées interceptées. Cela dénote que le législateur voyait l’interception et la divulgation de communications interceptées comme deux choses différentes et ne voulait donc pas que la divulgation ou l’utilisation de communications interceptées entrent dans la notion d’interception.
8. Le caractère fondamental de cette distinction pour le régime établi par la loi a été relevé par un des premiers commentateurs de la loi. David Watt (à présent juge à la Cour d’appel de l’Ontario), se demandant si le fait de rejouer, réentendre ou réenregistrer une conversation déjà enregistrée constituait une « interception », a conclu comme suit :

[traduction] Le fait de rejouer ou de réentendre la conversation interceptée à l’origine peut fort bien constituer chaque fois une utilisation ou divulgation au sens de l’interdiction applicable, mais utiliser ou divulguer n’est pas nécessairement intercepter, et assimiler les deux revient à faire abstraction de la distinction fondamentale que la loi établit entre ces actes. [Je souligne.]

(*Law of Electronic Surveillance in Canada* (1979), p. 44)

1. La structure des dispositions de la partie VI créant les infractions reflète cette distinction entre interception et divulgation. En d’autres termes, le texte de loi exprime précisément l’objet énoncé dans les notes explicatives. La partie VI crée des infractions distinctes conformément à l’objet énoncé dans ces notes.
2. Une infraction, je le répète, interdit l’*interception d’une communication privée*. Selon l’art. 184 du *Code*, « [e]st coupable d’un acte criminel et passible d’un emprisonnement maximal de cinq ans quiconque, au moyen d’un dispositif électromagnétique, acoustique, mécanique ou autre, intercepte volontairement une communication privée ». Des exceptions s’appliquent, comme nous le verrons un peu plus loin. L’autre infraction concerne *la divulgation ou l’utilisation des renseignements interceptés*. Aux termes de l’art. 193 du *Code*, commet un acte criminel quiconque utilise ou divulgue le contenu d’une communication privée ou en divulgue l’existence sans le consentement de son auteur ou de la personne à laquelle son auteur la destinait. Là encore, il existe des exceptions et j’y reviendrai. La création de ces deux infractions distinctes souligne que l’acte d’intercepter et l’acte de divulguer ou d’utiliser des communications interceptées sont des actes distincts que le régime établi par la loi traite différemment.
3. Dans le cas de la première infraction, relative à l’interception, plusieurs « réserves » excluent des actes qui constitueraient par ailleurs une interception illégale. Ces exclusions sont utiles à la compréhension du régime législatif parce qu’elles distinguent *l’interception* de communications de *l’utilisation ou la conservation* des communications interceptées. Sans entrer dans tous les détails, précisons qu’il existe trois catégories d’exonérations de responsabilité criminelle. L’interception d’une communication privée au moyen d’un dispositif électromagnétique, acoustique, mécanique ou autre ne constitue pas une infraction (i) si l’auteur de la communication ou la personne qui la reçoit y a consenti (al. 184(2)*a*)); (ii) si l’interception est autorisée en conformité des dispositions en cette matière (al. 184(2)*b*)); ou (iii) si l’interception intervient pour la fourniture d’un service de communications ou est faite par un fonctionnaire fédéral chargé de la régulation du spectre des fréquences de radiocommunication ou encore si elle sert à des fins de gestion ou de protection d’un ordinateur (al. 184(2)*c*), *d*) et *e*)).
4. Ce qui importe est que la troisième réserve — celle qui concerne l’interception en lien avec un ordinateur — distingue *l’interception* de la communication, d’une part, de *l’utilisation* ou de *la* *conservation* de la communication interceptée, d’autre part. L’alinéa 184(2)*e*) exclut de l’infraction l’interception, par une personne en possession ou responsable d’un ordinateur, de communications privées passant par l’ordinateur lorsque l’interception est raisonnablement nécessaire pour la gestion de la qualité du service de l’ordinateur ou pour la protection de celui‑ci. Le paragraphe 184(3), qui repose sur la distinction entre *l’interception* et *l’utilisation ou la conservation*, vient préciser cette exception; une communication privée *interceptée* par une personne en possession ou responsable d’un ordinateur ne peut être *utilisée ou conservée* que si elle est essentielle pour empêcher un dommage à l’ordinateur ou si elle est divulguée conformément à une autre disposition du *Code*.
5. Ainsi, les dispositions relatives à l’infraction d’interception distinguent l’interception de l’utilisation ou la conservation des communications interceptées, ce qui indique que le législateur y voyait des actes différents et distincts.
6. Cela nous amène à la deuxième infraction prévue par le régime, qui interdit l’utilisation ou la divulgation de communications privées interceptées. Aux termes du par. 193(1), commet une infraction quiconque *utilise* ou *divulgue* le contenu ou l’existence d’une communication privée interceptée sans qu’il y ait eu consentement. Je signale que l’infraction d’utilisation ou de divulgation concerne « tout ou partie de cette communication privée, ou la substance, le sens ou l’objet de tout ou partie de celle‑ci ». L’existence de cette infraction en tant qu’infraction distincte de celle d’interception montre que le législateur considérait l’interception, d’une part, et la divulgation ou l’utilisation, d’autre part, comme des concepts distincts.
7. La comparaison des exemptions prévues aux art. 184 et 193 me conforte dans cette position. L’article 193 prévoit des exemptions beaucoup plus permissives que celles prévues à l’art. 184, en particulier en ce qui a trait aux enquêtes en matière pénale. Aux termes de l’art. 184, la police ne peut intercepter des communications que si elle est autorisée à le faire (al. 184(2)*b*)) ou dans certaines circonstances exceptionnelles (art. 184.4). L’article 193, par contre, comprend de larges exemptions qui permettent la divulgation de communications interceptées dans diverses circonstances, notamment lors de poursuites civiles ou pénales (al. 193(2)*a*)) et « au cours ou aux fins d’une enquête en matière pénale » (al. 193(2)*b*)). On peut penser que, si le législateur considérait la divulgation de communications privées interceptées comme une forme d’interception, il y aurait eu une correspondance substantielle entre les exemptions relatives à l’interception et celles qui se rapportent à la divulgation. Or, ce n’est manifestement pas le cas.
8. La comparaison des exemptions particulières qui s’appliquent aux fournisseurs de services de communications, énoncées aux par. 193(2) et 184(2), étaye encore plus ce point. On se rappellera que l’interception de communications par les fournisseurs de services de communications ne constitue pas une infraction si elle intervient pour les fins de la fourniture de ces services (al. 184(2)*c*)). Une exception comparable s’applique à l’infraction de divulgation. L’alinéa 193(2)*d*) écarte la responsabilité criminelle à l’égard de la divulgation intervenant dans le cadre de l’exploitation d’un système de communications ou d’un service de gestion ou de protection d’un ordinateur, si la divulgation est nécessairement accessoire aux fins pour lesquelles les exploitants peuvent être exonérés de l’infraction d’interception. Ainsi, les exploitants de systèmes de communications comme Telus jouissent, dans certaines circonstances, d’une exception à l’infraction d’interception et à celle de divulgation. Cela souligne une fois de plus que le législateur considérait ces actes comme distincts.
9. Pour résumer, le régime législatif crée deux infractions distinctes, l’une qui concerne l’interception, et l’autre, l’utilisation ou la divulgation d’une communication. La distinction entre ces actes est un élément fondamental du régime : si la divulgation ou l’utilisation d’une communication privée en constituait l’interception, il n’aurait pas été nécessaire de les ériger en infraction distincte. De la même façon, les exonérations de responsabilité criminelle prévues par le législateur indiquent qu’il a établi une distinction entre l’interception, d’une part, et la conservation, l’utilisation et la divulgation, d’autre part.

2. Le mandat général autorisait‑il l’interception de communications privées?

1. Comment cela se rattache‑t‑il à ce que Telus et la police accomplissaient en vertu du mandat général en l’espèce? S’agissant de Telus, nul ne conteste qu’elle interceptait les messages textes lorsqu’elle les copiait pour les besoins de gestion de ses propres systèmes. Il est pareillement reconnu que Telus n’a pas commis une infraction d’interception illégale (ce que je tiens pour acquis pour le besoin du présent pourvoi). Elle a réalisé des interceptions dans un but autorisé visé par une exonération de responsabilité criminelle. L’alinéa 184(2)*c*) établit clairement que l’interception de communications privées par un fournisseur de services de communications comme Telus ne constitue pas une infraction lorsqu’elle est nécessaire, entre autres choses, pour le contrôle de la qualité des services. Aux termes de l’al. 193(2)*d*), ces fournisseurs peuvent aussi, pour les mêmes besoins, divulguer les communications interceptées sans encourir de responsabilité criminelle. Il ne fait donc aucun doute en l’espèce que Telus a licitement intercepté des communications privées.
2. Qu’en est‑il de ce qu’a fait la police en vertu du mandat général? La police a demandé à Telus la divulgation de renseignements que Telus avait déjà légalement interceptés. Le mandat général n’obligeait pas Telus à intercepter des communications, mais à fournir copie de communications qu’elle avait déjà interceptées à des fins licites qui lui étaient propres. Nul ne prétend que Telus procédait à ces interceptions à la demande de la police; des interceptions effectuées pour des fins policières nécessiteraient clairement une autorisation puisque ces fins ne sont pas visées par l’exception prévue à l’al. 184(2)*c*). Toutefois, comme l’indique clairement le régime législatif, la divulgation ou l’utilisation de communications interceptées légitimement ne constituent pas une interception. J’ai déjà précisé que la partie VI du *Code* établit une distinction fondamentale entre *l’interception*, d’une part — c.‑à‑d. écouter, enregistrer ou prendre volontairement connaissance d’une communication ou de sa substance, son sens ou son objet — et, d’autre part, *l’utilisation ou la divulgation* d’une communication privée ou de sa substance, son sens ou son objet, ou la divulgation de son existence. La reconnaissance de cette distinction est manifeste dans l’objet des dispositions, dans la création d’infractions distinctes pour l’interception illégale et pour l’utilisation ou la divulgation illégales, ainsi que dans les réserves qui s’appliquent à ces infractions.
3. À mon avis, la conclusion que la police interceptait des communications privées en recevant de Telus des copies de messages textes déjà interceptés et stockés est incompatible avec la distinction fondamentale qu’établit le texte de loi.

3. Les motifs de la juge Abella

1. Ce qui m’amène à examiner les motifs de la juge Abella. Selon elle, le mandat général visait à autoriser une interception parce qu’il permettait « la communication *prospective* de futurs messages textes se trouvant dans l’ordinateur d’un fournisseur de services » (par. 15 (en italique dans l’original)); le fait que les messages étaient stockés dans une base de données constitue simplement une différence « technique » propre au mode de prestation de service de Telus qui ne devrait pas priver les abonnés de Telus de la protection du *Code* (par. 3). Par conséquent, la police devait disposer d’une autorisation d’écoute électronique, non d’un mandat général. Cette interprétation s’appuie sur l’inclusion, dans la définition d’« intercepter », des mots « prendre volontairement connaissance d’une communication ou de sa substance, son sens ou son objet » (art. 183) et sur la nature prospective des autorisations d’écoute électronique. À mon avis, ce raisonnement n’est pas convaincant pour trois raisons.
2. Le premier problème que j’y vois est qu’il ne donne pas effet à la distinction claire que fait la loi entre l’interception et la divulgation. Pour les motifs que j’ai déjà exposés, j’estime que l’on ne peut, en la qualifiant de simple « différence technique », rejeter cette distinction, qui constitue un élément fondamental du régime créé par les dispositions en cause. Le législateur a traité l’« interception » et la « divulgation » comme des actes distincts, donnant naissance à des infractions et à des exceptions différentes, même si elles peuvent se rapporter aux mêmes communications privées. Lorsque Telus remet à la police les copies de communications déjà interceptées, elle les divulgue, elle ne les intercepte pas à nouveau. Je ne vois pas comment cette divulgation par Telus de données stockées dans ses bases de données peut constituer une interception par la police.
3. Le deuxième problème découle de ce que ma collègue s’appuie sur la définition d’« intercepter » énoncée à l’art. 183 et, plus particulièrement, sur le fait qu’« intercepter » inclut « prendre volontairement connaissance d’une communication ou de sa substance, son sens ou son objet ». Dans son sens large, cette définition d’« intercepter » signifie que chaque fois que la police prend connaissance d’une communication privée au moyen d’un dispositif électromagnétique, acoustique, mécanique ou autre, elle effectue une interception. À mon avis, le contexte et l’objet de la partie VI exigent que les mots « prendre volontairement connaissance d’une communication ou de sa substance, son sens ou son objet » reçoivent une interprétation plus étroite.
4. Tout d’abord, le sens des mots « prendre volontairement connaissance » doit être interprété en fonction du contexte où ils s’insèrent; ils font partie d’une énumération comprenant « écouter » et « enregistrer », deux actions se produisant en même temps que l’interception de la communication. Ils servent aussi à expliquer le mot « intercepter », et il est clair, je pense, que beaucoup de façons de prendre volontairement connaissance du contenu d’une communication ne peuvent être considérées comme une interception. De plus, si, comme l’affirme ma collègue la juge Abella (par. 37), « [l]a prise de connaissance de la substance d’une communication privée se trouvant dans un ordinateur exploité par un fournisseur de services de télécommunications » constitue une interception, il se pourrait fort bien alors qu’une autorisation d’écoute électronique soit nécessaire pour une multitude de fouilles ou perquisitions qui ne sont manifestement pas visées par la partie VI du *Code*. La police pourrait devoir obtenir une autorisation sous le régime de cette partie chaque fois qu’elle veut avoir accès au contenu de communications privées, peu importe quand le message a été envoyé ou qu’il ait été reçu ou stocké dans l’appareil du destinataire. Par exemple, selon une interprétation large de « prendre volontairement connaissance », la saisie de courriels d’un appareil BlackBerry constituerait une interception, parce qu’il y a prise de connaissance du contenu de communications privées. De la même façon, une personne autorisée en vertu du par. 487(2.1) à effectuer une perquisition dans un ordinateur aurait besoin d’une autorisation d’écoute électronique pour prendre copie des communications personnelles qui y sont stockées (y compris, par exemple, les courriels et les copies de clavardage). Un tel raisonnement irait à l’encontre du courant jurisprudentiel canadien selon lequel le mandat de perquisition est suffisant pour autoriser l’accès par la police à des documents et données conservés dans un ordinateur : voir, p. ex., *R. c. Cole*, 2012 CSC 53, [2012] 3 R.C.S. 34, par. 73; *R. c. Jones*, 2011 ONCA 632, 107 O.R. (3d) 241, par. 33; *R. c. Bahr*, 2006 ABPC 360, 434 A.R. 1; *R. c. Cross*, 2007 CanLII 64141 (C.S.J. Ont.), par. 25‑27; *R. c. Little*,2009 CanLII 41212 (C.S.J. Ont.), par. 154; *R. c. Tse*, 2008 BCSC 906 (CanLII), par. 198; *R. c. Weir*, 2001 ABCA 181, 281 A.R. 333, par. 19.Si les mots « prendre volontairement connaissance d’une communication ou de sa substance, son sens ou son objet » recevaient une interprétation large, les communications privées stockées auxquelles la police a depuis longtemps accès au moyen de mandats de perquisition ordinaires seraient visées par la partie VI.
5. Compte tenu de l’objet des dispositions en matière d’écoute électronique et du régime qu’elles créent, il ne convient pas, à mon avis, d’interpréter de façon aussi large les mots « prendre volontairement connaissance ». Je ne reprendrai pas l’analyse exposée précédemment, sauf à dire qu’il en découle que l’on n’intercepte pas des communications déjà interceptées et stockées en en prenant connaissance, parce qu’une telle interprétation large est incompatible avec la nette distinction que font les dispositions législatives entre interception et divulgation. L’application générale de cette interprétation de « prendre volontairement connaissance » élargirait bien au‑delà de tout ce qui a déjà pu être envisagé le champ des techniques d’enquête nécessitant une autorisation d’écoute électronique.
6. Ce qui m’amène à traiter l’aspect temporel de la notion d’interception qu’introduit la juge Abella, et c’est la troisième difficulté que me pose son approche. Si je comprends bien, il y a interception si la prise de connaissance du contenu d’une communication privée est autorisée de façon prospective. Par conséquent, la question de savoir si un acte constitue une interception ne dépend pas de la nature de l’acte lui‑même ou du moment où il est posé, mais du moment où il est autorisé. Il s’ensuit nécessairement que la saisie de messages textes déjà interceptés et stockés ne constituerait pas une interception dès lors qu’elle était autorisée *après* le stockage des messages. La police pourrait obtenir une ordonnance de communication à la fin de chaque jour pendant la période visée par le mandat général et il n’y aurait pas d’interception. Toutefois, suivant ce critère de l’autorisation prospective, si la police devait saisir les mêmes renseignements, sous la même forme et par les mêmes moyens en vertu d’une autorisation accordée *avant* que les messages ne soient stockés, elle procéderait à une interception. À mon sens, cette conception confond l’acte d’intercepter et la nature de son autorisation.
7. L’interception est une technique, une façon de prendre connaissance de la substance d’une communication privée. Je ne comprends pas comment la même technique, donnant connaissance de l’information sous la même forme, peut constituer soit une saisie de renseignements stockés, soit une interception, selon le moment où elle est autorisée. C’est pourtant ce à quoi conduit le raisonnement de ma collègue la juge Abella. Je ne puis me rallier à cette conclusion.

4. Conclusion relative à la première question

1. Je suis d’avis que la technique d’enquête que la police était autorisée à employer par le mandat général ne constituait pas une interception au sens des dispositions du *Code* en matière d’écoute électronique.

B. *Deuxième question : Si la saisie de messages textes stockés n’est pas une interception, la condition qu’il n’y ait « aucune disposition » énoncée à l’al. 487.01(1)c) interdit‑elle néanmoins la délivrance d’un mandat général du fait que la technique que l’on demande d’autoriser équivaut fondamentalement à de l’écoute électronique?*

1. Mon collègue le juge Moldaver, comme la juge Abella, annulerait le mandat général au motif que la police n’a pas respecté la condition qu’il n’y ait « aucune disposition », énoncée à l’al. 487.01(1)*c*). Le juge Moldaver parvient toutefois à cette conclusion par un raisonnement différent s’appuyant, si je comprends bien, sur trois points principaux. Premièrement, le mandat général constitue une autorisation qu’il faut utiliser de façon limitée et avec modération (par. 56). Je ne puis accepter ni ce postulat ni le résultat qu’il produit en l’espèce. Deuxièmement, la technique proposée ici par la police équivaut « sur le plan du fond » à une interception et elle ne peut donc être autorisée en vertu du par. 487.01(1) en raison de la condition qu’il n’y ait « aucune disposition », énoncée à l’al. *c*). J’estime respectueusement que le critère de l’« équivalence sur le plan du fond » n’entre pas dans l’analyse relative à l’al. 487.01(1)*c*), et qu’en supposant même qu’il entre dans cette analyse, il ne s’appliquerait pas compte tenu des faits de la présente espèce. Troisièmement, vu cette similarité « sur le plan du fond », le recours au mandat général par la police constitue un « recours abusif » à l’art. 487.01, une « façon commode » pour elle d’éviter la rigidité de l’autorisation d’écoute électronique. Bien que j’estime, comme mon collègue, que les tribunaux doivent veiller à ce que les dispositions relatives au mandat général ne soient pas indûment élargies ou utilisées, ces préoccupations selon moi n’ont pas lieu d’être en l’espèce.

1. L’objet des dispositions relatives au mandat général

1. Le juge Moldaver préconise une interprétation téléologique, et non littérale, de ces dispositions. Je conviens, évidemment, que toutes les lois doivent recevoir une interprétation téléologique, mais je ne partage pas son avis au sujet du résultat de l’interprétation téléologique de ces dispositions.
2. J’examine d’abord l’objet des dispositions relatives au mandat général.  Je ne puis accepter que le par. 487.01(1) ait pour objet de n’accorder l’autorisation prévue que dans des circonstances très restreintes et qu’il faut en conséquence n’y recourir qu’avec « modération ». Au contraire, cette disposition est formulée en termes larges, ainsi que le signalent de nombreux auteurs. Comme l’a indiqué un auteur reconnu :

[traduction] En édictant l’art. 487.01 (et l’art. 487.02), le législateur a prévu un pouvoir vaste et complet d’octroi de mandats afin que pratiquement toutes les techniques d’enquête pouvant satisfaire aux conditions posées par *Hunter* en matière d’autorisation judiciaire préalable puissent être autorisées.

(S. C. Hutchison, *Hutchison’s Canadian Search Warrant Manual 2005* (2e éd. 2004), p. 143)

Lorsque la Cour d’appel de l’Ontario a examiné cette question dans *R. c. Ha*,2009 ONCA 340, 96 O.R. (3d) 751, par. 35, autorisation d’appel refusée, [2009] 3 R.C.S. vii, elle s’est refusée à interpréter l’art. 487.01 de façon restrictive. Elle a plutôt confirmé la nature réparatrice de la disposition en citant son arrêt *R. c. Lauda* (1998), 37 O.R. (3d) 513, p. 522‑523, conf. par [1998] 2 R.C.S. 683, où elle avait jugé que le mandat général permet une gamme souple de méthodes d’enquête; voir aussi *R. c. Noseworthy* (1997), 33 O.R. (3d) 641, p. 644.

1. Compte tenu de cette conception de l’objet de l’art. 487.01, j’en aborde l’interprétation différemment de mon collègue. Plus particulièrement, je rejette la prémisse voulant que cet article doive être interprété de façon à en restreindre sévèrement l’utilisation. L’examen porte sur deux points (outre, bien sûr, les motifs raisonnables de croire qu’une infraction a été commise et que l’autorisation demandée permettra d’obtenir des renseignements la concernant) : L’autorisation porte‑t‑elle sur l’utilisation d’« un dispositif ou une technique ou une méthode d’enquête » ou « l’accomplissement d’un [. . .] acte » prévu par une autre disposition législative fédérale et sert‑elle au mieux l’administration de la justice?
2. Si l’on délaisse l’objet de l’art. 487.01 pour s’attacher plus précisément à l’examen du texte et de l’objet de l’al. 487.01(1)*c*), la disposition ne met pas l’accent sur l’*objectif* d’une enquête mais sur les *moyens* de la réaliser. L’alinéa 487.01(1)*c*) prévoit qu’un mandat général peut être décerné « s’il n’y a aucune disposition [. . .] qui prévoie un mandat, une autorisation ou une ordonnance permettant une telle utilisation [d’un dispositif, une technique ou une méthode d’enquête] ou l’accomplissement d’un tel acte ». Les mots « une telle utilisation [d’un dispositif, une technique ou une méthode d’enquête] » et « l’accomplissement d’un tel acte » renvoient tous à *ce que* la police veut faire, non aux *raisons* motivant ce choix. Cet alinéa n’exige pas que le juge saisi examine s’il existe des techniques analogues et si elles permettent d’obtenir les mêmes éléments de preuve, mais simplement si *une telle utilisation* peut être autorisée par une autre disposition.
3. C’est ce raisonnement que la jurisprudence relative à cette disposition a toujours tenu, et c’est ce qu’a affirmé le juge MacPherson, dans *Ha*, lorsqu’il a indiqué ce qui suit, au par. 43 :

[traduction] L’analyse relative à l’al. 487.01(1)*c*) ne porte pas sur l’existence d’autres techniques d’enquête qui pourraient répondre aux besoins ou aux objectifs d’enquête de la police; elle porte plutôt sur la technique ou méthode d’enquête particulière que la police cherche à utiliser et sur la possibilité que cette utilisation puisse être autorisée par une autre disposition. [Je souligne.]

Il ne s’agit pas simplement d’une interprétation étroite et littérale de l’art. 487.01. Il s’agit plutôt d’une interprétation qui rend compte de son objet : l’octroi au juge du vaste pouvoir discrétionnaire d’autoriser la police « à utiliser un dispositif ou une technique ou une méthode d’enquête, ou à accomplir tout acte », pourvu, naturellement, que le juge soit convaincu que l’autorisation sert au mieux l’administration de la justice après avoir accordé l’importance voulue à la protection constitutionnelle contre les fouilles, perquisitions et saisies abusives. Je souscris entièrement à l’opinion du juge MacPherson, qui rendait le jugement de la Cour d’appel de l’Ontario dans *Ha*, lorsqu’il écrit qu’il ne voit [traduction] « aucune raison de principe justifiant que l’on s’acharne à restreindre la portée de l’art. 487.01 en y ajoutant des mots que le législateur n’y a pas expressément employés » (par. 37).

1. Je constate que le juge Moldaver s’appuie sur le même paragraphe de l’arrêt *Ha* pour affirmer que les objectifs d’enquête interviennent dans l’analyse relative à l’al. 487.01(1)*c*), sous‑entendant que, dans ce passage, le juge MacPherson a adopté une approche qui prend en compte les différences « de fond » entre les diverses techniques (par. 70). Lorsqu’on les considère dans leur intégralité, toutefois, les motifs du juge MacPherson n’appuient pas une telle affirmation. Le juge MacPherson, à mon sens, n’« expliqu[ait] [pas] en quoi la fouille autorisée [. . .] dans l’arrêt *Ha* était différente, sur le plan du fond, d’une fouille nécessitant plusieurs mandats ordinaires » (le juge Moldaver, par. 70). Cela ressort clairement non seulement du passage du paragraphe que j’ai cité précédemment, mais aussi de la façon dont le juge MacPherson résume sa conclusion au par. 41 : [traduction] « Il n’existe tout simplement aucune disposition [. . .] permettant d’autoriser un nombre illimité d’entrées et de fouilles clandestines dans une propriété privée pour une période de deux mois. » Le juge MacPherson a simplement comparé, dans son analyse relative à l’al. 487.01(1)*c*), la fouille ou perquisition pour laquelle la police demandait un mandat général avec d’autres dispositions en matière de fouilles et perquisitions, et il a conclu qu’aucune de ces dispositions n’autoriserait ce que la police cherchait à faire.
2. De la même façon, le juge Frankel, rendant jugement pour la cour dans *R. c. Brand*, 2008 BCCA 94, 229 C.C.C. (3d) 443 (*sub nom. R. c. Ford*), par. 50, a déclaré que [traduction] « [l]e recours à un mandat général n’est interdit que lorsque l’autorisation judiciaire de l’“utilisation” proposée ou l’“accomplissement d’un tel acte” pourrait être obtenue aux termes d’une autre disposition législative fédérale. » On ne trouve nulle part dans ses motifs d’indication qu’une analyse de l’équivalence fondamentale ou de la nécessité pour l’enquête est requise.
3. La comparaison de l’al. 487.01(1)*c*) avec l’al. 186(1)*b*), qui énonce l’exigence en matière de nécessité pour l’enquête à laquelle il faut satisfaire pour que l’écoute électronique soit autorisée, me conforte dans mon interprétation. Selon l’al. 186(1)*b*), l’autorisation visée ne peut être donnée que si le juge est convaincu que

d’autres méthodes d’enquête ont été essayées et ont échoué, ou ont peu de chance de succès, ou que l’urgence de l’affaire est telle qu’il ne serait pas pratique de mener l’enquête relative à l’infraction en n’utilisant que les autres méthodes d’enquête.

Dans *R. c. Araujo*, 2000 CSC 65, [2000] 2 R.C.S. 992, la Cour a posé qu’aux termes de l’al. 186(1)*b*), l’autorisation d’écoute électronique ne peut être accordée que si le juge est convaincu que « [s]ur le plan pratique » il n’existe « aucune autre méthode d’enquête raisonnable, dans les circonstances de l’enquête criminelle considérée » (par. 29 (soulignement omis)). Le législateur a prévu ici une norme élevée; il ne suffit pas que l’interception soit « plus efficace » que d’autres techniques utilisables, elle doit être *nécessaire* à l’enquête (*Araujo*,par. 39).

1. L’alinéa 487.01(1)*c*), par contre, exige uniquement que le juge soit convaincu qu’aucune disposition du *Code* ou d’une autre loi fédérale ne peut autoriser la technique envisagée. Il n’a pas à être convaincu en outre que la technique nouvelle est nécessaire à l’enquête ou qu’elle n’est pas équivalente sur le plan du fond à un procédé pouvant être autorisé par une autre disposition. Le législateur savait comment exiger que le juge examine la question de savoir si d’autres techniques d’enquête permettraient d’atteindre le but visé par l’enquête. Il l’a fait à l’al. 186(1)*b*). Mais il ne l’a pas fait à l’al. 487.01(1)*c*).
2. Évidemment, cela ne veut pas dire qu’un juge devrait autoriser tout ce que la police cherche à faire simplement parce que l’autorisation n’est pas prévue par un autre texte législatif. Son pouvoir discrétionnaire de décerner le mandat doit s’exercer en donnant pleinement effet à la protection des attentes raisonnables en matière de vie privée, comme l’établit l’abondante jurisprudence relative à l’art. 8 de la *Charte canadienne des droits et libertés*. L’exercice de ce pouvoir discrétionnaire du juge ne doit pas permettre à la police de recourir au mandat général pour échapper aux exigences en matière d’autorisation préalable que le législateur a imposées à l’égard de certaines techniques d’enquête. Ainsi que je vais l’expliquer, toutefois, j’estime que, lorsque la question surgit, elle relève directement et expressément de l’al. 487.01(1)*b*), non de l’al. 487.01(1)*c*) auquel on aurait ajouté par interprétation une restriction qui n’y est pas prévue.
3. Pour résumer ce point, l’inclusion à l’al. 487.01(1)*c*) d’un critère de « l’équivalent sur le plan du fond » n’est étayée ni par le texte de cette disposition, ni par son objet, ni par la jurisprudence. La question posée par cet alinéa est simple : Est‑ce qu’une loi fédérale prévoit « un mandat, une autorisation ou une ordonnance permettant une telle utilisation ou l’accomplissement d’un tel acte »? Lorsque cette condition préalable est respectée, le juge peut envisager d’accorder l’autorisation demandée. La question de savoir *s’il y a lieu* d’accorder l’autorisation demandée ne relève pas de cet alinéa. Ainsi que je l’expliquerai, pour déterminer s’il y a lieu de décerner un mandat général, il faut plutôt se tourner vers l’al. 487.01(1)*b*), lequel pose la question de savoir si la délivrance du mandat général servirait au mieux l’administration de la justice. J’estime que le texte et l’objet de la disposition de même que la jurisprudence étayent une telle approche, alors que celle que propose le juge Moldaver engendre aussi une incertitude inutile et détourne le juge de la question de la compatibilité de la technique visée par la demande d’autorisation avec le droit à la protection contre les fouilles, perquisitions et saisies abusives.
4. Abordons en premier lieu la question de l’incertitude. J’estime que la prévisibilité et la clarté du droit revêtent une importance particulière en matière d’autorisation judiciaire préalable de fouilles et de perquisitions. L’autorisation judiciaire préalable est un pilier de la protection garantie par la *Charte* contre les fouilles, perquisitions et saisies abusives. L’autorisation préalable n’a pas pour but premier de détecter après le fait des fouilles ou perquisitions abusives, mais d’en prévenir l’existence. Les exigences en matière d’autorisation préalable doivent être aussi claires que possible pour assurer l’entière protection du droit garanti par la *Charte*.
5. La clarté sert également un important objectif pratique. Contrairement à ce qui s’est produit en l’espèce, la contestation de l’autorisation préalable intervient généralement après le fait, lors du procès. Si elle est accueillie, elle compromet l’admissibilité de la preuve obtenue grâce à la fouille ou la perquisition autorisée. La police ne peut remédier après le fait à l’utilisation d’un procédé d’enquête dont l’autorisation est par la suite jugée viciée. C’est pourquoi la clarté du droit revêt une grande importance pratique pour les juges et juges de paix appelés à autoriser des fouilles ou perquisitions et pour les policiers qui demandent ces autorisations.
6. Je vois de sérieuses lacunes à cet égard dans l’interprétation retenue par mon collègue le juge Moldaver. Celle‑ci ne permet pas de déterminer quand une technique d’enquête équivaut fondamentalement à une autre et quand les différences touchent simplement la forme. Comme il en sera question dans la section suivante de mes motifs, l’application que fait mon collègue du critère de l’« équivalent sur le plan du fond » en l’espèce illustre cette incertitude.
7. J’estime en outre que cette interprétation de l’al. 487.01(1)*c*) n’aidera pas les juges saisis de demandes d’autorisation à donner effet à la protection contre les fouilles, perquisitions et saisies abusives garantie par la Constitution. Cette question doit s’examiner directement en fonction de l’al. 487.01(1)*b*), non par l’appréciation du degré de ressemblance entre deux techniques au moyen d’un exercice comparatif vague, inutile et en grande partie sémantique. Comme je l’exposerai, même lorsqu’on aborde directement la question en l’espèce, les arguments invoqués à l’encontre de l’autorisation du mandat général, à mon humble avis, ne convainquent pas.

2. La technique proposée est‑elle « l’équivalent sur le plan du fond » de l’interception?

1. Même si j’admettais (et ce n’est pas le cas) que l’al. 487.01(1)*c*) comporte une idée d’équivalence fondamentale de diverses techniques d’enquête, je ne conclurais pas que la technique visée par la demande d’autorisation en l’espèce équivaut fondamentalement à l’autorisation d’écoute électronique. Mon collègue le juge Moldaver est d’avis que le mandat général autorisait en l’espèce une technique constituant au fond une interception « car il permet *prospectivement* à la police d’accéder à des communications privées *futures* de façon *continue* pendant une période prolongée » et que, « [a]bstraction faite du délai de 24 heures, les techniques d’enquête étaient les mêmes » (par. 61 et 68 (en italique dans l’original)).
2. J’estime avec égards que cette affirmation n’est ni étayée par les faits ni conforme au droit.
3. S’agissant d’abord des faits, l’autorisation d’écoute électronique seule ne permettrait pas à la police d’obtenir les renseignements que Telus devait fournir en exécution du mandat général.  D’ailleurs, la preuve soumise par Telus montre qu’il faudrait trois autorisations distinctes pour que la police ait accès à l’information qu’elle recevrait grâce au mandat général.  Comme je l’ai expliqué précédemment, lorsque Telus donne suite à une autorisation d’écoute électronique, elle installe un dispositif qui réachemine en temps réel à la police une copie de tout message texte envoyé ou reçu par un numéro particulier. En l’espèce, le mandat général obligeait Telus à faire plus : elle devait extraire de ses bases de données des messages textes qui y étaient stockés et fournir, avec eux, les renseignements relatifs à l’abonné qui s’y rapportaient.
4. Dans l’affidavit qu’elle a déposé devant le juge siégeant en révision, une analyste en sécurité chez Telus, Corinne McNish a indiqué que trois autorisations différentes seraient nécessaires pour obtenir les renseignements demandés en vertu du mandat général : une autorisation prévue au par. 492.2(1) pour placer un téléphone sous enregistreur de numéros, une autorisation prévue au par. 492.2(2) pour obtenir des registres de téléphone, et une autorisation visée à la partie VI. J’ajouterais que, pour tirer parti d’une autorisation relevant de la partie VI, la police doit disposer d’une salle ou d’un poste d’écoute pour la réception des messages et affecter des agents au traitement de l’information entrante, au traitement des renseignements obtenus de l’enregistreur de numéros de téléphone et à l’examen des registres de téléphone.
5. Compte tenu de la preuve soumise par Telus elle‑même, il me semble plutôt exagéré d’affirmer que les techniques d’enquête étaient fondamentalement les mêmes.
6. En dépit de ces différences claires et importantes entre les deux techniques, mon collègue conclut à leur équivalence fondamentale en s’appuyant largement sur deux faits : le fait qu’en vertu du mandat général, l’accès de la police aux renseignements n’était décalé que de 24 heures, et le fait que le mandat général autorisait « prospectivement » la transmission des messages stockés. Selon moi, le premier fait est inexact, et le second n’étaye pas la conclusion qui en est tirée.
7. Pour ce qui est du délai, mon collègue estime que le temps écoulé entre le moment où les messages étaient envoyés et celui où la police devait les recevoir était si court que leur communication équivalait, sur le plan du fond, à une interception. Bien qu’il se refuse à indiquer combien de temps devrait s’écouler avant que la technique se différencie, sur le plan du fond, d’une interception, il conclut que « l’intervalle de 24 heures en l’espèce était insuffisant » (note de bas de page 2). Je ne suis pas d’accord avec lui pour deux raisons.
8. Premièrement, comme le mandat général lui‑même l’indique clairement, la réception de certains messages qui devaient être remis à la police pouvait être décalée de 72 heures, non de 24 heures. La communication ordonnée par le mandat général devait débuter le 30 mars 2010 et prendre fin le 16 avril de la même année. Le mardi 30 mars, Telus devait communiquer les renseignements se rapportant à la période du 18 au 30 mars, et le ministère public reconnaît que ces renseignements, qui pouvaient s’obtenir au moyen d’une ordonnance de communication, ne pouvaient faire l’objet d’un mandat général.  Relativement aux deux semaines et demie subséquentes, le mandat général créait deux intervalles différents, ainsi que je l’ai déjà indiqué. Du mardi au vendredi, Telus devait fournir chaque jour, à 14 h au plus tard, les messages envoyés et reçus entre 11 h la veille et 11 h le jour en cause. Pendant les week‑ends, toutefois, l’« intervalle » s’allongeait; les lundis, Telus devait fournir à 14 h au plus tard les messages stockés entre 11 h le vendredi précédent et 11 h le lundi. Ainsi, il y a eu 12 jours où la communication a été quotidienne, mais pour les six jours visés par le mandat général qui tombaient pendant un week‑end, l’« intervalle » passait à 72 heures. Il faut donc se demander si ce délai de 72 heures « était insuffisant » lui aussi et, s’il ne l’était pas, si la police aurait eu besoin d’autorisations différentes pour les messages qu’elle recevait le lundi et pour ceux qu’elle recevait les autres jours de la semaine.
9. Deuxièmement, parce que je partage l’avis du juge siégeant en révision selon lequel la police aurait pu obtenir une série d’ordonnances de communication quotidiennes, il m’est difficile d’accepter que l’« intervalle » de 24 heures sur lequel s’appuie le juge Moldaver fait du mandat général l’équivalent, sur le plan du fond, d’une interception. Une telle série d’ordonnances aurait fourni à la police des copies des messages textes dans les 24 heures suivant leur envoi. Compte tenu de ce qui est, sur le plan du fond, une interception, selon mon collègue, certaines ordonnances de communication pourraient donc équivaloir elles aussi à des interceptions. Cela fait ressortir, selon moi, la confusion et l’incertitude inhérentes à l’application du concept d’équivalence à l’al. 487.01(1)*c*) sur le plan du fond.
10. Le deuxième fait sur lequel repose la conclusion d’équivalence sur le plan du fond est la nature « prospective » de l’autorisation. Comme je l’ai déjà indiqué, toutefois, on comprend difficilement de quelle façon, exactement, une même technique peut ou non équivaloir à une interception selon le moment où elle est autorisée. Si, pour les besoins du présent pourvoi, nous reconnaissons — ce que je fais — que la police pouvait légalement obtenir des ordonnances quotidiennes de communication, il est tout simplement incompréhensible que le fait d’autoriser cette technique deux semaines plus tôt convertisse l’ordonnance de communication en une autorisation d’écoute électronique.
11. Enfin, la conclusion d’équivalence sur le plan du fond est incompatible avec le texte des dispositions relatives à l’écoute électronique et le régime qu’elles établissent. Comme je l’ai déjà expliqué en détail, la divulgation de communications privées déjà interceptées est considérée et traitée, au *Code*, comme un acte distinct de l’interception elle‑même. Je ne puis donc voir une simple différence de forme dans une distinction à laquelle le législateur a attaché valeur juridique.
12. En résumé, je suis d’avis que, même si l’on acceptait l’ajout par interprétation, à l’al. 487.01(1)*c*), d’un critère de « l’équivalent sur le plan du fond », ni les faits ni le droit n’étayent son application en l’espèce.
13. Cela souligne aussi, selon moi, la confusion et l’incertitude qu’engendrerait l’adoption d’un tel critère. Mon collègue ne fournit aucune indication utile sur ce point, exception faite de celle qui concerne l’« intervalle » de 24 heures, qui est d’ailleurs problématique parce qu’elle entre en conflit avec la possibilité d’obtenir des ordonnances quotidiennes de communication en vertu de l’art. 487.012. À mon avis, il ne faut pas laisser aux juges saisis de demandes d’autorisation et aux enquêteurs de la police le soin de tirer eux‑mêmes la ligne en espérant, sans avoir beaucoup de motifs d’optimisme, qu’à l’issue d’un voir‑dire on leur donnera raison au procès.

3. Le recours abusif au mandat général

1. Nous en arrivons au véritable nœud de la question : Fallait‑il refuser de décerner le mandat général parce qu’il constituait, comme le laisse entendre mon collègue, un « recours abusif » à l’art. 487.01, une « solution facile », une « façon commode », un « moyen », ou un « moyen détourné » qui permet à la police « de contourner les exigences » de la partie VI? (par. 72, 81, 90 et 105). D’après ce que je comprends des motifs du juge Moldaver, il arrive à cette interprétation de l’al. 487.01(1)*c*) en raison de la nécessité d’empêcher l’exercice abusif du pouvoir de décerner un mandat général.  J’admets que le juge saisi d’une demande de mandat général doit veiller à ce que toute technique d’enquête autorisée respecte entièrement le droit à la protection contre les fouilles, perquisitions et saisies abusives. Toutefois, j’estime que cette analyse doit relever directement de l’al. 487.01(1)*b*), et non passer par le prisme d’une interrogation sur l’équivalence de deux techniques sur le plan du fond.
2. Comme le juge MacPherson l’a judicieusement fait remarquer dans *Ha*, la condition énoncée à l’al. 487.01(1)*c*) qu’il n’y ait « aucune disposition » n’est pas la seule qui doive être respectée pour qu’un mandat général soit décerné  (par. 44). Il ne faut pas aborder cet article en supposant que le législateur voulait que chaque technique d’enquête non autorisée ailleurs puisse être autorisée en vertu du par. 487.01(1) : voir, p. ex., S. Coughlan, « *R. v. Ha* : Upholding General Warrants without Asking the Right Questions » (2009), 65 C.R. (6th) 41. Il faut plutôt que le juge saisi de la demande de mandat soit également convaincu que l’autorisation de la technique en cause sert au mieux l’administration de la justice (al. 487.01(1)*b*)). Selon moi, c’est sous l’autorité de cette disposition que s’examine la question des recours potentiellement abusifs au mandat général.  Naturellement, même lorsque les conditions énoncées aux al. 487.01(1)*b*) et *c*) sont respectées, il faut, conformément au par. 487.01(3), que le mandat général énonce « les modalités que le juge estime opportunes pour que la fouille, la perquisition ou la saisie soit raisonnable dans les circonstances ».
3. L’alinéa 487.01(1)*b*) n’a pas été invoqué dans le présent pourvoi et je ne veux pas le commenter longuement, sauf pour dire qu’il s’agit, à mon avis, de la partie de l’art. 487.01 qui permet d’aborder les préoccupations liées à l’opportunité d’autoriser une nouvelle technique d’enquête. Cela dit, j’estime que les préoccupations évoquées par le juge Moldaver lorsqu’il propose le critère de l’« équivalent sur le plan du fond » ne sont pas du tout convaincantes.
4. Premièrement, je ne suis pas prêt à conclure que la demande de la police visant à obtenir un mandat général en l’espèce était une « façon commode » de contourner les exigences de la partie VI. Bien entendu, cela n’a pas été prouvé. Deuxièmement, je ne souscris pas à l’affirmation que les droits à la vie privée qui sont en jeu en l’espèce et lors d’une demande d’autorisation d’écoute électronique sont exactement les mêmes. Le juge siégeant en révision a estimé que des ordonnances de communication quotidiennes pouvaient être accordées pour permettre à la police d’obtenir des copies de messages stockés, et je suis d’accord avec lui. Je ne vois pas comment les droits au respect de la vie privée en cause diffèrent si l’autorisation de procéder ainsi est donnée deux semaines à l’avance. Troisièmement, pour tous les motifs formulés par le juge siégeant en révision, il était plus pratique de recourir au mandat général que de demander une série d’ordonnances de communication. Quatrièmement, le mandat général a autorisé une technique qui, outre qu’elle différait d’une interception, répondait mieux aux besoins de la police. Plus particulièrement, elle était beaucoup moins onéreuse en termes de ressources policières, du fait qu’elle n’obligeait pas la police à affecter du personnel à une salle d’écoute et à extraire les renseignements des registres d’abonnés et des enregistreurs de numéros. À mon avis, le mandat général permettait l’atteinte des objectifs légitimes de l’enquête policière de façon beaucoup plus pratique et économique que ce qui aurait pu être autorisé en vertu de toute autre disposition.
5. Bien sûr, le mandat général avait pour effet de transférer les coûts à Telus. Cependant, cela n’a rien à voir avec le droit à la vie privée des abonnés. Qui plus est, le juge siégeant en révision a catégoriquement rejeté la preuve et les arguments de Telus se rapportant au fardeau que le mandat général lui imposait, et Telus ne les a pas présentés devant nous.
6. Dans le dossier qui nous a été soumis, je ne vois pas de preuve de « recours abusif » à l’art. 487.01 ou de tentative par la police de « contourner les exigences » de la partie VI. Je constate plutôt qu’un service de police municipal de taille plutôt réduite a mené une enquête de façon efficace et pratique, en respectant pleinement le droit à la vie privée des personnes visées par l’enquête ainsi que des autres abonnés de Telus.

C. *Conclusion*

1. Pour ces motifs, je suis d’avis que le mandat général n’a pas autorisé une interception nécessitant une autorisation d’écoute électronique sous le régime de la partie VI et que la condition qu’il n’y ait « aucune disposition », énoncée à l’al. 487.01(1)*c*), a été respectée.

IV. Dispositif

1. Je suis d’avis de rejeter le pourvoi.

**ANNEXE**

*Code criminel*, L.R.C. 1985, ch. C‑46

PARTIE VI

ATTEINTES À LA VIE PRIVÉE

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

. . .

« 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 auteur la destine.

. . .

« 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.

. . .

**184.**(1)Est coupable d’un acte criminel et passible d’un emprisonnement maximal de cinq ans quiconque, au moyen d’un dispositif électromagnétique, acoustique, mécanique ou autre, intercepte volontairement une communication privée.

(2) Le paragraphe (1) ne s’applique pas aux personnes suivantes :

*a*) une personne qui a obtenu, de l’auteur de la communication privée ou de la personne à laquelle son auteur la destine, son consentement exprès ou tacite à l’interception;

*b*) une personne qui intercepte une communication privée en conformité avec une autorisation ou en vertu de l’article 184.4, ou une personne qui, de bonne foi, aide de quelque façon une autre personne qu’elle croit, en se fondant sur des motifs raisonnables, agir en conformité avec une telle autorisation ou en vertu de cet article;

*c*) une personne qui fournit au public un service de communications téléphoniques, télégraphiques ou autres et qui intercepte une communication privée dans l’un ou l’autre des cas suivants :

(i) cette interception est nécessaire pour la fourniture de ce service,

(ii) à l’occasion de la surveillance du service ou d’un contrôle au hasard nécessaire pour les vérifications mécaniques ou la vérification de la qualité du service,

(iii) cette interception est nécessaire pour protéger ses droits ou biens directement liés à la fourniture d’un service de communications téléphoniques, télégraphiques ou autres;

*d*) un fonctionnaire ou un préposé de Sa Majesté du chef du Canada chargé de la régulation du spectre des fréquences de radiocommunication, pour une communication privée qu’il a interceptée en vue d’identifier, d’isoler ou d’empêcher l’utilisation non autorisée ou importune d’une fréquence ou d’une transmission;

*e*) une personne — ou toute personne agissant pour son compte — qui, étant en possession ou responsable d’un ordinateur — au sens du paragraphe 342.1(2) —, intercepte des communications privées qui sont destinées à celui‑ci, en proviennent ou passent par lui, si l’interception est raisonnablement nécessaire :

(i) soit pour la gestion de la qualité du service de l’ordinateur en ce qui concerne les facteurs de qualité tels que la réactivité et la capacité de l’ordinateur ainsi que l’intégrité et la disponibilité de celui‑ci et des données,

(ii) soit pour la protection de l’ordinateur contre tout acte qui constituerait une infraction aux paragraphes 342.1(1) ou 430(1.1).

(3) La communication privée interceptée par la personne visée à l’alinéa (2)*e*) ne peut être utilisée ou conservée que si, selon le cas :

*a*) elle est essentielle pour détecter, isoler ou empêcher des activités dommageables pour l’ordinateur;

*b*) elle sera divulguée dans un cas visé au paragraphe 193(2).

. . .

**185.**(1) Pour l’obtention d’une autorisation visée à l’article 186, une demande est présentée *ex parte* et par écrit à un juge d’une cour supérieure de juridiction criminelle, ou à un juge au sens de l’article 552, et est signée par le procureur général de la province ou par le ministre de la Sécurité publique et de la Protection civile ou par un mandataire spécialement désigné par écrit pour l’application du présent article par :

*a*) le ministre lui‑même ou le sous‑ministre de la Sécurité publique et de la Protection civile lui‑même, si l’infraction faisant l’objet de l’enquête est une infraction pour laquelle des poursuites peuvent, le cas échéant, être engagées sur l’instance du gouvernement du Canada et conduites par le procureur général du Canada ou en son nom;

*b*) le procureur général d’une province lui‑même ou le sous‑procureur général d’une province lui‑même, dans les autres cas;

il doit y être joint un affidavit d’un agent de la paix ou d’un fonctionnaire public pouvant être fait sur la foi de renseignements tenus pour véridiques et indiquant ce qui suit :

*c*) les faits sur lesquels le déclarant se fonde pour justifier qu’à son avis il y a lieu d’accorder une autorisation, ainsi que les détails relatifs à l’infraction;

*d*) le genre de communication privée que l’on se propose d’intercepter;

*e*) les noms, adresses et professions, s’ils sont connus, de toutes les personnes dont les communications privées devraient être interceptées du fait qu’on a des motifs raisonnables de croire que cette interception pourra être utile à l’enquête relative à l’infraction et une description générale de la nature et de la situation du lieu, s’il est connu, où l’on se propose d’intercepter des communications privées et une description générale de la façon dont on se propose de procéder à cette interception;

. . .

*h*) si d’autres méthodes d’enquête ont ou non été essayées, si elles ont ou non échoué, ou pourquoi elles paraissent avoir peu de chance de succès, ou si, étant donné l’urgence de l’affaire, il ne serait pas pratique de mener l’enquête relative à l’infraction en n’utilisant que les autres méthodes d’enquête.

. . .

**186.** (1) Une autorisation visée au présent article peut être donnée si le juge auquel la demande est présentée est convaincu que :

*a*) d’une part, l’octroi de cette autorisation servirait au mieux l’administration de la justice;

*b*) d’autre part, d’autres méthodes d’enquête ont été essayées et ont échoué, ou ont peu de chance de succès, ou que l’urgence de l’affaire est telle qu’il ne serait pas pratique de mener l’enquête relative à l’infraction en n’utilisant que les autres méthodes d’enquête.

. . .

(4)Une autorisation doit :

*a*) indiquer l’infraction relativement à laquelle des communications privées pourront être interceptées;

*b*) indiquer le genre de communication privée qui pourra être interceptée;

*c*) indiquer, si elle est connue, l’identité des personnes dont les communications privées doivent être interceptées et donner une description générale du lieu où les communications privées pourront être interceptées, s’il est possible de donner une description générale de ce lieu, et une description générale de la façon dont les communications pourront être interceptées;

*d*) énoncer les modalités que le juge estime opportunes dans l’intérêt public;

*e*)  être valide pour la période maximale de soixante jours qui y est indiquée.

. . .

**193.** (1) Lorsqu’une communication privée a été interceptée au moyen d’un dispositif électromagnétique, acoustique, mécanique ou autre sans le consentement, exprès ou tacite, de son auteur ou de la personne à laquelle son auteur la destinait, quiconque, selon le cas :

a) utilise ou divulgue volontairement tout ou partie de cette communication privée, ou la substance, le sens ou l’objet de tout ou partie de celle‑ci;

b) en divulgue volontairement l’existence,

sans le consentement exprès de son auteur ou de la personne à laquelle son auteur la destinait, est coupable d’un acte criminel et passible d’un emprisonnement maximal de deux ans.

(2) Le paragraphe (1) ne s’applique pas à une personne qui divulgue soit tout ou partie d’une communication privée, ou la substance, le sens ou l’objet de tout ou partie de celle‑ci, soit l’existence d’une communication privée :

a) au cours ou aux fins d’une déposition lors de poursuites civiles ou pénales ou de toutes autres procédures dans lesquelles elle peut être requise de déposer sous serment;

b) au cours ou aux fins d’une enquête en matière pénale, si la communication privée a été interceptée légalement;

c) en donnant le préavis visé à l’article 189 ou en fournissant des détails complémentaires en application d’une ordonnance rendue en vertu de l’article 190;

d) au cours de l’exploitation :

(i) soit d’un service de communications téléphoniques, télégraphiques ou autres à l’usage du public,

(ii) soit d’un ministère ou organisme du gouvernement du Canada,

(iii) soit d’un service de gestion ou de protection d’un ordinateur — au sens du paragraphe 342.1(2) —,

si la divulgation est nécessairement accessoire à une interception visée aux alinéas 184(2)c), d) ou e);

e) lorsque la divulgation est faite à un agent de la paix ou à un poursuivant au Canada ou à une personne ou un organisme étranger chargé de la recherche ou de la poursuite des infractions et vise à servir l’administration de la justice au Canada ou ailleurs;

f) lorsque la divulgation est faite au directeur du Service canadien du renseignement de sécurité ou à un employé du Service et vise à permettre au Service d’exercer les fonctions qui lui sont conférées en vertu de l’article 12 de la *Loi sur le Service canadien du renseignement de sécurité*.

. . .

PARTIE XV

Procédure et pouvoirs spéciaux

. . .

**487.** (1) Un juge de paix qui est convaincu, à la suite d’une dénonciation faite sous serment selon la formule 1, qu’il existe des motifs raisonnables de croire que, dans un bâtiment, contenant ou lieu, se trouve, selon le cas :

*a*) une chose à l’égard de laquelle une infraction à la présente loi, ou à toute autre loi fédérale, a été commise ou est présumée avoir été commise;

*b*) une chose dont on a des motifs raisonnables de croire qu’elle fournira une preuve touchant la commission d’une infraction ou révélera l’endroit où se trouve la personne qui est présumée avoir commis une infraction à la présente loi, ou à toute autre loi fédérale;

*c*) une chose dont on a des motifs raisonnables de croire qu’elle est destinée à servir aux fins de la perpétration d’une infraction contre la personne, pour laquelle un individu peut être arrêté sans mandat;

*c.1*) un bien infractionnel,

peut à tout moment décerner un mandat autorisant un agent de la paix ou, dans le cas d’un fonctionnaire public nommé ou désigné pour l’application ou l’exécution d’une loi fédérale ou provinciale et chargé notamment de faire observer la présente loi ou toute autre loi fédérale, celui qui y est nommé :

*d*) d’une part, à faire une perquisition dans ce bâtiment, contenant ou lieu, pour rechercher cette chose et la saisir;

*e*) d’autre part, sous réserve de toute autre loi fédérale, dans les plus brefs délais possible, à transporter la chose devant le juge de paix ou un autre juge de paix de la même circonscription territoriale ou en faire rapport, en conformité avec l’article 489.1.

(2) Lorsque le bâtiment, contenant ou lieu est situé dans une autre circonscription territoriale, le juge de paix peut délivrer son mandat dans la même forme, modifiée selon les circonstances, et celui‑ci peut être exécuté dans l’autre circonscription territoriale après avoir été visé, selon la formule 28, par un juge de paix ayant juridiction dans cette circonscription; le visa est apposé sur l’original du mandat ou sur une copie transmise à l’aide d’un moyen de télécommunication.

(2.1) La personne autorisée à perquisitionner des données contenues dans un ordinateur se trouvant dans un lieu ou un bâtiment peut :

*a*) utiliser ou faire utiliser tout ordinateur s’y trouvant pour vérifier les données que celui‑ci contient ou auxquelles il donne accès;

*b*) reproduire ou faire reproduire des données sous forme d’imprimé ou toute autre forme intelligible;

*c*) saisir tout imprimé ou sortie de données pour examen ou reproduction;

*d*) utiliser ou faire utiliser le matériel s’y trouvant pour reproduire des données.

. . .

**487.01** (1) Un juge de la cour provinciale, un juge de la cour supérieure de juridiction criminelle ou un juge au sens de l’article 552 peut décerner un mandat par écrit autorisant un agent de la paix, sous réserve du présent article, à utiliser un dispositif ou une technique ou une méthode d’enquête, ou à accomplir tout acte qui y est mentionné, qui constituerait sans cette autorisation une fouille, une perquisition ou une saisie abusive à l’égard d’une personne ou d’un bien :

*a*) si le juge est convaincu, à la suite d’une dénonciation par écrit faite sous serment, qu’il existe des motifs raisonnables de croire qu’une infraction à la présente loi ou à toute autre loi fédérale a été ou sera commise et que des renseignements relatifs à l’infraction seront obtenus grâce à une telle utilisation ou à l’accomplissement d’un tel acte;

*b*) s’il est convaincu que la délivrance du mandat servirait au mieux l’administration de la justice;

*c*) s’il n’y a aucune disposition dans la présente loi ou toute autre loi fédérale qui prévoie un mandat, une autorisation ou une ordonnance permettant une telle utilisation ou l’accomplissement d’un tel acte.

. . .

(3) Le mandat doit énoncer les modalités que le juge estime opportunes pour que la fouille, la perquisition ou la saisie soit raisonnable dans les circonstances.

. . .

(5.1) Le mandat qui autorise l’agent de la paix à perquisitionner secrètement doit exiger, dans le cadre des modalités visées au paragraphe (3), qu’un avis de la perquisition soit donné dans le délai suivant son exécution que le juge estime indiqué dans les circonstances.

. . .

**487.012** (1) Sauf si elle fait l’objet d’une enquête relative à l’infraction visée à l’alinéa (3)*a*), un juge de paix ou un juge peut ordonner à une personne :

*a*) de communiquer des documents — originaux ou copies certifiées conformes par affidavit — ou des données;

*b*) de préparer un document à partir de documents ou données existants et de le communiquer.

(2) L’ordonnance précise le moment, le lieu et la forme de la communication ainsi que la personne à qui elle est faite — agent de la paix ou fonctionnaire public nommé ou désigné pour l’application ou l’exécution d’une loi fédérale ou provinciale et chargé notamment de faire observer la présente loi ou toute autre loi fédérale.

(3) Le juge de paix ou le juge ne rend l’ordonnance que s’il est convaincu, à la suite d’une dénonciation par écrit faite sous serment et présentée *ex parte*, qu’il existe des motifs raisonnables de croire que les conditions suivantes sont réunies :

*a*) une infraction à la présente loi ou à toute autre loi fédérale a été ou est présumée avoir été commise;

*b*) les documents ou données fourniront une preuve touchant la perpétration de l’infraction;

*c*) les documents ou données sont en la possession de la personne en cause ou à sa disposition.

(4) L’ordonnance peut être assortie des conditions que le juge de paix ou le juge estime indiquées, notamment pour protéger les communications privilégiées entre l’avocat — et, dans la province de Québec, le notaire — et son client.

*Pourvoi accueilli, la juge en chef* McLachlin *et le juge* Cromwell *sont dissidents.*

Procureurs de l’appelante : Stockwoods, Toronto.

Procureur de l’intimée : Service des poursuites pénales du Canada, Toronto.

Procureur de l’intervenant le procureur général de l’Ontario : Procureur général de l’Ontario, Toronto.

Procureurs de l’intervenante l’Association canadienne des libertés civiles : Torys, Toronto.

Procureur de l’intervenante la Clinique d’intérêt public et de politique d’Internet du Canada Samuelson‑Glushko : Université d’Ottawa, Ottawa.

1. La validité d’une série d’ordonnances de communication quotidiennes (ou plus fréquentes) n’a pas été contestée par les parties. Il n’est pas non plus nécessaire d’examiner cette question pour trancher le présent pourvoi. Par conséquent, je ne déterminerai pas si la Constitution ou une loi empêche la police de solliciter des ordonnances de cette nature. [↑](#footnote-ref-1)
2. Il n’est ni prudent ni nécessaire d’établir précisément en l’espèce à quel moment le délai modifierait la technique de la fouille sur le fond de façon à ce qu’un mandat général soit acceptable. Quel que soit le délai, l’intervalle de 24 heures en l’espèce était insuffisant. Dans la mesure où une affaire ultérieure présente une incertitude, elle doit être dissipée conformément à l’interprétation de l’al. 487.01(1)*c*) formulée en l’espèce. Je relève en outre que mon collègue le juge Cromwell insiste beaucoup sur le fait que « la réception de certains messages qui devaient être remis à la police pouvait être décalée de 72 heures, non de 24 heures » (par. 183). Avec égards, je ne comprends pas pourquoi il insiste sur ce fait. Même à supposer qu’un délai de 72 heures diffère d’une interception sur le plan du fond, il ne s’ensuit pas pour autant que l’autorisation intégrale doive être maintenue en vigueur parce qu’un élément d’une autorisation par ailleurs illégale est valide. [↑](#footnote-ref-2)
3. Le dossier en l’espèce porte à croire que tous les renseignements sollicités par la police auraient pu être obtenus conformément à une autorisation visée par la partie VI, à l’autorisation d’utiliser un enregistreur de numéro sur le fondement du par. 492.2(1) et à une ordonnance en vue d’obtenir un registre de téléphone fondée sur le par. 492.2(2). Devant notre Cour, aucune des parties ne s’est penchée sur ces deux dernières autorisations; les parties se sont plutôt attardées sur la question de savoir si l’essence du mandat — la communication de messages textes — constituait une interception. [↑](#footnote-ref-3)