L'expectative raisonnable de vie privée et les principaux contextes de communications dans Internet

François BLANCHETTE

Maître en droit (LL.M.)
Faculté de droit de Montréal
Mémoire réalisé sous la direction du Professeur Pierre Trudel

Décembre 2001

Contact : francois.blanchette@justice.gc.ca

Plan

Introduction

Partie 1 - Les grands principes généralement reconnus en matière d'expectative raisonnable de vie privée

Chapitre I - Les dispositions législatives principales et le concept de droit à la vie privée

Section I - L'article 32 de la *Charte canadienne*

Section II - L'article 8 de la *Charte canadienne*

Section III - Les paragraphes 24(1) et (2) de la *Charte canadienne*

Section IV - Bref rappel historique de la genèse de la notion d'expectative raisonnable de vie privée en droit criminel au Canada

Section V - Principes fondamentaux de la protection offerte par l'article 8 de la *Charte canadienne*

Section VI - Une définition possible du concept de droit à la vie privée?

Chapitre II - La détermination de l'expectative raisonnable de vie privée et l'approche de principe

Section I - L'arrêt *Dyment* et la naissance des sphères d'intimité

Section II - L'arrêt *Duarte* et le rejet de l'analyse fondée sur le risque

Section III - L'arrêt *Wong* et le début de la fin de l'approche de principe

Chapitre III - La détermination de l'expectative raisonnable de vie privée et l'approche pragmatique ou au cas par cas

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>

Juriscom.net
droit des technologies de l'information

Section I - L'approche de principe s'effrite de plus en plus dans l'arrêt *R. c. Wise*

Section II - L'approche pragmatique ou au cas par cas se précise davantage dans l'arrêt *Plant*

Section III - L'approche pragmatique ou au cas par cas et la notion d'intérêt à soulever une violation constitutionnelle consacrée dans l'arrêt *Edwards*

Section IV - Conclusion quant à l'approche pragmatique ou au cas par cas

Chapitre IV - L'expectative raisonnable de vie privée inexistante, reconnue ou réduite?

Section I - Exemples de cas où l'expectative raisonnable de vie privée est inexistante

Section II - Exemples de cas où l'expectative raisonnable de vie privée a été reconnue

Section III - Exemples de cas où l'expectative raisonnable de vie privée est réduite

Chapitre V - La protection « *post* immixtion » de la vie privée

Section I - L'autorisation par la loi

Section II - Le caractère non abusif ou raisonnable de l'autorisation légale

Section III - La détermination du caractère non abusif de l'immixtion dans une expectative raisonnable de vie privée

Chapitre VI - La protection statutaire de la vie privée en matière de « communication privée » et de correspondance

Section I - Les définitions à la base de la protection accordée par le *Code criminel*

Section II - La distinction entre une « communication privée » et une communication bénéficiant d'une expectative raisonnable de vie privée est-elle académique?

Section III - L'interception d'une « communication privée »

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>

Juriscom.net
droit des technologies de l'information

Section IV - L'interception d'une communication privée dans le contexte de l'obtention de courriels en attente de livraison en droit américain

Section V - La protection de la correspondance

Partie II - Identification et explication des contextes techniques apportés par les nouvelles TI et Internet

Chapitre I - Les contextes techniques généraux apportés par l'utilisation de l'informatique, d'Internet et des nouvelles TI

Section I - Le contexte de l'évolution des technologies en matière de communication

Section II - Le contexte de l'utilisation de l'informatique, d'Internet et des nouvelles TI

Section III - La Cour suprême américaine décrit Internet

Section IV - Le contexte technique d'Internet

Section V - Le contexte du branchement à Internet

Section VI - Le contexte territorial ou juridictionnel d'Internet et la notion d'ubiquité

Chapitre II - Les contextes techniques particuliers de communication apportés par Internet et les nouvelles TI

Section I - Le Web

Section II - Le courriel

Section III - Le transfert de fichiers FTP

Section IV - Les groupes de discussions ou nouvelles *Usenet*

Section V - Les sessions en mode terminal *Telnet*

Section VI - Le bavardage-clavier ou clavardage du service IRC

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>

Juriscom.net droit des technologies de l'information

Section VII - La téléphonie et vidéoconférence Internet

Section VIII - La messagerie instantanée

Chapitre III- Les technologies particulières ayant une influence sur le caractère privé des communications effectuées dans les divers contextes apportés par Internet et les nouvelles TI

Section I - La cryptographie

Section II - La stéganographie

Section III - Techniques favorisant l'anonymat

Partie III- Les nouveaux facteurs émanant des contextes apportés par Internet et les nouvelles TI influant sur le niveau d'expectative raisonnable de vie privée

Conclusion

Bibliographie

Annexes

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>

Introduction

L'informatique est de plus en plus populaire dans toutes les couches de la société[1]. Les nouvelles technologies de l'information et des communications[2] contribuent largement à cet essor, notamment par l'utilisation grandissante d'Internet[3]. Il est raisonnable d'affirmer que,

---

1 *Reno c. ACLU,* 521 U.S. 844 (1997), à la p. 850, [ci-après *Reno c. ACLU*] qui confirmait déjà l'augmentation fulgurante de l'utilisation d'Internet :

> « *The Internet has experienced "extraordinary growth."(5) The number of "host" computers—those that store information and relay communications—increased from about 300 in 1981 to approximately 9,400,000 by the time of the trial in 1996. Roughly 60% of these hosts are located in the United States. About 40 million people used the Internet at the time of trial, a number that is expected to mushroom to 200 million by 1999.* »

Le nombre d'utilisateurs d'Internet aux États-Unis était évalué en décembre 2000, à 164,4 millions : *NUA Internet Surveys*, *NUA*, en ligne : <http://www.nua.com/surveys/how_many_online/n_america.html> (date d'accès : 12 août 2001). Pour une étude de l'évolution des statistiques visant le Canada voir Canada, Statistique Canada, *Être branché ou ne pas l'être : croissance de l'utilisation des services de communication par ordinateur*, Ottawa, Indicateurs des services, 63F0002XPB no 27, novembre 1999, aux pp. 2-3 (Auteurs : P. Dickinson et J. Ellison). Cette étude évalue à 4,3 millions, le nombre de ménages canadiens qui utilisent régulièrement Internet. En décembre 1999, on évaluait à 13,28 millions, le nombre d'utilisateurs adultes (plus de 16 ans) d'Internet au Canada. *NUA Internet Surveys*, en ligne : <http://www.nua.com/surveys/how_many_online/n_america.html> (date d'accès : 12 août 2001). Ce nombre serait passé à un peu plus de 14 millions en juin 2001. *Media Metrix Canada release June 2001,* communiqué, « *Total Canada at Home Web Use Report on Internet Usage Stats* », (25 juillet 2001), *Media Metrix*, en ligne : <http://ca.mediametrix.com/press/releases/20010725.jsp> (date d'accès : 12 août 2001). Voir également Ipsos-Reid Canada, communiqué, « *Canadian Internet access continues to grow, and users say the Net has had a significant impact on their lives* », (26 juillet 2000), Ipsos-Reid, en ligne : <http://www.angusreid.com/media/content/displaypr.cfm?id_to_view=1061> (date d'accès :12 août 2001), qui tend également à confirmer cette évolution et le nombre d'utilisateurs pour le Canada. Nous voulons préciser ici que nous avons utilisé le *Manuel canadien de la référence juridique,* 4e édition, pour les références de la présente étude. Pour alléger les notes de bas de page, nous avons par contre décidé de n'indiquer dans le texte, que les références Internet, autres que la jurisprudence. On pourra toujours trouver les références Internet de la jurisprudence dans la bibliographie à la fin de l'étude. Si le texte est lu à partir d'un ordinateur branché à Internet, toutes les références indiquant un lien hypertexte sont accessibles, dans la mesure où la version du logiciel du traitement de texte utilisé, donne accès aux liens hypertextes. Il s'agit donc de références dynamiques.

2 L'expression « technologie de l'information » signifie l'ensemble du matériel, des logiciels et des services utilisés pour la collecte, le traitement et la transmission de l'information. Le *matériel* comprend notamment les claviers, imprimantes, télécopieurs et autres périphériques d'entrée ou de sortie des données. Par *logiciels*, on entend les logiciels d'application (traitement de texte, par exemple), mais aussi les systèmes d'exploitation et autres progiciels, gestionnaires de réseaux, outils de développement, didacticiels et pilotes de périphériques. Enfin, les *services* sont principalement ceux qui sont offerts dans les sites inforoutiers pour accéder à des bases de données, faire des transactions commerciales, échanger des documents de toutes sortes, obtenir du soutien technique, etc. Par exemple, ces services peuvent faire appel à la reconnaissance vocale, à l'animation vidéo ou aux écrans tactiles. Ils correspondent souvent à la version automatisée de services fournis autrefois de manière plus personnalisée. Office de la langue française, 2001, *s.v.* « technologie de l'information », en ligne : <http://www.olf.gouv.qc.ca/ressources/internet/fiches/8875723.htm>. Le concept de « nouvelles technologies de l'information et de la communication » est apparu pour marquer l'évolution fulgurante qu'ont connue les technologies de l'information avec l'avènement des autoroutes de l'information (notamment l'utilisation d'Internet) et l'explosion du multimédia. Office de la langue française, 2001, *s.v.* « nouvelle technologie de l'information et des communications », en ligne : <http://www.olf.gouv.qc.ca/technologies.html#expression> (date d'accès : 21 février 2001). Nous utiliserons désormais l'acronyme « nouvelles TI » pour désigner nouvelles technologies de l'information et de la communication.

3 Le terme Internet a été formé à partir de l'anglais *INTERconnected NETworks* (ou de *INTERconnection of NETworks*, selon certains) équivalant à *réseaux interconnectés* (ou à *interconnexion de réseaux*). Office de la

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

plus il y aura d'utilisateurs, plus le potentiel d'usages malveillants augmentera. Les organismes d'application de la loi seront donc appelés de plus en plus à mener des enquêtes dans des contextes informatiques. Certains crimes traditionnels seront facilités par Internet et les nouvelles TI. D'autres, propres à l'informatique, ne pourront être commis que par son biais.

Les méthodes d'enquête devront conséquemment s'adapter à cette nouvelle réalité technologique. Certaines méthodes d'enquête, notamment la surveillance électronique, devront être effectuées dans des contextes techniques encore aujourd'hui inexplorés par le droit.

La surveillance électronique peut entraîner une immixtion[4] dans une quelconque expectative raisonnable de vie privée. Un individu bénéficiant d'une expectative raisonnable de vie privée, sera protégé contre les immixtions injustifiées de l'État. La détermination de ce qui constitue une situation où un individu doit effectivement être protégé contre les immixtions de l'État, constitue le nœud du problème. À ce jour, la majorité des cas où la Cour suprême du Canada a dû déterminer s'il existait ou non une telle expectative, l'ont été alors que les nouvelles TI et Internet n'existaient pas encore. L'étude des contextes apportés par les nouvelles TI et Internet devient donc nécessaire afin d'être en mesure de prévoir si l'on peut bénéficier ou non de la protection contre les immixtions injustifiées de l'État et, dans quelle mesure cette protection trouve application.

Le problème à la base de cette étude est donc celui de l'impact des nouvelles TI et d'Internet sur le concept d'expectative raisonnable de vie privée existant en droit canadien. Ce concept découle de la protection constitutionnelle, accordée par l'article 8 de la *Charte canadienne des droits et libertés*[5], contre les fouilles saisies et perquisitions abusives. En pratique, cette protection se concrétise généralement par la nécessité d'obtenir une autorisation judiciaire avant que l'État ne puisse s'immiscer dans la vie privée d'un individu. Dans le cadre de la présente étude, l'État sera généralement représenté par les organismes d'application de la loi.

Les contextes apportés par les nouvelles TI et Internet compliquent également la question de la détermination de la nature de l'autorisation préalable à obtenir. Certains types d'autorisation s'appliquent à des contextes technologiques particuliers[6] alors que d'autres s'appliquent indépendamment du contexte technologique[7]. La présente étude ne traitera pas de la question reliée à la détermination de l'autorisation appropriée. Par contre, l'étude des

---

langue française, 2001, *s.v.* « Internet », en ligne : <http://www.olf.gouv.qc.ca/ressources/internet/fiches/2074841.htm> (date d'accès : 21 février 2001).

4 Nous verrons que la jurisprudence de la Cour Suprême fait parfois référence à la notion d'*intrusion* d'agent de l'État dans la sphère de vie privée d'un individu. Nous préférons utiliser le terme immixtion qui correspond mieux au concept d'ingérence non appropriée dans une sphère de vie privée. Le terme intrusion, provenant probablement d'une traduction malheureuse du mot i*ntrusion* en anglais, fait plutôt référence à un empiétement physique dans un lieu. Nous verrons que le concept de vie privée ne fait plus principalement référence à la protection des lieux. C'est pourquoi nous n'utilisons pas le terme intrusion, qui porte à confusion. Malgré tout, le terme *intrusion* apparaîtra lorsque nous citerons les passages de jugements utilisant cette expression. Voir Le nouveau petit Robert, 1993, *s.v.* « intrusion » [ci après *le Robert*].

5 *Charte canadienne des droits et libertés*, partie I de la *Loi Constitutionnelle de 1982*, constituant l'annexe B de la *Loi de 1982 sur le Canada* (R.-U.), 1982, c. 11, [ci-après *Charte canadienne*].

6 Voir l'article 492.1 du *Code criminel,* L.R.C. 1985, c. C-46 [ci-après *Code criminel*] traitant des balises de localisation et de l'article 492.2 du *Code criminel* traitant des enregistreurs de numéros de téléphone.

7 Voir la partie VI du *Code criminel*, traitant de l'interception des « communications privées » et l'article 487.01 du *Code criminel* traitant du mandat général.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

contextes apportés par les nouvelles TI et Internet pourra apporter des pistes de réflexions intéressantes à ce sujet.

L'impact des nouvelles TI et d'Internet sur la vie privée des individus a été traité à maintes reprises[8]. Ces études portaient généralement sur la protection des renseignements personnels détenus par l'État ou des organismes privés, et sur les problèmes que soulevaient l'informatique, les nouvelles TI, ou Internet à leur égard. Notre étude porte plutôt sur la protection que la *Charte canadienne* accorde aux individus dans le contexte d'enquêtes criminelles. Il s'agit de la dimension constitutionnelle du droit à la vie privée et non de sa dimension civile ou privée[9].

L'étude des contextes se justifie également par le fait que la Cour suprême du Canada interprète généralement la *Charte canadienne* à la lumière de ceux-ci. C'est ce qu'il convient d'appeler la méthode contextuelle d'interprétation de la *Charte canadienne*. La détermination et l'explication des contextes factuels apportés par les nouvelles TI et Internet sont donc compatibles avec l'utilisation de cette méthode d'interprétation.

De ces nouveaux contextes émergeront de nouvelles rationalités[10]. Leur identification devient importante car elles pourraient être la base de possibles modifications législatives. Ces nouvelles rationalités pourront notamment entraîner une variation, dans un sens ou dans l'autre, du niveau d'expectative raisonnable de vie privée auquel un individu peut s'attendre dans un contexte donné. Elles constitueront l'assise du droit nouveau en matière d'expectative raisonnable de vie privée. Émergeront également de ces nouvelles rationalités, de nouveaux facteurs propres aux contextes apportés par les nouvelles TI et Internet qui seront, eux aussi, susceptibles de moduler le niveau d'expectative raisonnable de vie privée dans un sens ou dans l'autre. Nous nous attarderons spécifiquement à identifier ces facteurs dans la présente étude, afin d'en dresser un tableau qui pourra notamment servir de matrice décisionnelle face à un contexte factuel donné.

---

8 Voir notamment sur le sujet avant qu'Internet et les nouvelles TI n'aient leur forme actuelle K. Benyekhlef, *La protection de la vie privée dans les échanges internationaux d'information*, Montréal, Thémis, 1992; R. Côté et R. Laperrière, dir., *Vie privée sous surveillance :la protection des renseignements privés en droit québécois et comparé*, Cowansville (Qc.), Yvon Blais, 1994; Canada, Ministère de la justice, *Vie privée sans frontières : les flux transfrontières de renseignements personnels en provenance du Canada*, Ottawa, Approvisionnements et Services Canada, 1990 (Étude réalisée par le Groupe de Recherche en Informatique et Droit). Pour une étude ayant été réalisée sur le sujet depuis qu'Internet et les nouvelles TI ont leur formes actuelles, voir notamment P. Trudel *et al*., *Droit du Cyberespace*, Montréal, Thémis, Centre de recherche en droit public, Faculté de droit, 1997 aux pp. 11-1 à 11-70 [ci-après *Droit du Cyberespace*]. Pour une étude de la protection civile du droit à la vie privée dans le contexte médiatique voir M. Michaud, *Le droit au respect de la vie privée dans le contexte médiatique : de Warren Brandeis à l'Inforoute*, Cowansville (Qc.), Yvon Blais, 1996.

9 Voir un article intéressant du professeur Benyekhlef à ce sujet où l'on traite plus à fond des distinctions appropriées entre les différentes protections à la vie privée, qu'accorde la loi : K. Benyekhlef, « Les dimensions constitutionnelles du droit à la vie privée » dans P. Trudel, dir., *Droit du public à l'information et vie privée : deux droits irréconciliable?*, à la p. 17 [ci-après « Les dimensions »].

10 Comme le définissent P. Trudel *et al*, dans *Droit du Cyberespace*, supra note 8 à la p. 1-1.
[d]errière tout corpus de règles, se profilent des principes, valeurs et intérêts qui en sous-tendent la légitimité. Très souvent, la règle est le résultat d'une décision conciliatrice des différents intérêts et valeurs ou reflète des choix. Le cadre juridique de l'information et de la communication repose au premier chef, sur les valeurs au nom desquelles émergent des demandes afin d'en encadrer certains aspects. C'est cela que nous appelons «rationalités»». […] «Les rationalités cristallisent les raisons pour lesquelles s'expriment des besoins de normativité et les types d'intervention juridique ou parajuridiques que ces besoins appellent.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

La présente étude ne constitue pas une étude exhaustive du concept de vie privée. Comme l'affirme le professeur Karim Benyekhlef, il serait de toute façon périlleux de définir trop précisément ce que devrait être le droit à la vie privée[11]. La présente étude constitue plutôt une analyse de l'influence que les contextes apportés par les nouvelles TI et Internet auront sur le niveau ou degré d'expectative raisonnable de vie privée[12]. L'analyse des contextes et de leurs influences nous semble être compatible avec l'interprétation du principe juridique que constitue le droit à la vie privée[13].

Il serait illusoire de traiter de tous les contextes possibles que les nouvelles TI et Internet apportent. Par contre, un individu communiquant par le biais d'Internet et des nouvelles TI, se place indubitablement dans un contexte technique donné. Même si cette communication peut s'effectuer de différentes manières, donc dans des contextes techniques différents, il est relativement aisé d'en déterminer les principaux et de les expliquer. Il s'agit en quelque sorte de déterminer le cadre factuel de base dans lequel se placera à un individu chaque fois qu'il communiquera par le biais d'Internet et des nouvelles TI.

La présente étude sera divisée en trois parties. La première fera le point sur l'état du droit au Canada en matière de protection accordée par l'article 8 de la *Charte canadienne*. Il s'agit essentiellement de faire ressortir les principes de droit généralement reconnus ou établis en la matière. Cette mise au point est nécessaire parce qu'elle constitue l'assise légale à partir de laquelle la détermination et l'explication des nouveaux contextes s'effectueront. Au chapitre 1, nous traiterons brièvement du cadre législatif et tenterons de cerner le concept de vie privée qui en découle. Nous traiterons ensuite des différentes méthodes de détermination de l'expectative raisonnable de vie privée, soit l'approche de principe au chapitre 2 et l'approche pragmatique ou au cas par cas au chapitre 3.

Compte tenu des divers niveaux de protection accordés par la *Charte canadienne*, nous traiterons au chapitre 4 des cas où l'expectative raisonnable de vie privée a été reconnue par les tribunaux, des cas où elle était réduite et des cas où elle était inexistante.

La mécanique constitutionnelle entourant l'application de l'article 8 de la *Charte canadienne* nous oblige de traiter au chapitre 5 de ce que nous appellerons la protection *post* immixtion de la vie privée. Il s'agit en fait de discuter de la détermination du caractère non abusif de l'immixtion dans une expectative raisonnable de vie privée.

L'article 8 de la *Charte canadienne* ne constitue pas la seule protection de la vie privée en matière de communication. En effet le *Code criminel* protège les communications privées d'un individu, notamment contre les immixtions injustifiées de l'État. Nous traiterons donc au chapitre 6 de la notion de « communication privée », concept fondamental en la matière. De

---

[11] « Les dimensions » *supra* note 9 aux pp. 17-32.

[12] Cette approche nous semble compatible avec celle de P. Trudel *et al*. dans *Droit du Cyberespace*, *supra* note 8 à la p. 11-25 :

> « La notion de vie privée connaît un sens qui varie en fonction du contexte, des époques, des mœurs et, surtout, des personnes. La vie privée est une notion qui n'a pas à être déterminée de façon définitive ; ce qui ne l'empêche pas d'être une notion déterminable dans chaque situation concrète ».

[13] « Les dimensions » *supra* note 9 aux pp. 18-22.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

plus, compte tenu de la similitude entre le courriel[14] et la correspondance, nous y traiterons brièvement de la protection que lui accorde le droit canadien.

Dans la seconde partie, nous identifierons et expliquerons les contextes apportés par les nouvelles TI et Internet. Nous traiterons au chapitre 1 des contextes techniques généraux apportés par l'utilisation de l'informatique, d'Internet et des nouvelles TI. Nous y traiterons du contexte de l'évolution des technologies en matière de communication, du contexte de l'utilisation de l'informatique, d'Internet et des nouvelles TI, d'Internet tel que décrit par la Cour suprême américaine, du contexte technique d'Internet, du contexte du branchement à Internet, du contexte territorial ou juridictionnel d'Internet et de la notion d'ubiquité.

Le sujet traité au chapitre 2 sera le plus dense et le plus détaillé. Ceci est nécessaire afin de bien identifier les contextes techniques particuliers apportés par Internet et les nouvelles TI. Il s'agit du Web, du courriel, du transfert de fichiers FTP, des groupes de discussions ou nouvelles *Usenet*, des sessions en mode terminal *Telnet*, du bavardage-clavier ou clavardage du service IRC, de la téléphonie et vidéoconférence Internet et de la messagerie instantanée.

L'hypothèse opérationnelle de la présente étude repose principalement sur le fait que la majorité de ces contextes particuliers restent encore inexplorés par le droit. Chacun de ceux-ci fera l'objet d'un constat des limites à l'expectative raisonnable de vie privée lors de leur utilisation, en fonction des critères qui auront été établis en première partie. Afin d'être en mesure de présenter un portrait légal le plus complet possible, nous nous référerons, dans bien des cas, à d'autres sources que le droit canadien, notamment au droit américain[15]. Cette approche nous permettra d'anticiper rationnellement le droit susceptible d'application au Canada dans un contexte factuel donné, le tout avec les distinctions nécessaires.

Au chapitre 3, nous traiterons des technologies particulières ayant une influence sur le caractère privé des communications effectuées dans les divers contextes apportés par Internet et les nouvelles TI. Il s'agit de l'utilisation de la cryptographie, de la stéganographie et des techniques favorisant l'anonymat.

Dans la troisième partie, nous élaborerons une grille d'analyse qui servira d'outil ou de matrice décisionnelle pour la détermination du niveau d'expectative raisonnable de vie privée dans les contextes précédemment traités. Encore une fois, il ne s'agit pas de l'élaboration d'une liste exhaustive de facteurs, mais plutôt d'un outil général qui servira à donner des pistes de départ ou à identifier les grands principes à considérer avant de se prononcer sur le niveau d'expectative raisonnable de vie privée dans un contexte donné. Nous présenterons les

---

[14] L'expression « courriel » constitue un diminutif de l'expression « courrier électronique ». On définit le courrier électronique comme étant un service de correspondance sous forme d'échange de messages électroniques, à travers un réseau informatique. Par extension, on utilise aussi les termes *courrier électronique* et *courriel* pour désigner le message lui-même. Office de la langue française, 2001, *s.v.* « courriel », en ligne : <http://www.olf.gouv.qc.ca/ressources/internet/fiches/1299117.htm> (consulté le 18 juin 2001).

[15] Compte tenu des nombreuses références par la jurisprudence canadienne à l'interprétation du IV^e^ amendement américain dans le contexte de l'interprétation de l'article 8 de la *Charte canadienne*, notamment dans les arrêts *Hunter c. Southam*, [1984] 2 R.C.S. 145 [ci-après *Hunter*], *R. c. Edwards*, [1996] 1 R.C.S.128 [ci-après *Edwards*], et *R. c. Belnavis*, [1997] 3 R.C.S. 341 [ci-après *Belnavis*], nous pensons qu'il est approprié de référer principalement au droit américain. Nous ferons par contre les distinctions nécessaires entre le droit américain et canadien, le cas échéant.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

nouveaux facteurs émanant des contextes de communication apportés par Internet et les nouvelles TI influant sur le niveau d'expectative raisonnable de vie privée, nous identifierons ensuite les divers facteurs émanant des divers contextes de communication apportés par les nouvelles TI et Internet, pour finalement les insérer au Tableau I, en indiquant dans chaque cas s'ils ont tendance à favoriser ou non l'existence d'une quelconque expectative raisonnable de vie privée.

Nous conclurons en reprenant les principaux apports qui auront été dégagés au cours des différentes parties. Nous soulignerons également leurs intérêts mais également leurs limites et leurs insuffisances, le cas échéant. Cela nous mènera à cerner et à énoncer les principales questions qui restent à résoudre.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>

Partie I – Les grands principes généralement reconnus en matière d'expectative raisonnable de vie privée

Nous présenterons dans cette partie les dispositions législatives principales et le concept de droit à la vie privée au chapitre 1. Nous traiterons ensuite de la détermination de l'expectative raisonnable de vie privée et de l'approche de principe au chapitre 2; de la détermination de l'expectative raisonnable de vie privée et l'approche pragmatique ou au cas par cas au chapitre 3; de l'expectative raisonnable de vie privée présente, moindre ou inexistante, au chapitre 4; de la protection « *post* immixtion » de la vie privée au chapitre 5; et de la protection statutaire accordée en matière de « communication privée » et de correspondance au chapitre 6.

Chapitre I - Les dispositions législatives principales et le concept de droit à la vie privée

Le concept d'expectative raisonnable de vie privée découle de l'article 8 de la *Charte canadienne*[16]. Cet article s'applique en relation avec d'autres articles de la *Charte canadienne*, soit les articles 32 et 24. Nous traiterons donc dans l'ordre suivant des articles 32, 8 et 24 de la *Charte canadienne*. Nous ferons ensuite un bref rappel historique de la genèse de la notion d'expectative raisonnable de vie privée en droit criminel canadien et traiterons des principes fondamentaux de la protection offerte par l'article 8 de la *Charte canadienne*. Finalement nous traiterons de la difficulté à définir le concept de droit à la vie privée.

Section 1 - L'article 32 de la *Charte canadienne*

Cet article prévoit que :

> « 32. (1) *La présente charte s'applique:*
> *a) au Parlement et au gouvernement du Canada, pour tous les domaines relevant du Parlement, y compris ceux qui concernent le territoire du Yukon et les territoires du Nord-Ouest;*
> *b) à la législature et au gouvernement de chaque province, pour tous les domaines relevant de cette législature* ».

Par l'effet de l'article 32, la *Charte canadienne* s'applique à tous les domaines relevant de l'autorité tant du Parlement et du gouvernement du Canada que des législatures et des gouvernements des provinces. Il s'ensuit que les droits et libertés énumérés à la *Charte canadienne* ne sont garantis que contre les atteintes découlant des mesures prises par le Parlement et le gouvernement du Canada ou par les législatures et les gouvernements des

[16] Nous sommes conscients qu'un certain courant jurisprudentiel énonce que la protection de la vie privée découle également de la protection offerte par l'article 7 de la *Charte canadienne*. Voir notamment à cet effet : *R. c. Morgentaler (No2)*, [1988] 1 R.C.S. 30 ; *Rodriguez c. Colombie-Britannique (Procureur Général)*, [1993] 3 R.C.S. 519 ; *R. v. O'Connor*, [1995] 4 R.C.S. 411 [ci-après *O'Connor*] et *M. (A.) c. Ryan*, [1997] 1 R.C.S. 157. Par contre nous considérons pour les fins de la présente étude que la protection en matière de vie privée découle principalement de l'article 8 de la *Charte canadienne*. Cette position est justifiée par la jurisprudence majoritaire sur le sujet en matière criminelle et le fait que l'arrêt *R. c. Mills*, [1999] 3 R.C.S. 668 [ci-après *Mills*] qui constitue en quelque sorte une révision des principes énoncés dans l'arrêt *O'Connor*, évacue complètement la question de l'application de l'article 7 de la *Charte canadienne*. La Cour énonce plutôt que l'article 8 de la *Charte canadienne* constitue la base constitutionnelle de la protection de la vie privée. En définitive il s'agit d'une distinction théorique.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

provinces. En l'absence d'action d'une de ces entités portant atteinte à quelque droit ou liberté garanti par la *Charte canadienne*, il ne peut y avoir violation de cette dernière[17].

Dans le contexte de la présente étude, les atteintes découlant des mesures prises par le Parlement et le gouvernement du Canada ou par les législatures et les gouvernements des provinces, prendront la forme d'une surveillance électronique, fouille, perquisition ou saisie; il s'agit en définitive d'une immixtion dans une quelconque expectative raisonnable de vie privée.

Section II - L'article 8 de la *Charte canadienne*

L'article 8 de la *Charte canadienne* constitue l'assise constitutionnelle de la protection accordée en matière de vie privée contre les immixtions injustifiées de l'État dans la vie privée d'un individu. Même si le droit à la vie privée n'y est pas spécifiquement énoncé, c'est par la protection qu'il accorde contre les fouilles saisies et perquisitions abusives qu'il sera protégé. Cet article prévoit que:

> « 8. *Chacun a droit à la protection contre les fouilles, perquisitions et saisies abusives* »[18].

L'article 8 de la *Charte canadienne* a donc pour objet de protéger les personnes contre les immixtions injustifiées de l'État dans leur vie privée.

Nous verrons plus en détail dans la section suivante, que l'article 8 de la *Charte canadienne* protège les personnes et non pas les lieux; ceux-ci bénéficient d'une protection uniquement dans la mesure de leur interaction avec les personnes[19]. Par exemple, une maison d'habitation jouit d'un très haut niveau de protection parce qu'elle constitue le domicile d'une personne[20].

Même si l'article 8 de la *Charte canadienne* protège les personnes et non les lieux ou les choses, il protège les individus uniquement contre les actions de l'État (au sens de l'article 32 de la *Charte canadienne*) qui portent atteinte à la vie privée parce qu'elles constituent un recours abusif aux pouvoirs de fouille, perquisition ou saisie. Par conséquent, le lieu de la fouille, de la perquisition ou de la saisie a effectivement de l'importance, si la mesure en question a été exécutée à l'extérieur du Canada par des personnes ne relevant pas de l'autorité du gouvernement canadien[21].

L'article 8 de la *Charte canadienne* s'applique non seulement aux personnes physiques mais également aux personnes morales[22]. Par contre, les personnes morales exerceront généralement leurs activités dans un contexte commercial ou réglementaire ce qui entraîne, en

---

17 *Schreiber c. Canada (Procureur général),* [1998] 1 R.C.S. 841, à la p. 858 [ci-après *Schreiber*].

18 Le terme « fouille » s'adresse aux personnes alors que le terme « perquisition » vise généralement les lieux. Voir de façon générale sur cette question : *Hunter, supra* note 15 et *R. c. Collins*, [1987] 1 R.C.S. 265 [ci-après *Collins*]. Comme nous en discuterons plus loin, ces distinctions perdent de leur sens, dans la mesure où l'État s'est immiscé dans une quelconque expectative raisonnable de vie privée.

19 *Hunter, supra* note 15 à la p. 159.

20 Voir entre autres *R. c. Silveira*, [1995] 2 R.C.S. 297 [ci-après *Silveira*] et *R. c. Feeney,* [1997] 2 R.C.S. 117 [ci-après *Feeney*]

21 *Schreiber, surpa* note 17 à la p. 861. Voir également sur cette question *R. c. Cook*, [1998] 2 R.C.S. 597.

22 *R. c. CIP Inc.,* [1992] 1 R.C.S. 843, aux pp. 854-55.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

principe, une attente raisonnable moindre de respect de la vie privée. Nous y reviendrons plus loin.

Bien que l'article 8 de la *Charte canadienne* soit la garantie fondamentale pour la protection d'un individu contre les fouilles, perquisitions et saisies abusives, il faut quand même tenir compte de l'application complémentaire de l'article 24 de la *Charte canadienne*. Dans un contexte judiciaire criminel ou pénal, l'article 8 de la *Charte canadienne* n'a de sens que si la sanction de l'article 24 de la *Charte canadienne* trouve application. Ceci nous amène donc à traiter de l'article 24 de la Charte canadienne.

Section III - Les paragraphes 24(1) et (2) de la *Charte canadienne*

L'article 24 de la *Charte canadienne* sanctionne le non-respect d'une des garanties constitutionnelles, dont celle prévue à l'article 8. L'article 24 de la *Charte canadienne* prévoit que:

> « 24. (1) *Toute personne, victime d'une violation ou de la négation des droits ou libertés qui lui sont garantis par la présente charte, peut s'adresser à un tribunal compétent pour obtenir la réparation que le tribunal estime convenable et juste eu égard aux circonstances.*
>
> *(2) Lorsque, dans une instance visée au paragraphe (1) le tribunal a conclu que des éléments de preuve ont été obtenus dans des circonstances qui portent atteinte aux droits et libertés garantis par la présente charte, ces éléments de preuve sont écartés s'il est établi, eu égard aux circonstances, que leur utilisation est susceptible de déconsidérer l'administration de la justice* ».

Pour que l'article 24 de la Charte canadienne s'applique, on devra déterminer si la garantie prévue à l'article 8 de la *Charte canadienne* trouve application dans un contexte donné. De plus on devra déterminer qui peut se prévaloir des recours prévus à l'article 24 de la *Charte canadienne*, étant donné que la disposition semble exiger que seule la victime de la violation ou d'une négation de ses droits personnels puisse s'adresser au tribunal compétent pour obtenir réparation, le plus souvent par l'exclusion de la preuve obtenue en violation de la protection accordée.

Nous ne nous attarderons pas davantage à l'article 24 de la *Charte canadienne* et à la procédure s'y rapportant qui pourraient faire, à eux seuls, l'objet d'un mémoire. Il suffit de retenir, pour les fins de la présente étude, que l'article 8 de la *Charte canadienne* n'a de sens que si l'exclusion d'un élément de preuve est prononcée par la cour en vertu de son paragraphe 24(2). C'est de cette manière que la vie privée d'un individu sera protégée contre les immixtions injustifiées : l'État ne pourra utiliser cette preuve dans un procès contre lui.

Nous venons de traiter sommairement de la mécanique entourant l'application de la protection constitutionnelle prévue à l'article 8 de la *Charte canadienne*. Il convient maintenant de traiter plus en détail du concept de vie privée.

Section IV - Bref rappel historique de la genèse de la notion d'expectative raisonnable de vie privée en droit criminel au Canada

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

Ce bref rappel historique a pour but de mieux situer le lecteur. Il n'a donc aucune prétention historique ou scientifique. Il faut remonter un peu dans l'histoire américaine pour trouver la justification du concept d'expectative raisonnable de vie privée. Après la guerre civile, les États-Unis ont connu une industrialisation et urbanisation rapides. Les petits villages n'ont jamais été reconnus pour le respect de la vie privée, mais dans de telles communautés, l'étendue des commérages était limitée compte tenu qu'ils ne voyageaient pas très loin. L'invention de l'imprimerie à grande échelle a entraîné l'augmentation du nombre de journaux, notamment des journaux à sensations ou « *yellow journals* ». Les commérages pouvaient du coup voyager beaucoup plus vite et à plus grande échelle.

En réponse à certains articles au sujet de sa famille provenant de ces multiples publications, Samuel Warren, éditeur d'un reconnu et distingué journal, et son ancien partenaire, l'avocat Samuel Brandeis -qui deviendra plus tard juge à la Cour suprême des Etats-Unis- écrivirent dans le *Harvard Law Review* un article au sujet du droit à la vie privée. La nomination de Brandeis contribuera certainement à faire de cet article un canon sur le sujet. Warren et Brandeis y argumentèrent que le changement apporté par la technologie commandait une réponse législative[23] **:**

> [Traduction libre] « *Qu'un individu devrait avoir la pleine protection dans sa personne et sur ses biens est un principe aussi vieux que la Common Law, mais il a été nécessaire de redéfinir, de temps à autre, la nature exacte de l'étendue d'une telle protection [...] Autrefois la loi ne protégeait que les ingérences contre la vie et les biens [...] Plus tard, on en vint à reconnaître la nature spirituelle de l'être humain, de ses sentiments et de son intellect. L'étendue de ses droits s'est graduellement agrandie. Le droit à la vie s'est donc transformé pour comprendre désormais le droit de jouir de la vie : le droit de ne pas être importuné par autrui (the right to be let alone...).*
>
> *[…] Les photographies instantanées et les entreprises journalistiques ont envahi les limites sacrées de la vie privée et familiale. De plus en plus de moyens techniques menacent de rendre vraie la prédiction voulant que ce qui est murmuré dans la garde-robe sera proclamé du haut des toits* »[24]

Beaucoup plus tard, soit en 1967, la Cour suprême des États-Unis a énoncé pour la première fois le concept « *d'expectative raisonnable de vie privée* »[25]. Dans la cause *Charles Katz c.*

---

[23] Le changement technologique du temps W. Diffie, et S. Landau, *Privacy on the Line. The Politics of Wiretapping and Encryption*, MIT Press, Cambridge, 1998, aux pp. 130-31 [ci-après *Privacy on the Line*].

[24] Texte original en anglais dans "S. D. Warren, et L. D. Brandeis, « The Right toPrivacy », (1890) *Harv. L.R.* 193, aux pp. 193, 195:

> That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. […] Thus, in very early times, the law gave a remedy only for physical interference with life and property […]. Later, there came a recognition of man's spiritual nature, of his feelings and his intellect. Gradually the scope of these legal rights broadened; and now the right to life has come to mean the right to enjoy life, -- the right to be let alone; […]
>
> […] Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops.

[25] *Privacy on the Line, supra* note 23 à la p.167.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

United-States[26], la Cour a déterminé qu'une partie de la preuve provenant d'un microphone électronique miniature placé sans mandat dans une cabine téléphonique était inadmissible. La Cour a déterminé que le IV[e] amendement protégeait les personnes et non les lieux. Cette position était diamétralement opposée à la position antérieure de la Cour sur la question. En effet, dans la décision rendue dans *Olmstead c. United States*[27], la Cour avait affirmé qu'une intrusion, au sens physique du terme, était nécessaire pour qu'il y ait violation du IV[e] amendement. En changeant de position, la Cour revenait à sanctionner l'opinion dissidente du juge Brandeis dans *Olmstead*, qui affirmait déjà à l'époque que le IV[e] amendement s'appliquait même s'il n'y avait aucune interférence physique par un agent de l'État. De plus, la Cour dans *Katz* a directement fait référence au concept déjà énoncé par Brandeis et Warren dans leur article du *Harvard Law Review* : le droit de ne pas être importuné par autrui ou « *…the right to be let alone…* »

En 1984, la Cour suprême du Canada reprendra et adoptera dans l'arrêt *Hunter*[28], les grands principes de l'arrêt *Katz*.

Section V - Principes fondamentaux de la protection offerte par l'article 8 de la *Charte canadienne*

Historiquement au Canada la protection qu'offrait le *common law* contre les fouilles, les perquisitions et les saisies effectuées par le gouvernement ou les agents de l'État, se fondait sur le droit de toute personne à la jouissance de ses biens et était liée au droit applicable en matière d'intrusion ou, en anglais, de *trespass*[29]. L'arrêt *Hunter* est venu « étendre » cette protection de la même manière que l'avait faite la Cour suprême américaine dans *Katz*. Conséquemment, les droits protégés par l'article 8 de la *Charte canadienne* ont désormais une portée plus large que la protection offerte par le *common law*[30] : l'article 8 de la *Charte canadienne* protège désormais les personnes et non seulement les lieux[31]. Ceux-ci bénéficient d'une protection uniquement dans la mesure de leur interaction avec les personnes[32]. Par exemple, une maison d'habitation jouit d'un très haut niveau de protection parce qu'elle constitue le domicile d'une personne[33].

Les notions de propriété d'un bien et d'intrusion sur une propriété ne constituent donc plus la rationalité sous-jacente principale à la protection contre les immixtions de l'État au Canada[34]. Nous verrons, par contre, que le fait d'être propriétaire d'un lieu où se produit une immixtion de l'État demeure quand même un facteur important dans la détermination de l'expectative raisonnable de vie privée d'un individu.

---

26 *Katz v. United States,* 389 U.S. 347 (1967) [ci-après *Katz*].
27 *Olmstead c. United States,* 277 U.S. 438 (1928).
28 *Hunter*, s*upra* note 15 à la p. 145.
29 *Ibid.* aux pp. 145, 157.
30 *Ibid.* aux pp. 145, 158.
31 *Ibid.* aux pp.145, 158-59, où le juge la Cour, par la plume du juge en chef Dickson, adopte la position énoncée par la Cour suprême américaine dans *Katz, supra* note 26 à la p. 347.
32 *Hunter, Ibid.* aux pp. 145, 159.
33 Voir notamment sur la question de l'importance du domicile pour un individu *Silveira*, *supra* note 20 et *Feeney, supra* note 20.
34 *R. c. Plant,* [1993] 3 R.C.S 281, 291-292 [ci-après *Plant*].

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

À notre avis, cette citation du président américain Lyndon B. Johnson illustre le bien-fondé de la modification de la rationalité sous-jacente à la protection de la vie privée apportée par l'évolution de la technologie :

> *« The principle that a man's home is his castle is under new attack. For centuries the law of trespass protected a man's lands and his home. But in this age of advanced technology, thick walls and locked doors cannot guard our privacy or safeguard our personal freedom. »*[35]

C'est maintenant dans cette réalité technologique que s'inscrit le débat entourant la protection de la vie privée dans les différents contextes de communication apportés par l'émergence des nouvelles TI et d'Internet. Il convient maintenant de traiter des définitions du concept de vie privée, énoncées par la Cour suprême du Canada.

Section VI - Une définition possible du concept de droit à la vie privée?

Définir le concept de vie privée n'est pas chose facile puisqu'il s'agit d'un concept qui émane d'une protection constitutionnelle « assez vague et générale »[36]. En effet, plusieurs définitions ont été énoncées par la Cour suprême du Canada au cours des dernières années à travers les décisions rendues. Nous tenterons ici d'en dégager les principaux aspects, même si nous sommes conscients qu'il ne s'agit peut-être pas de l'approche idéale[37].

Le concept de vie privée ne doit pas être restreint par des classifications formalistes étroites[38]. La *Charte* doit être interprétée libéralement, en fonction de son but : « garantir et protéger, dans des limites raisonnables, la jouissance des droits et libertés qu'elle enchâsse »[39]. Dans le cadre de la présente étude, il s'agit du droit à la vie privée dans le contexte des communications effectuées par le biais des nouvelles TI et d'Internet.

Comme nous l'avons vu, le droit à la vie privée a été étendu au « droit de ne pas être importuné par autrui » [40]. Il s'agit de l'expectative raisonnable des citoyens en matière de vie privée, dans une société libre et démocratique[41]. Ce qui veut dire que l'on pourra qualifier l'attente en fonction des réalités quotidiennes ayant cours dans d'autres pays démocratiques semblables au Canada et non en fonction des réalités quotidiennes ayant cours dans des pays gouvernés par une dictature ou un régime totalitaire.

Même si ces définitions semblent plutôt vagues, on a tout de même défini le droit à la vie privée comme comportant le « droit d'être à l'abri de toute intrusion ou ingérence »[42]. Mais encore faut-il qu'un tel droit existe.

---

35 Cité dans A. Bacard, *The Computer Privacy Handbook*, Berkeley, California, Peachpit Press, 1995 à la p. 21 [ci-après *The Computer Privacy Handbook*].
36 *Hunter, supra* note 15 aux pp. 145, 154.
37 Voir les remarques en introduction concernant les limites relatives aux tentatives de définition du concept de vie privée.
38 *R. c. Dyment,* [1988] 2 R.C.S. 417, 426 [ci-après *Dyment*].
39 *Hunter, supra* note 15 aux pp. 145, 156.
40 *Ibid.* aux pp. 145, 159.
41 *Ibid.*
42 *Edwards, supra* note 15 à la p. 128, au para. 50.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

La notion de vie privée est au cœur de celle de la liberté dans un État moderne. Fondée sur l'autonomie morale et physique de la personne, la notion de vie privée est essentielle à son bien-être. Elle revêt aussi une importance capitale sur le plan de l'ordre public. Il s'agit de l'essence même de l'État démocratique[43].

La limite « inférieure » du droit à la vie privée correspond au fait que les citoyens du pays sont protégés par les enquêtes non souhaitables menées à l'aveuglette par l'État par le biais de ses organismes d'application de la loi[44]. La limite « supérieure » du droit à la vie privée a été articulée par le juge Dickson de la Cour suprême du Canada, de la façon suivante : « *Le droit de l'État de déceler et de prévenir le crime commence à l'emporter sur le droit du particulier de ne pas être importuné, lorsque les soupçons font place à la probabilité fondée sur la crédibilité* »[45]. Donc, en principe, si cette probabilité fondée sur la crédibilité existe au préalable, les agents de l'État pourront s'immiscer légalement dans la vie privée d'un individu. Dans ce contexte, le droit à la vie privée n'est pas absolu. Il est limité par les impératifs de l'application des lois en matière criminelle et pénale et de la recherche de la vérité.

En raison de la portée très large de la notion d'expectative raisonnable de vie privée, la jurisprudence en est venue à considérer comme étant des fouilles, perquisitions ou saisies une multitude de gestes qui, à prime abord, ne semblaient pas en être.

En principe, toute activité étatique qui déjoue une attente ou expectative raisonnable en matière de respect de la vie privée, constitue une fouille ou une perquisition au sens de l'article 8 de la *Charte canadienne*[46]. Par ailleurs, constitue une « saisie », le fait pour l'appareil étatique de prendre toute chose appartenant à quelqu'un sans son consentement[47].

De façon générale, l'activité étatique, dans le contexte d'une enquête de nature criminelle ou pénale, est effectuée par un policier ou agent de la paix. Par contre, il se peut que d'autres personnes soient appelées à agir à titre de représentant de l'État. En effet, un directeur d'école ou son directeur adjoint peut voir s'appliquer la *Charte canadienne* à son action[48].

Étant donné la définition précédente de ce qui constitue, sur le plan constitutionnel, une « fouille, saisie ou perquisition », il devient nécessaire de déterminer, dans chaque cas, si la conduite de l'État a empiété sur quelque droit raisonnable des appelants à la vie privée. Si cette conduite a effectivement fait en sorte qu'un agent de l'État s'est immiscé dans une « attente ou expectative raisonnable en matière de vie privée » d'un individu, elle constitue alors une fouille, saisie ou perquisition au sens de l'art. 8 de la *Charte canadienne* et elle est assujettie aux exigences de cet article, notamment à celle de l'obtention d'une autorisation judiciaire préalable.

Dans le cas contraire, on ne s'immisce dans aucun droit. Conséquemment aucune autorisation judiciaire préalable ou existence de motifs raisonnables ne sont requises, d'où l'importance de la détermination de l'existence ou non d'une expectative raisonnable de vie privée.

---

43 *Dyment, supra* note 38 aux pp. 428-29.
44 *R. c. Araujo*, [2000] 2 R.C.S. 992, au para. 29.
45 *Hunter, supra* note 15 aux pp. 167-68.
46 *R. c. Wise*, [1992] 1 R.C.S. 527, 533 [ci-après *Wise*].
47 *Dyment*, *supra* note 38 à la p. 431.
48 *R. c M. (M.R.),* [1998] 3 R.C.S. 393 [ci-après *M.R.*].

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

Il appartient donc à la personne qui invoque une expectative en matière de vie privée « d'inscrire » la perquisition dans les paramètres de l'article 8 de la *Charte canadienne*, sans quoi elle ne pourra bénéficier de sa protection et, en bout de ligne, de l'exclusion de la preuve par l'effet de l'article 24(2) de la *Charte canadienne*[49].

Ainsi, la jurisprudence a considéré comme constituant une fouille, perquisition ou saisie au sens de l'article 8 de la *Charte*, le prélèvement de substances corporelles[50], l'interception de communications effectuée de manière confidentielle[51], l'interrogatoire d'une personne détenue concernant le contenu d'objets en sa possession[52], la captation d'images vidéo d'un lieu ou d'une personne[53], l'utilisation d'un dispositif de localisation[54] (*bumper beeper*), l'inspection de documents commerciaux faite dans le cadre d'un régime réglementaire[55], la prise de copies d'un document[56], l'inspection du périmètre d'une maison d'habitation[57], le gel des lieux dans l'attente d'un mandat de perquisition[58], la fouille olfactive d'une maison d'habitation pour déceler une odeur de marijuana[59], une ordonnance de communication de documents[60], la photocopie de documents bénéficiant d'une expectative raisonnable de vie privée[61], ainsi qu'une ordonnance de communication de dossiers fondée sur les articles 278.1 à 278.91 du Code criminel[62].

Compte tenu de l'ensemble des actions étatiques ci-avant énumérées, les notions de fouille, saisie et perquisition perdent un peu de leur sens. À tout le moins, on peut dire que ces actions étatiques ne constituent pas toutes, d'emblée, ce qui pourrait être considéré, par une personne ordinaire, comme une fouille, saisie ou perquisition. Le test à appliquer sera plutôt de savoir s'il existe ou non une activité étatique qui a entraîné une immixtion dans une quelconque expectative raisonnable de vie privée. Pour ce faire, la Cour suprême du Canada a adopté une approche basée sur l'appréciation de l'ensemble des circonstances pour chaque cas. C'est ce que nous appelons l'approche pragmatique ou au cas par cas. Cette approche est relativement récente, car l'approche initialement favorisée par la Cour suprême du Canada semblait plutôt basée sur une norme plus générale. C'est ce que nous appelons l'approche de principe. Afin de clarifier les distinctions entre les deux approches et de bien comprendre leur évolution, il convient maintenant de traiter de la mécanique entourant la détermination de l'attente ou l'expectative raisonnable de vie privée. Cela nous aidera notamment à mieux anticiper la façon dont les tribunaux appliqueront les critères relatifs à la détermination de l'expectative raisonnable de vie privée dans le contexte d'Internet et des nouvelles TI.

---

49 *Edwards, supra* note 15.
50 *Dyment*, *supra* note 38.
51 *R. c. Duarte*, [1990] 1 R.C.S. 30 [ci-après *Duarte*] et *R. c. Thompson,*[1990] 2 R.C.S.1111, 1136-1137 [ci-après *Thompson*].
52 *R. c. Mellenthin*, [1992] 3 R.C.S. 615, 623-624.
53 *R. c. Wong*, [1990] 3 R.C.S. 36 [ci-après *Wong*].
54 *Wise*, *supra* note 46 à la p. 538.
55 C*omité paritaire c. Potash*, [1994] 2 R.C.S. 406, 418 [ci-après *Potash*].
56 *Potash*, *supra* note 55 à la p. 416.
57 *R. c. Kokesch*, [1990] 3 R.C.S. 3, 15 [ci-après *Kokesch*].
58 *Silveira*, *supra* note 20 à la p. 363.
59 *R. c. Evans*, [1996] 1 R.C.S. 8 [ci-après *Evans*]
60 *Thompson Newspapers Ltd. c. Canada (Directeur des enquêtes et recherches, Commission sur les pratiques restrictives en matière de commerce),* [1990] 1 R.C.S. 425 et *R. c. Mellenthin Transport Ltd.,* [1990] 1 R.C.S. 627.
61 *Potash, supra* note 55.
62 *Mills*, *supra* note 16.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

Chapitre II - La détermination de l'expectative raisonnable de vie privée et l'approche de principe

Dans le présent chapitre nous traiterons de l'arrêt *Dyment*[63] et de la naissance des sphères d'intimité; de l'arrêt *Duarte*[64] et du rejet de l'analyse fondée sur le risque; et de l'arrêt *Wong*[65] et du début de la fin de l'approche de principe.

Section I - L'arrêt *Dyment* et la naissance des sphères d'intimité

Comme nous l'avons vu, l'arrêt de base en matière d'expectative raisonnable de vie privée au Canada est l'arrêt *Hunter*. Par contre, cet arrêt n'a pas vraiment précisé **comment** procéder à la détermination de l'expectative raisonnable de vie privée. En fait, les définitions avancées y était plutôt vagues et générales. Certaines précisions ont été apportées à cet égard dans l'arrêt *Dyment*. Il s'agissait d'une décision impliquant la prise d'échantillon sanguin dans le contexte d'une accusation en matière de conduite avec les facultés affaiblies et un taux d'alcoolémie supérieur à 0,08 mg d'alcool par 100 ml de sang.

En l'espèce, un médecin avait recueilli le sang de l'accusé qui s'écoulait d'une plaie ouverte suite à un accident de la route et avait par la suite remis ce sang à un agent de police. Le tout avait été effectué sans le consentement de l'accusé, celui-ci étant inconscient. Compte tenu de la relation de confidentialité qui doit exister entre le patient et son médecin, et compte tenu que le médecin ne pouvait se servir de cet échantillon qu'à des fins médicales, la Cour a déterminé qu'il s'agissait d'une atteinte à une sphère de la vie privée essentielle au maintien de la dignité humaine. L'utilisation du corps d'une personne sans son consentement, en vue d'obtenir des renseignements à son sujet, est également le fondement d'une atteinte à cette sphère de la vie privée.

La vie privée serait composée de trois domaines ou sphères. Les principales revendications en matière de vie privée sont réparties de la façon suivante : celles qui comportent des aspects territoriaux ou spatiaux; celles qui ont trait à la personne; et celles qui sont faites dans le contexte informationnel[66]. Il est à noter que la Cour, par la plume du juge La Forest, se base sur un rapport traitant d'informatique et vie privée datant de 1972 pour étayer son raisonnement[67]. Sans trop s'avancer, il est raisonnable d'affirmer que l'informatique a beaucoup évolué depuis. Le contexte technique de l'époque ne correspond plus du tout au contexte technique d'aujourd'hui. Nous décrirons les principaux contextes techniques plus loin ce qui entraînera, notamment, l'émergence du concept d'intelligence collective.

Le droit à la vie privée en matière d'information est fondé sur la notion de dignité et d'intégrité de la personne. Cette conception découle du postulat selon lequel l'information de

---

63 *Supra* note 38.

64 *Duarte, supra* note 51.

65 *Wong, supra* note 53.

66 *Dyment, supra* note 38 à la p. 428. Les immixtions de l'État effectuées dans le contexte des nouvelles TI et d'Internet s'effectueront généralement dans la sphère informationnelle. Elles pourront également survenir dans la sphère territoriale ou spatiale. Il sera question dans ce cas, de déterminer à partir de quel endroit Internet et les nouvelles TI auront été utilisés. Il faudra ensuite déterminer la nature de l'interaction entre la personne, visée par l'immixtion, et l'endroit.

67 Canada. Rapport du groupe d'étude établi conjointement par le Ministère des Communications et le Ministère de la Justice. *L'ordinateur et la vie privée,* Ottawa, Information Canada, 1972.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>

caractère personnel est propre à l'intéressé, qui est libre de la communiquer ou de la taire comme il l'entend[68].

Dans ce contexte, la vie privée peut se définir comme le droit du particulier de déterminer lui-même quand, comment et dans quelle mesure il diffusera des renseignements personnels[69].

Plus tard, il sera déterminé que les valeurs protégées par le droit à la vie privée sont les plus directement touchées lorsque les renseignements confidentiels (ou personnels), contenus dans un dossier, portent sur des aspects de l'identité d'une personne ou lorsque la préservation de la confidentialité est essentielle à une relation thérapeutique ou à toute autre relation également fondée sur la confiance[70].

Section II - L'arrêt *Duarte* et le rejet de l'analyse fondée sur le risque

Il s'agissait ici de déterminer l'étendue de la protection accordée par l'art. 8 de la *Charte canadienne* contre l'enregistrement électronique de conversations de particuliers avec des policiers agissant à titre d'agent d'infiltration et avec des indicateurs, sans autorisation judiciaire. Encore une fois, il est important de préciser le contexte factuel de cette décision, étant donné les implications probables de cette décision en matière de surveillance électronique dans le contexte des nouvelles TI et d'Internet.

Dans le cadre d'une enquête sur le trafic de stupéfiants, la Police provinciale de l'Ontario et la Police de la communauté urbaine de Toronto ont loué un appartement que devait occuper un indicateur de police qui collaborait avec un agent d'infiltration. L'appartement était pourvu d'un matériel d'enregistrement audiovisuel installé dans un mur. Avant l'installation de ce matériel, l'indicateur et l'agent d'infiltration avaient consenti à ce que leurs conversations soient interceptées, comme le prévoyait à l'époque l'alinéa 178.11(2)a) du *Code criminel*[71].
Grâce à l'opération, l'agent d'infiltration a fait la connaissance d'un certain Paul Vidotto. Quelques jours après leur rencontre, Vidotto, l'appelant Mario Duarte et deux autres personnes se sont rendus à l'appartement pour discuter d'une affaire de cocaïne avec l'agent d'infiltration et l'indicateur. L'agent d'infiltration a pris des notes au sujet de ces conversations et d'une conversation ultérieure, notes qui, a-t-il reconnu, étaient fondées sur les enregistrements.

Duarte a par la suite été accusé de l'infraction de complot en vue d'importer un stupéfiant. À son procès, il a contesté dans le cadre d'un voir-dire, la validité de l'al. 178.11(2)a) du *Code criminel* qui prévoyait comme exception à l'interdiction de la surveillance électronique non autorisée, l'interception de conversations avec le consentement d'un des interlocuteurs. Le

---

68 *Dyment, supra* note 38 à la p. 429.

69 *Duarte, supra* note 51 à la p. 46. Voir également la *Loi sur la protection des renseignements personnels dans le secteur privé*, L.R.Q. c. P-39.1, en ligne : Les publications du Québec <http://publicationsduquebec.gouv.qc.ca/fr/cgi/frameset.cgi?url=/documents/lr/P_39_1/P39_1.html> (date d'accès 30 août 2001) ; *Loi sur la protection des renseignements personnels et les documents électroniques*, L.R.C. 1985, c. P-8.6, en ligne : Ministère de la justice <http://lois.justice.gc.ca/fr/P-8.6/74408.html> (date d'accès : 30 août 2001). Ces lois offrent des protections aux individus face aux organismes du secteur privé.

70 *Mills, supra* note 16 au para. 89.

71 Aujourd'hui : 184(2)a) *du Code criminel*, tel que modifié par la *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, c. 40, art. 3.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

ministère public voulait se servir de ces communications en preuve, d'autant plus que l'agent d'infiltration s'en était servies pour confectionner ses notes, ce à quoi s'objectait Duarte.

La question était donc de savoir si ce qu'on appelle communément la surveillance "consensuelle" ou "participative", c'est-à-dire la surveillance électronique dans un cas où l'un des participants à une conversation -généralement un agent d'infiltration ou un indicateur- l'enregistre subrepticement, porte atteinte au droit garanti par l'article 8 de la *Charte canadienne* à la protection contre les fouilles, les perquisitions et les saisies abusives.

En l'espèce, malgré la violation de l'article 8 de la *Charte canadienne*, la preuve n'a finalement pas été exclue en vertu de 24(2) de la *Charte canadienne*. Par contre, les principes énoncés en matière de surveillance électronique restent entiers.

En principe, la surveillance électronique d'un particulier par un organe de l'État constitue une fouille, perquisition ou saisie abusive au sens de l'art. 8 de la *Charte canadienne*[72].

La Cour, par la plume du juge La Forest, conclut:

> « *Une conversation avec un indicateur n'est pas une fouille, une perquisition ou une saisie au sens de la Charte. Toutefois l'interception et l'enregistrement électroniques clandestins d'une communication privée*[73] *en sont (note rajoutée). De plus, l'enregistrement devrait être considéré comme une fouille, une perquisition ou une saisie dans toutes les circonstances, à moins que tous les participants à la conversation n'aient expressément consenti à ce qu'elle soit enregistrée. Il s'ensuit que la constitutionnalité de la surveillance participative devrait se décider par l'application de la même norme que dans le cas de la surveillance par un tiers, c.-à-d. par l'application de la norme du caractère raisonnable énoncée dans l'arrêt Hunter c. Southam Inc., précité. Quand on applique cette norme, la surveillance participative sans mandat faite par la police en l'espèce était manifestement inconstitutionnelle* »[74].

La Cour arrive donc à la conclusion qu'une autorisation judiciaire préalable est nécessaire dans ce cas. La rationalité sous-jacente au raisonnement du juge La Forest semble être l'affirmation suivante :

> « *Puisque nous ne pouvons jamais savoir si notre interlocuteur est un indicateur et que, s'il en est un, nous sommes réputés avoir accepté tacitement le risque que l'État écoute et enregistre nos conversations, nous devons être prêts à courir ce risque chaque fois que nous parlons. Je conclus donc que l'analyse fondée sur le risque adoptée par la Cour d'appel aboutit logiquement à l'anéantissement de toute aspiration au respect de la vie privée.*

---

[72] *Duarte, supra* note 51 à la p. 42.

[73] Nous soumettons que l'on devrait plutôt lire «communication faite en privée ou bénéficiant d'une expectative raisonnable de vie privée» plutôt que «communication privée» au sens du *Code criminel.* En effet, vu le consentement d'un des interlocuteurs et l'absence d'interception par un tiers, il ne s'agissait pas d'une communication privée au sens de l'article 184 du *Code criminel.*

[74] *Duarte, supra* note 51 à la p. 57.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

Je ne vois pas de similitude entre le risque que quelqu'un écoute nos propos avec l'intention de les répéter et le risque couru quand quelqu'un les écoute et en fait simultanément un enregistrement électronique permanent. Ces risques ne sont pas du même ordre de grandeur. Dans le contexte de l'application des lois, l'un des risques peut être considéré comme une atteinte raisonnable à la vie privée, l'autre une atteinte abusive. Ils présentent pour les individus et la société des dangers différents. En d'autres termes, le droit reconnaît que nous devons par la force des choses assumer le risque posé par le "rapporteur", mais refuse d'aller jusqu'à conclure que nous devons en outre supporter, comme prix de l'exercice du choix d'adresser la parole à un autre être humain, le risque que soit fait un enregistrement électronique permanent de nos propos »[75].

Les premiers jalons du concept de surveillance électronique, en dehors du contexte des «communications privées» au sens du *Code criminel*, venaient d'être posés. Il y avait eu renonciation de la part d'un des participants à la conversation, d'où l'absence d'aspect « privé » de la communication au sens de l'article 184 *du Code criminel*[76]. La Cour venait donc de confirmer la notion qu'une protection constitutionnelle résiduelle peut s'appliquer dans un contexte donné[77]. Par contre, le contexte de la surveillance électronique semble être très large aux yeux de la Cour, plus particulièrement à ceux du juge La Forest. En effet, l'affirmation voulant qu'en principe, la surveillance électronique d'un particulier par un organe de l'État constitue une fouille, perquisition ou saisie abusive au sens de l'art. 8 de la *Charte canadienne*, constitue un bon exemple de ce que nous appelons l'approche de principe. Cette affirmation semble basée sur un principe qui fait fi des autres éléments contextuels apportés par les faits de la cause[78].

Nous pensons plutôt qu'il s'agit d'un énoncé de principe qui doit être placé dans le contexte de la surveillance participative où deux individus, en présence l'un de l'autre dans un appartement, donc dans des circonstances telles que l'on pouvait raisonnablement s'attendre à bénéficier d'une certaine confidentialité, s'adressent la parole alors que l'un d'eux fait,

---

75 *Duarte, Ibid.* aux pp. 47-48.

76 L'alinéa 184 (2) a) du *Code criminel*, prévoit qu'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, «n'intercepte» pas la communication au sens du paragraphe 184(1) du *Code criminel.*

77 Cette décision a entraîné l'adoption de la *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, c. 40, concernant notamment la surveillance participative. Voir les articles 183.1, 184.1, 184.2, 184.3, 184.4 du *Code criminel*, entrés en vigueur le 1er août 1993.

78 Dans *R. c. Wijesinha*, [1995] 3 R.C.S. 422. Le ministère public a concédé que, que l'obtention des conversations entre le policier et l'appelant à l'aide d'un micro émetteur, a porté atteinte aux droits de l'appelant garantis par l'art. 8 de la *Charte canadienne*. Nous sommes d'avis qu'une telle concession n'aurait pas dû être faite, du moins depuis la décision rendue dans *Edwards, supra* note 15 dont nous parlerons plus loin. De plus, dans *Wijesinha*, l'accusé savait qu'il parlait à un policier. Il ne pouvait conséquemment s'attendre subjectivement qu'un policier identifié ne l'enregistre pas dans un contexte où une activité illégale, du moins du point de vue déontologique, est proposée au policier. Dans *R. c. Shergill* (1997), 23 O.T.C. 290 (Gen. Div.), il a été décidé que l'enregistrement subreptice d'une déclaration faite par un individu à un policier ne bénéficiait pas de la protection de l'article 8 de la *Charte canadienne*. En effet, la cour a déterminé que l'individu ne pouvait raisonnablement s'attendre à ce que sa conversation ne soit pas entendue par des agents de l'État : la déclaration a effectivement été faite à des policiers identifiés et en fonction ! Dans ce contexte, l'identité de l'interlocuteur, dans la mesure où elle est révélée et qu'il s'agit d'un agent de l'État, a effectivement de l'importance dans la détermination de ce qui constitue ou non une communication bénéficiant d'une expectative raisonnable de vie privée.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

simultanément, un enregistrement électronique clandestin (audiovisuel) de leurs échanges verbaux. Cet énoncé semble redondant, mais il est nécessaire afin de pouvoir faire les distinctions appropriées dans les contextes apportés par Internet et les nouvelles TI. Il est également utile, compte tenu de l'approche qui sera favorisée plus tard par la Cour.

Section III - L'arrêt *Wong* et le début de la fin de l'approche de principe

Dans *Wong* la Cour suprême du Canada est venue préciser la nature de la protection accordée par l'article 8 de la *Charte canadienne* contre l'enregistrement magnétoscopique effectué subrepticement dans des chambres d'hôtel par la police en l'absence d'autorisation judiciaire. Dans cette affaire un groupe de joueurs retenaient régulièrement une chambre d'hôtel dans le but de s'adonner à leur passion. Les personnes avaient accès à ce lieux, qui était tenu verrouillé, uniquement sur invitation.

Après avoir conclu que la surveillance magnétoscopique était le seul moyen pratique d'observer le déroulement des activités dans la chambre, les policiers ont installé une caméra vidéo dans la cantonnière des rideaux de la chambre retenue par M. Wong. La caméra, dont la lentille avait environ la dimension d'une mine de crayon, était reliée à du matériel d'enregistrement simultané qui permettait de surveiller l'intérieur d'une chambre d'hôtel adjacente. Les policiers ont installé ce matériel avec la permission et la collaboration de la direction de l'hôtel. M. Wong et dix autres prévenus ont par la suite été accusés d'avoir tenu une maison de jeu.

Cette décision reprend notamment les principes énoncés en matière de surveillance participative dans *Duarte* et confirme qu'une surveillance magnétoscopique effectuée subrepticement par des agents de l'État constitue une perquisition, une fouille et une saisie au sens de l'article 8 de la *Charte canadienne*[79]. De plus la Cour conclut que les principes énoncés dans l'arrêt *Duarte* embrassent tous les moyens actuels permettant à des agents de l'État de s'introduire électroniquement dans la vie privée des personnes, et tous les moyens que la technologie pourra à l'avenir mettre à la disposition des autorités chargées de l'application de la loi[80]. Cet énoncé ressemble, du moins quant à sa formulation, à celui mentionné plus haut dans *Duarte*. Il s'agit en fait d'un énoncé qui s'appuie plus sur les principes que sur les faits.

Nous sommes d'avis que l'expectative raisonnable de vie privée de M. Wong a été déterminée par le biais d'un critère objectif plutôt général. Le juge La Forest pour la majorité affirme à cet effet :

> « *La question devrait plutôt être posée en termes plus généraux et plus neutres de sorte que l'on se demande plutôt si dans une société comme la nôtre, les personnes qui se retirent dans une chambre d'hôtel et qui ferment la porte*

[79] *Wong, supra* à la note 53 à la p. 43. Il est à noter que la surveillance vidéo n'était pas permise à cette époque. La décision rendue dans *Wong*, a entraîné l'adoption de dispositions dans la *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, c. 40, concernant notamment la surveillance par vidéo. Voir les articles 487.01, 487.02 et 487.03 du *Code criminel*, entrés en vigueur le 1er août 1993.

[80] *Ibid.* aux pp. 43-44.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

derrière elles peuvent raisonnablement s'attendre au respect de leur vie privée »[81]. (soulignés rajoutés)

Le juge La Forest considère les faits de l'espèce en les opposant à une norme générale de respect de la vie privée dans le cadre d'une société libre et démocratique dont une personne jouit en tout temps. Étant donné qu'on ne saurait accepter dans une telle société que les agents de l'État puissent braquer des caméras dissimulées sur des membres de la société, en tout temps et en tout lieu, à leur gré, le juge La Forest conclut à une violation de l'article 8 de la *Charte*. On ne semble pas faire la différence entre l'expectative raisonnable de vie privée de M. Wong dans ces circonstances et l'expectative raisonnable de vie privée de toute personne se trouvant dans une chambre d'hôtel[82].

Le juge Lamer, dans une opinion dissidente, conclut plutôt qu'il n'y avait pas d'attente raisonnable en matière de vie privée. Malgré la longueur de la citation il convient ici de la reproduire pour bien comprendre la distinction faite par la Cour entre ce que nous avons appelé l'approche de principe et l'approche pragmatique ou au cas par cas :

« *Je conviens avec mon collègue que la surveillance électronique subreptice non autorisée peut, dans certaines circonstances, porter atteinte aux droits garantis par l'art. 8. Je conviens qu'une telle surveillance porte atteinte à l'art. 8 lorsque la personne qui en fait l'objet peut raisonnablement s'attendre au respect de la vie privée. Toutefois, à mon avis, la question de savoir si une personne a une attente raisonnable en matière de respect de la vie privée ne peut être tranchée que dans le contexte factuel particulier de la surveillance, et non en fonction d'une notion générale de respect de la vie privée dans une société libre et démocratique dont une personne jouit en tout temps. Une personne a le droit, aux termes de l'art. 8, de ne pas être assujettie à une surveillance électronique subreptice non autorisée lorsqu'elle s'attend raisonnablement à ce que les agents de l'État ne surveillent pas ses activités ou ses conversations privées et ne les enregistrent pas. La question de savoir si une telle attente est raisonnable dépendra des circonstances particulières; une personne ne jouit pas nécessairement de ce droit dans toutes les circonstances. Il suffit pour régler l'espèce de se demander si l'appelant pouvait raisonnablement s'attendre au respect de la vie privée dans cette chambre d'hôtel qui avait en fait été convertie en maison de jeu publique. Il n'est pas nécessaire de décider si l'appelant aurait une telle attente en toutes circonstances selon une notion générale du respect de la vie privée. L'étendue du concept de l'attente raisonnable en matière de respect de la vie privée sera déterminée par les situations de fait qui surviendront dans l'avenir.*

Je souscris à l'opinion du juge La Forest qu'une personne qui se retire dans une chambre d'hôtel et qui ferme la porte derrière elle s'attendra normalement et raisonnablement au respect de sa vie privée. La nature de l'endroit où la surveillance a lieu sera toujours un facteur important dont il faudra tenir compte pour déterminer si la personne cible s'attend raisonnablement au respect de la vie privée dans les circonstances. Ce facteur n'est toutefois pas

[81] *Ibid*. à la p. 50.
[82] *Ibid*. aux pp. 48-57.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

déterminant. Une personne qui se trouve dans ce qui serait normalement qualifié de lieu public (un restaurant, par exemple) peut très bien s'attendre raisonnablement au respect de la vie privée. Par exemple, elle ne s'attendrait raisonnablement pas à ce que la police surveille et enregistre subrepticement la conversation privée qu'elle tient à sa table. De la même façon, ce qui serait normalement qualifié de lieu privé (une résidence personnelle, par exemple) peut très bien, selon son utilisation, devenir un lieu où une personne ne saurait s'attendre raisonnablement au respect de la vie privée.

L'attente en matière de respect de la vie privée qui existe normalement à l'égard d'une chambre d'hôtel ne sera pas restreinte par le fait qu'une activité illégale peut s'y dérouler, et elle ne sera pas nécessairement écartée par le simple fait que d'autres personnes ont été invitées dans la chambre. Toutefois, dans certains cas, d'autres faits pourront indiquer que la personne visée n'a pas une attente raisonnable en matière de respect de la vie privée.

En l'espèce, l'appelant se trouvait dans une chambre d'hôtel. Dans la plupart des cas, une chambre d'hôtel est un lieu dans lequel une personne s'attend raisonnablement au respect de la vie privée. Toutefois, en l'espèce, l'appelant avait, au hasard, lancé des invitations aux séances de jeu qui devaient avoir lieu dans la chambre d'hôtel. Il avait distribué de nombreux avis dans des restaurants publics et des bars, invitant de la sorte le public à la chambre d'hôtel. Il est impossible de conclure qu'une personne raisonnable, dans la situation de l'appelant, pourrait s'attendre au respect de la vie privée dans de telles circonstances. Une personne raisonnable saurait que lorsqu'une telle invitation est lancée au grand public, elle ne peut désormais plus s'attendre à ce qu'il n'y ait pas d'étrangers, y compris des policiers, dans la chambre. En l'espèce, les policiers étaient présents dans la chambre par l'entremise de la caméra vidéo qui avait été installée dans la cantonnière des rideaux.

Je ne veux pas que l'on pense que j'adopte l'« analyse fondée sur le risque » que cette Cour a rejetée dans l'arrêt Duarte, précité. Je ne confonds pas le risque que des étrangers se trouvent dans une chambre d'hôtel et le risque que des policiers enregistrent électroniquement l'activité dans la chambre d'hôtel. La question ne porte pas tant sur le risque mais sur les attentes raisonnables. En l'espèce, il n'était pas raisonnable que l'appelant s'attende à ce qu'il n'y ait pas d'étrangers, voire des policiers, dans la chambre.

L'appelant aurait bien pu s'attendre raisonnablement au respect de la vie privée dans la chambre d'hôtel en cause s'il avait lancé quelques invitations à des personnes en particulier. Toutefois, ce n'est pas le cas en l'espèce. À mon avis, et avec égards pour les autres opinions, l'appelant n'avait aucune attente raisonnable en matière de vie privée dans ces circonstances; par conséquent, il n'y a pas eu fouille ou perquisition au sens de l'art. 8 »[83]

[83] *Ibid*. aux pp.61-63.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>

Le critère de l'ensemble des circonstances, qui constitue ce que nous avons appelé l'approche pragmatique ou au cas par cas, était donc favorisé par le juge Lamer. Il convient maintenant de traiter des décisions qui ont concrétisé l'application de cette approche dissidente.

Chapitre III - La détermination de l'expectative raisonnable de vie privée et l'approche pragmatique ou au cas par cas

Dans le présent chapitre, nous traiterons de l'effritement de l'approche de principe dans *Wise*[84], du fait que l'approche pragmatique ou au cas par cas se précise davantage dans l'arrêt *Plant*[85], de la consécration de l'approche pragmatique ou au cas par cas et la notion d'intérêt à soulever une violation constitutionnelle dans *Edwards*[86], pour finalement conclure sur le concept de l'approche pragmatique ou au cas par cas.

Section I - L'approche de principe s'effrite de plus en plus dans l'arrêt *R. c. Wise*

Il s'agissait ici de déterminer si la surveillance d'un véhicule exercée au moyen d'une balise constitue une fouille abusive pour les fins de l'article 8 de la *Charte canadienne*.

L'appelant a été accusé d'avoir commis un méfait à l'égard d'un bien, contrairement au par. 387(3) (maintenant le par. 430(3)) du *Code criminel.* Afin d'établir sa culpabilité, le ministère public a tenté d'introduire la preuve de ses allées et venues, obtenue grâce à un dispositif de surveillance électronique (une "balise") dissimulé dans sa voiture. Une balise est un poste émetteur, ordinairement à piles, qui émet périodiquement des signaux pouvant être captés par un récepteur.

La "balise" a été dissimulée dans le caoutchouc mousse du siège arrière du véhicule de M. Wise, ce qui l'a légèrement endommagé. Cette installation, a conclu le juge du procès, a été effectuée sur la foi d'un "simple soupçon" et, naturellement, sans autorisation judiciaire. Ce dispositif a permis aux policiers de suivre M. Wise jour et nuit, même s'il s'agissait d'un dispositif assez rudimentaire qui, aux dires de son installateur, n'indiquait qu'une localisation générale. La balise émettait un signal radio pouvant être capté sur une distance de trois kilomètres par un récepteur à balayage des policiers.

Le juge Cory, pour la majorité, y compris le juge Lamer, a déterminé que la surveillance du véhicule de M. Wise exercée au moyen d'une balise déjouait une attente raisonnable en matière de respect de la vie privée puisque cette activité de la police constituait également une fouille[87]. Par contre, bien qu'il subsiste une certaine attente en matière de respect de la vie privée lorsqu'on circule en automobile, cette attente est manifestement moindre que celle qui existe à l'intérieur de la résidence ou du bureau.

---

84 *Supra* note 46.
85 *Supra* note 34.
86 *Supra* note 15.
87 *Wise, supra* note 46 à la p. 538. De toute façon le ministère public avait admis que l'installation de la balise constituait une fouille abusive en violation de l'article 8 de la *Charte canadienne*. On pourrait fonder cette position sur les principes énoncés dans *Duarte* et *Wong* voulant que tous les moyens actuels permettant à des agents de l'état de s'introduire électroniquement dans la vie privée des personnes, et tous les moyens que la technologie pourra mettre à l'avenir à la disposition des autorités chargées de l'application de la loi, constituent une violation de l'article 8 de la *Charte*.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

De plus, le non-respect de l'attente qui subsiste à cet égard par suite de l'utilisation du dispositif en question est minime. La balise en cause ici était un prolongement très rudimentaire de la surveillance visuelle. La balise était fixée au véhicule de l'appelant et non à l'appelant lui-même. Un tel dispositif est très différent, tant dans son fonctionnement que dans son incidence sur la personne, de la caméra vidéo cachée ou du dispositif de surveillance électronique qui intercepte clandestinement les communications privées.

L'atteinte à l'expectative raisonnable de vie privée étant moindre en l'espèce, la Cour a conclu que la preuve en violation des droits de l'article 8 de la *Charte canadienne*, ne devait pas finalement être écartée en vertu du paragraphe 24(2)[88]. Cette décision a par la suite justifié la mise en vigueur le 1er août 1993 de l'article 492.1 du *Code criminel*, qui prévoit notamment une norme d'émission moindre que celle énoncée dans *Hunter*, soit les «motifs raisonnables de soupçonner» plutôt que les «motifs raisonnables de croire»[89].

On constate donc que le niveau d'intrusion de la technologie utilisée pour surveiller électroniquement sera désormais pris en considération dans l'analyse de l'existence d'une violation de l'article 8 de la *Charte canadienne*[90]. Cette façon d'envisager la surveillance électronique se démarque ainsi des premiers arrêts rendus par la Cour suprême dans *Duarte* et *Wong*, desquels on aurait pu croire en l'existence d'une norme plus générale d'appréciation de l'existence d'une violation de l'article 8 de la *Charte canadienne*.

Le juge La Forest, dissident, reprend essentiellement les raisonnements énoncés dans les arrêts *Duarte* et *Wong*, pour conclure que l'intrusion initiale et la surveillance subséquente, constituaient des violations aux droits garantis par l'article 8 de la *Charte canadienne*. Bien que le juge La-Forest concède que l'expectative raisonnable de vie privée est moindre dans une voiture que dans un domicile, il considère toutefois que la surveillance électronique en l'espèce était grave et que la *Charte canadienne* devrait s'appliquer dans toute sa vigueur[91].

Section II - L'approche pragmatique ou au cas par cas se précise davantage dans l'arrêt *Plant*

Cette décision soulève la question de savoir si la vérification par la police de données informatiques, appartenant à un établissement public, constitue une perquisition. L'inspection par l'État de dossiers informatisés de consommation d'électricité a-t-elle été effectuée en violation de l'article 8 de la *Charte canadienne* ? Une description précise des faits est importante pour bien saisir la portée des principes énoncés dans ce contexte particulier.

Afin de pouvoir obtenir confirmation de renseignements fournis par un informateur anonyme concernant une culture illégale de chanvre indien, et ce, dans le but d'obtenir un mandat de perquisition, un policier utilise un terminal se trouvant dans la section des enquêtes du service de police de Calgary, et qui était relié à l'unité centrale des services publics de la ville; grâce à

---

88 *Ibid.* à la p. 548.

89 *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, c. 40.

90 Voir également l'article 492.2 du *Code criminel*, qui traite de la technologie de l'enregistreur de numéro de téléphone, résultat de la décision *R. c. Feagan* (1993), 80 C.C.C. (3d) 356 (Ont. C.A.). On applique la même logique que l'arrêt *Wise* ; il y aurait atteinte à l'article 8 de la *Charte*, dans le contexte d'une expectative raisonnable de vie privée moindre, d'où l'exigence réduite de «motifs de soupçonner».

91 *Wise, supra* note 46 aux pp. 549 à 67.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

ce terminal, la police pouvait, moyennant un mot de passe, vérifier la consommation d'électricité à une adresse donnée.

En comparant la consommation d'électricité de l'endroit visé pendant les six mois précédents avec celle de deux résidences de dimension comparable à Calgary, le policier a constaté que la consommation à cette adresse était, pour cette même période, quatre fois supérieure à la moyenne des deux autres. Cette information permit notamment au policier d'obtenir un mandat de perquisition visant la résidence en question. On devait donc déterminer si cette information dénoncée au soutien du mandat de perquisition visant la résidence, devait préalablement être elle-même obtenue par le biais d'un mandat de perquisition visant les installations de la compagnie d'électricité.

Après avoir repris les principes de *Dyment*[92] pour dégager certains des paramètres de la protection accordée par l'art. 8 de la *Charte canadienne* à l'égard des aspects informationnels de la vie privée et du fait qu'il ne soit pas nécessaire d'établir un lien de propriété entre la chose obtenue, dans ce cas l'information, le juge Sopinka, pour la majorité, énonce que l'examen de facteurs tels la nature des renseignements, celle des relations entre la partie divulguant les renseignements et la partie en réclamant la confidentialité, l'endroit où ils ont été recueillis, les conditions dans lesquelles ils ont été obtenus et la gravité du crime faisant l'objet de l'enquête, permet de pondérer les droits de la société à la protection de la dignité, de l'intégrité et de l'autonomie de la personne et l'application efficace de la loi[93]. Le juge conclut qu'il convient d'appliquer cette méthode contextuelle aux faits de l'espèce, ce qui en soi, semble déroger aux affirmations de principe en matière de surveillance électronique, énoncées par le juge La Forest dans les arrêts *Duarte* et *Wong*.

La Cour (avec l'appui du juge La Forest!) a déterminé en l'espèce qu'il n'y avait pas d'expectative raisonnable de vie privée à l'égard des renseignements de consommation d'électricité obtenus par les policiers pour les raisons suivantes :

- Ils ne sont pas de nature «personnelle et confidentielle»
- Ils ne sont pas biographiques
- Ils ne sont pas d'ordre personnel en ce sens que les particuliers pourraient, dans une société libre et démocratique, vouloir les constituer et les soustraire à la connaissance de l'État
- Ils ne tendent pas à révéler, notamment, des détails intimes sur le mode de vie et les choix personnels de l'individu
- Ils sont de nature commerciale et ne bénéficient pas d'une relation contractuelle obligeant d'en préserver la confidentialité
- Ils sont de nature commerciale ne satisfaisant pas à la norme de la «nature personnelle et confidentielle»
- Ils étaient accessibles au grand public
- Il n'y a pas intrusion dans des endroits ordinairement considérés comme privés, comme c'était le cas dans les arrêts *Duarte* et *R. c. Wong*[94]

---

92 *Supra* note 38 aux pp. 429-30.
93 *Plant, supra* note 34 aux pp. 291, 293.
94 *Wong*, *supra* note 53.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

- Il n'y a pas intrusion de mandataires de l'État dans les dossiers informatiques personnels constitués confidentiellement par un particulier (en l'espèce l'accusé)
- Il n'y a pas intrusion ou autorité de mandataires de l'État dans les locaux de l'organisme détenant les informations
- La gravité de l'infraction en l'espèce (participation au commerce illicite de chanvre indien) milite en faveur de la conclusion que les exigences de l'application de la loi l'emportent sur le droit de l'appelant au respect de sa vie privée
-

M. Plant n'a donc pas réussi à inscrire l'immixtion des agents de l'État dans les paramètres de l'art. 8 de la *Charte canadienne*. Les policiers pouvaient donc invoquer les données recueillies à l'appui de leur demande de mandat de perquisition[95].

Section III - L'approche pragmatique ou au cas par cas et la notion d'intérêt à soulever une violation constitutionnelle consacrée dans l'arrêt *Edwards*

Dans cette affaire, l'accusé a été déclaré coupable de possession de drogue en vue d'en faire le trafic. Il avait été soupçonné d'en faire le trafic à partir de sa voiture au moyen d'un téléphone cellulaire et de garder de la drogue chez lui ou à l'appartement de son amie. La police l'a arrêté relativement à une infraction au code de la route. Deux policiers se sont présentés à l'appartement de l'amie de l'accusé et ont obtenu sa collaboration en lui faisant un certain nombre de déclarations, certaines mensongères, d'autres à moitié vraies. La preuve était contradictoire quant à savoir si ces déclarations avaient été faites avant ou après que les policiers eurent été admis dans l'appartement. Dès qu'ils furent entrés, l'amie de l'accusé leur a indiqué l'endroit où était cachée une importante quantité de drogue. Au procès et en appel, l'accusé a nié être le propriétaire de la drogue. Il s'agissait donc de savoir si un accusé pouvait contester l'admission d'éléments de preuve obtenus par suite d'une perquisition dans les lieux occupés par un tiers.

La Cour, par la plume du juge Cory, énonce les critères à considérer lorsque l'on doit établir le droit à la protection contre les fouilles saisies ou les perquisitions abusives, garanti par l'article 8 de la *Charte canadienne*:

> « *Un examen des arrêts récents de notre Cour et de ceux de la Cour suprême des États-Unis, que j'estime convaincants et applicables à bon droit à la situation dont nous sommes saisis, indique qu'il est possible de dégager certains principes quant à la nature du droit à la protection contre les fouilles, les perquisitions ou les saisies abusives, garanti par l'art. 8. J'estime qu'ils peuvent être résumés de la façon suivante:*
>
> *1 Une demande de réparation fondée sur le par. 24(2) ne peut être présentée que par la personne dont les droits garantis par la Charte ont été violés. Voir R. c. Rahey, [1987] 1 R.C.S. 588, à la p. 619.*

[95] *Plant, supra* note 34 aux pp. 291, 294-96. Ces critères ont notamment été repris par la Cour dans *Schreiber*, *supra* note 17 dans le contexte de l'obtention d'information bancaire à l'étranger par le biais d'une demande d'entraide juridique présentée par le Canada aux autorités suisses.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

2 Comme tous les droits garantis par la Charte, l'art. 8 est un droit personnel. Il protège les personnes et non les lieux. Voir Hunter, précité.

3 Le droit d'attaquer la légalité d'une fouille ou perquisition dépend de la capacité de l'accusé d'établir qu'il y eu violation de son droit personnel à la vie privée. Voir Pugliese, précité.

4 En règle générale, deux questions distinctes doivent être posées relativement à l'art. 8. Premièrement, l'accusé pouvait-il raisonnablement s'attendre au respect de sa vie privée? Deuxièmement, si tel est le cas, la fouille ou la perquisition a-t-elle été effectuée de façon raisonnable par la police? Voir Rawlings, précité.

5 L'existence d'une attente raisonnable en matière de vie privée doit être déterminée eu égard à l'ensemble des circonstances. Voir Colarusso, précité, à la p. 54, et Wong, précité, à la p. 62.

6 Les facteurs qui peuvent être pris en considération dans l'appréciation de l'ensemble des circonstances incluent notamment:

(i) la présence au moment de la perquisition;

(ii) la possession ou le contrôle du bien ou du lieu faisant l'objet de la fouille ou de la perquisition;

(iii) la propriété du bien ou du lieu;

(iv) l'usage historique du bien ou de l'article;

(v) l'habilité à régir l'accès au lieu, y compris le droit d'y recevoir ou d'en exclure autrui;

(vi) l'existence d'une attente subjective en matière de vie privée;

(vii) le caractère raisonnable de l'attente, sur le plan objectif.

Voir United States c. Gomez, 16 F.3d 254 (8th Cir. 1994), à la p. 256.

7 Si l'accusé établit l'existence d'une attente raisonnable en matière de vie privée, il faut alors, dans un deuxième temps, déterminer si la perquisition ou la fouille a été effectuée de façon raisonnable »[96].

C'est à partir de ce moment que la notion d'intérêt a été confirmée pour être en mesure de faire valoir une violation. Dans le cas de M. Edwards, il n'a pas pu soulever l'intérêt requis pour contester la validité de l'immixtion étatique survenue dans l'appartement de son amie. Il n'était donc plus nécessaire de déterminer si la perquisition ou la fouille a été effectuée de façon raisonnable, car il n'y en avait pas eu à son égard!

Il est intéressant de noter que le juge Cory adopte la position dissidente du juge Lamer dans *Wong*. La Cour confirme donc la notion de la détermination selon l'ensemble des circonstances, ce que nous avons appelé l'approche pragmatique ou au cas par cas. De plus, il est également intéressant de noter que le juge Cory siégeait à la Cour d'appel de l'Ontario dans *Wong*. À l'instar du juge Lamer dans *Wong*, le juge Cory avait décidé qu'il n'y avait pas d'expectative raisonnable de vie privée dans la chambre d'hôtel où les joueurs s'étaient réunis. Comme nous l'avons vu, la Cour, par la plume du juge La Forest a infirmé le jugement rendu par la Cour d'appel de l'Ontario. La décision rendue dans l'arrêt *Edwards* constitue, à notre avis, la douce revanche du juge Cory contre le juge La Forest qui, bien sûr, était dissident sur la question de la nécessité de soulever un intérêt suffisant dans *Edwards*!

[96] *Edwards*, *supra* note 15 aux pp.145-46.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

Section IV - Conclusion quant à l'approche pragmatique ou au cas par cas

Afin de bénéficier de la protection de l'article 8 de la *Charte canadienne*, un individu doit avoir une expectative raisonnable de vie privée eu égard à la chose obtenue par l'État ou de l'information qui en découle. C'est donc dire que l'article 8 de la *Charte canadienne* ne protège pas un individu qui ne détient pas d'expectative raisonnable de vie privée dans les circonstances ayant donné lieu à l'obtention ou l'immixtion[97]. C'est la notion de *standing* ou d'intérêt à pouvoir invoquer une violation de ses droits[98]. L'individu ne possédant pas le *standing* requis, ne pourra bénéficier de la protection constitutionnelle de l'article 8 de la *Charte canadienne*. La notion d'intérêt est donc intimement liée à l'existence ou non d'une protection constitutionnelle.

Un individu qui agit illégalement et, par le fait même, en un lieu servant exclusivement à la commission d'infractions jouit néanmoins de la protection constitutionnelle[99] dans la mesure où il pourra établir qu'il bénéficiait dans ce lieu d'une expectative raisonnable de vie privée On ne peut justifier une immixtion de l'État en invoquant après le fait, qu'il y avait activité illégale.

Le besoin de respect de la vie privée peut varier selon la nature de ce qu'on veut protéger, les circonstances de l'ingérence de l'État, l'endroit où celle-ci se produit, et les buts de l'ingérence[100].

L'intérêt qu'a un plaignant dans la protection de sa vie privée est très élevé lorsque des renseignements ou informations contenus dans un dossier, portent sur son identité personnelle ou que la confidentialité du dossier est essentielle pour protéger une relation thérapeutique[101].

Doit-on appliquer les critères de détermination de l'expectative raisonnable de vie privée tels qu'établis dans les arrêts *Edwards*[102] (obtention d'une preuve de nature matérielle tangible) de façon complémentaire ou séparée des critères établis par les arrêts *Plant*[103] (obtention d'une preuve de nature informationnelle intangible) ? Sans dire qu'il s'agit d'une approche empirique, il faut quand même faire preuve de prudence et éviter de les appliquer machinalement comme les ingrédients d'une recette. Il semble qu'aucun facteur ne soit déterminant en soi. L'énumération énoncée dans l'arrêt *Edwards* au 6^{e} point commence par le mot « notamment », ce qui annonce que d'autres critères pourront être considérés.

Ces énumérations ne doivent pas être considérées comme une liste magique qui confirme ou infirme dans chaque cas l'existence ou non d'une quelconque expectative raisonnable de vie privée. Dans bien des cas l'existence ou non d'une expectative raisonnable de vie privée dans une situation ou un contexte donné, sera considérée comme une affirmation de principe qui sera modulée dans un sens ou dans l'autre, selon les circonstances particulières de chaque cas.

---

97 *M.R., supra* note 48.
98 *Edwards*, *supra* note 15.
99 *Wong*, *supra* note 53 aux pp. 49-50; *Duarte*, *supra* note 51 aux pp. 51-52.
100 *R. c. Colarusso*, [1994] 1 R.C.S. 20, 53 [ci-après *Colarusso*]. Nous assimilons ici les concepts d'ingérence et d'immixtion.
101 *Mills*, *supra* note 16 au para. 94.
102 *Supra* note 15 aux pp. 145-46. Ces critères on été repris dans *Belnavis, supra* note 15 ; *R. c. Lauda,* [1998] 2 R.C.S. 683, par.1 [ci-après *Lauda*]
103 *Plant*, *supra* note 34 à la p. 293.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

Malgré les difficultés rencontrées en matière de détermination de ce qui constitue effectivement une situation où un individu bénéficiera d'une expectative raisonnable de vie privée, il convient ici de traiter des cas où l'on a eu à décider s'il en existait une. Ces cas doivent être considérés avec prudence, en ayant notamment à l'esprit la chronologie de l'évolution des deux types d'approche dont nous avons traité précédemment.

Chapitre IV - L'expectative raisonnable de vie privée inexistante, reconnue ou réduite?

Dans ce chapitre nous traiterons des cas où l'expectative raisonnable de vie privée était inexistante, reconnue ou réduite. Ces cas nous démontrent que la *Charte canadienne* s'applique à des degrés différents, selon les contextes.

Section I - Exemples de cas où l'expectative raisonnable de vie privée est inexistante

Les tribunaux ont donc déterminé qu'il n'y avait pas d'expectative raisonnable de vie privée pour les fins de l'article 8 de la *Charte canadienne*, sur une terre agricole privée sur laquelle un individu, commettant une intrusion *(trespass)*, cultive des plants de marijuana à la vue de tous[104], sur un terrain de la Couronne où sont cultivés des plants de marijuana à la vue de tous[105], lors d'une conversation avec un indicateur de police[106], lors d'une poursuite immédiate[107], à l'égard des renseignements contenus dans les dossiers informatisés d'une société de services publics démontrant une consommation anormale d'électricité et qui étaient susceptibles d'être vérifiés par le public[108], sur les images photographiques ou vidéo prises d'un individu alors qu'il déambule dans un lieu public, comme un parc, le métro ou un commerce (aux heures d'affaires)[109], sur un objet abandonné par un individu sur la voie publique, tel un véhicule[110], en matière de contrôle de sécurité routière[111], sur les observations faites dans le vestibule d'un immeuble à logements[112], sur les rebuts abandonnés sur le bord de la rue pour être ramassés[113], sur les données d'un abonné téléphonique quant à son nom, adresse et numéro de téléphone lorsque celles-ci ne sont pas privées et qu'on aurait pu les retrouver dans un bottin téléphonique[114], sur les propos transmis par un téléavertisseur vocal

---

104 *Lauda, supra* note 102 à la p. 683, par.1.
105 *R. c. Boersma*, [1994] 2 R.C.S. 488, 489.
106 *Duarte*, *supra* note 51 à la p. 57
107 *R c. Macooh*, [1993] 2 R.C.S. 802.
108 *Plant*, *supra* note 34.
109 *R. c. Mills,* [1993] R.J.Q. 2563 (C.A.Qc.); (1993) 82 C.C.C. (3d) 455 (version traduite en anglais); requête en autorisation de pourvoi rejetée [1993] 4 R.C.S.
110 *R. c. Goodleaf*, [1997] A.Q. No 2665 (C.A.Qc.). Dans le contexte de l'abandon des objets lors d'une arrestation, voir *R. c. Stillman*, [1997] 1 R.C.S. 607 [ci-après *Stillman*], aux pp. 644-48. Dans certains cas, il pourra exister une attente raisonnable de vie privée à l'égard de la chose abandonnée, notamment si elle l'est dans le contexte d'une violation d'un droit prévu à la *Charte canadienne*, comme la violation du droit à l'avocat.
111 *R. c. Hufsky*, [1988] 1 R.C.S. 621 et *R. c. Ladouceur*, [1990] 1 R.C.S. 1257.
112 *R. c. Joyal* (1996), 43 C.R. (4th) 317 (C.A.Qc.).
113 *R. c. Krist* (1995), 100 C.C.C. (3d) 58 (C.A.C.-B.).
114 *R. c. Hutchings* (1996), 111 C.C.C. (3d) 215 (C.A.C.-B.). Dans *R. c. Solomon*, [1996] R.J.Q. 1789 [ci-après *Solomon*], appel rejeté par la Cour suprême, sans se prononcer sur la question, [1997] 3 R.C.S. 696, la Cour d'appel du Québec a déterminé qu'un abonné ne pouvait raisonnablement s'attendre que ses états de compte puissent bénéficier d'une quelconque expectative raisonnable de vie privée. À la p. 1794, la Cour, sous la plume du juge Gendreau, se base sur le fait qu'il s'agit de la détention par un tiers d'informations de nature non confidentielle ou biographique et qui ont été compilées dans un contexte commercial pour fins de facturation. La preuve retenue par la Cour pour arriver à cette conclusion repose sur le fait que les relevés ne donnent que l'identification de l'abonné inscrit, les numéros de téléphone joints et le nombre d'appel

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

sur lequel l'utilisateur n'a pas de contrôle et à l'égard de conversations tenues en public[115], sur le numéro civique d'une maison d'habitation[116], sur les renseignements obtenus par une action étatique étrangère suite à une demande d'entraide juridique par le Canada, concernant des comptes bancaires situés dans cet État étranger[117], sur les odeurs de marijuana émanant de l'appartement d'un individu lorsque la police se trouve dans un couloir qui ne lui appartenait pas exclusivement[118], à l'égard des empreintes digitales[119], lorsqu'on a renoncé à la protection offerte par la *Charte canadienne*[120], dans le cas de l'enregistrement de sessions de navigation dans le contexte d'une communication effectuée à un babillard électronique de nature commerciale et publique[121], non plus qu'à l'égard du contenu d'un ordinateur se trouvant sur les lieux du travail, faisant partie d'un réseau et faisant l'objet d'une directive patronale d'utilisation pour les fins du travail seulement[122].

---

effectués dans une période données par celui-ci. Les relevés ne révèlent pas l'identité de la personne jointe ou qu'on a tenté de joindre et l'identité de la personne qui a initié l'appel à partir de l'appareil d'origine visé par le relevé. Même si la Cour conclue qu'il n'y a pas d'expectative raisonnable de vie privée à l'égard de ces informations, elle conclue tout de même que les compagnies de téléphone compilent généralement des information de nature plus privée que celles relatives à la distribution d'électricité compilées par les compagnies d'électricité, comme c'était le cas dans l'arrêt *Plant, supra* note 34. Bien qu'il soit d'accord avec les conclusions du juge Gendreau quant à l'issu du pourvoi, le juge Beaudoin semble par contre attribuer un caractère privé plus élevé aux états de compte compilés par les compagnies de téléphone lorsqu'ils révèlent la liste complète des numéros de téléphone qu'un individu a appelés. Voir *Solomon*, *supra* note 114 à la p. 1799. Quelques mois plus tard, la Cour d'appel récidive sur le sujet dans *R. c. Robillard*, [1996] R.J.Q. 2886 (permission d'en appeler à la Cour suprême refusée [ci-après *Robillard*]. [1997] 2 R.C.S. vii, sous *R. c. Capobianco*. Le juge Beauregard, pour la majorité, adopte une position en accord avec celle du juge Beaudoin. En effet la page 2894 du jugement il affirme : « *Je pense que l'affaire R. c. Edwards touche au droit d'un abonné du téléphone de contester la perquisition de ces factures téléphoniques dans les dossiers de téléphone. Depuis la décision Télécom C.R.T.C. 86-7 du 25 septembre 1986, les abonnés peuvent raisonnablement s'attendre à ce que les factures ne soient pas communiquées à des étrangers. Je vois une différence entre une information concernant la quantité d'électricité consommée par un usager et l'identité des interlocuteurs d'un abonné* ». (notes omises) La distinction entre les informations révélées sur les individus et leurs numéros de téléphone ne s'applique donc plus. L'article 492.2 du *Code criminel*, qui permet l'obtention de copies du registre d'appel d'une personne ou d'un organisme qui le possède légalement afin de connaître les numéros composés ou reçus à partir d'un téléphone ou d'une ligne téléphonique, règle cette question en rendant obligatoire l'obtention d'une autorisation judiciaire pour ce faire. Le législateur présume par contre que l'expectative raisonnable de vie privée à l'égard des registres est moindre, étant donné la norme « réduite » des motifs raisonnables de soupçonner, nécessaire à l'obtention de l'autorisation judiciaire.

115 *R. c. Lubovac* (1989), 52 C.C.C. (3d) 551 (C.A. Alta.), requête en autorisation de pourvoi rejetée 53 C.C.C. (3d) vii [ci-après *Lubovac*].

116 *R. c. Neill* (1993), 54 W.A.C. 118 (C.A. C.-B.).

117 *Schreiber, supra* note 17 aux pp. 859-62.

118 *R. v. Laurin* (1997), 113 C.C.C. (3d) 519 (Ont. C.A.)

119 *R. c. Beare,* [1988] 2 R.C.S. 387, *R c. Bourque,* (1995) 103 C.C.C. (3d) 559 (C.A. Qc.). L'expectative raisonnable de vie privée pourrait par contre être plus élevée si les empreintes digitales sont obtenues dans le cadre d'une arrestation illégale. Voir *Feeney, supra* note 20 au para. 60.

120 *R. c. Clarkson*, [1986] 1 R.C.S. 383, *R. c. Bartle*, [1994] 3 R.C.S. 173 et *R. c. Borden*, [1994] 3 R.C.S. 145 [ci-après Borden]. Pour les fins de la présente étude, ce sera à la partie qui invoque la renonciation, généralement le ministère public, à établir selon la balance des probabilités que l'accusé a bel et bien renoncé à la protection offerte par l'article 8 de *Charte canadienne*.

121 *R. c. Morin* [1996] R.J.Q. 1758-1764 (C.Q.) [ci après *Morin*]. Nous reviendrons plus en détail sur cette décision, compte tenu de son application dans le contexte de l'utilisation d'Internet, notamment du *Web*.

122 *R. c. Tremblay* (29 mars 2001), Trois-Rivières 410-01-019056-001 [ci-après *Tremblay*], (C.Q.), pourvoi de plein droit à la C.A. Qc. (29 juin 2001). Nous reviendrons plus en détail sur cette décision, dans les sections traitant du branchement à Internet par rapport au lieu de l'établissement de la connexion et dans la section traitant du contexte particulier des communications effectuées par le biais du courriel. Nous référerons aux numéros de page de la transcription officielle du jugement oral.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

Section II - Exemples de cas où l'expectative raisonnable de vie privée a été reconnue

Par contre, selon la jurisprudence, une expectative raisonnable de vie privée a été reconnue dans un domicile[123], y compris eu égard à une fouille périphérique[124] et à une fouille olfactive[125] de celui-ci, elle a été également reconnue dans un bureau privé[126], sur les fluides corporels d'un individu, même s'ils ont été prélevés pour des fins médicales[127], sur toutes substances corporelles ou empreintes corporelles, comme le sang, la salive, les poils, les empreintes buccales[128], à l'égard de l'intégrité physique[129], sur un papier mouchoir jeté dans une poubelle alors que l'individu qui en dispose est détenu[130], à l'égard de documents bancaires d'un individu révélant des informations biographiques d'ordre personnel[131], sur les communications d'un individu lorsqu'il prend les dispositions nécessaires pour ne pas être entendu par des tiers[132], lors d'une surveillance vidéo dans une chambre d'hôtel ou de motel[133], sur la personne d'un élève fouillé par le directeur adjoint d'une école secondaire alors que l'élève se trouve à l'école[134], à l'égard du contenu des fichiers se trouvant dans un ordinateur, dans la mesure où celui-ci se trouvait au domicile de la personne visée par l'immixtion, dont ceux relatifs aux courriels et aux groupes de discussion ou nouvelles *Usenet*[135] et à l'égard du contenu des courriels se trouvant dans l'ordinateur d'un fournisseur de service Internet ou fsI, dans la mesure où il existe une relation empreinte de confidentialité avec celui-ci[136].

Section III - Exemples de cas où l'expectative raisonnable de vie privée est réduite

---

123 Sous réserve de l'arrêt *Edwards*, *supra* note 15 il existera, en principe, une expectative raisonnable de vie privée élevée eu égard au domicile. Voir *Hunter, supra* note 15 *Baron c. Canada*, [1993] 1 R.C.S. 416, *Silveira*, *supra* note 20 et *Feeney, supra* note 20.

124 *Kokesch*, *supra* note 57 ; *R. c. Grant*, [1993] 3 R.C.S. 223 [ci-après *Grant*].

125 *Evans*, *supra* note 59.

126 *Grant*, *supra* note 124 à la p. 242.

127 *Dyment*, *supra* note 38 aux pp. 431-32.

128 *Stillman*, *supra* note 110 aux pp. 641-43.

129 *R. c. Pohoretsky*, [1987] 1 R.C.S. 945 ; *Dyment*, *supra* note 38 ; *R. c. Greffe,* [1990] 1 R.C.S. 755 [ci-après *Greffe*] ; *R. c. Dersch*, [1993] 3 R.C.S. 768 ; *R. c. Erickson*, [1993] 2 R.C.S. 649 ; *Colarusso*, *supra* note 100 ; *Borden*, *supra* note 120.

130 *Stillman*, *supra* note 110 aux pp. 647-48.

131 *Schreiber, supra* note 17 et *Plant*, *supra* note 34. Voir également *a contrario* : *R. c. Lillico* (1994), 92 C.C.C. (3d) 90, 95 (C.Ont. Div.Gén.).

132 Articles 183 et 184 du *Code criminel* et *Duarte*, *supra* note 51 qui assimile en quelque sorte communication privée et communication bénéficiant d'une expectative raisonnable de vie privée. Voir également *a contrario Lubovac, supra* note 115.

133 *Wong*, *supra* note 53 à la p.50.

134 *M.R., supra* note 48.

135 *R. c. Gauthier*, REJB 99-14108 (C.Q.) [ci-après *Gauthier*]. Nous traiterons plus en détail de cette décision dans la section traitant des contextes particuliers de communication apportés par Internet et les nouvelles TI, plus particulièrement dans la section relative au branchement à Internet à partir du domicile.

136 *R. c. Weir* [1998] A.J. No 155, conf. en partie par 2001 ABCA 181. Nous traiterons plus en détail de cette décision dans la section traitant des contextes particuliers de communication apportés par Internet et les nouvelles TI, plus particulièrement dans la section relative au courriel. Un fsI ou fournisseur de service Internet, est une entreprise qui vend des accès à Internet. On dit aussi fournisseur d'accès Internet. Voir aussi M. Hayden, *Les réseaux*, Paris, Campus Press France, 1999 à la p. 254 [ci après *Les réseaux*]. Les accès seront offerts sous forme d'abonnements de types différents à des particuliers ou des entreprises. Voir D.J. Sohier, *Le guide de l'internaute 2000,* Montréal, Les éditions logiques, 2000 à la p.71 [ci-après *Le guide de l'internaute 2000*].

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

Finalement, la jurisprudence conclut à l'existence d'une expectative raisonnable de vie privée réduite, auquel cas l'article 8 de la *Charte canadienne* s'applique, mais pas dans toute sa vigueur. Ceci signifie, notamment, que la norme légale d'émission d'une autorisation peut se voir réduite. Les tribunaux ont donc déterminé que les déplacements d'un véhicule automobile[137], les dossiers commerciaux conservés dans le cadre d'un régime administratif de régulation[138], la personne se présentant à la frontière pour avoir accès au Canada[139], les registres téléphoniques d'un abonné comportant la facturation et les listes d'appels provenant de l'externe et étant destinés à l'externe[140], les élèves se trouvant à l'école ou participant à une activité scolaire[141], les médias[142], les personnes se trouvant dans un établissement de détention[143], « bénéficient » d'une protection réduite.

L'expectative raisonnable de vie privée varie donc selon le contexte, d'où l'importance de bien qualifier la situation factuelle de chaque cas d'espèce. C'est ce qu'on pourrait appeler de façon plus générale une composante de l'analyse contextuelle de la *Charte canadienne*.

La protection de l'article 8 de la *Charte canadienne* sera complète, diminuée ou inexistante selon le niveau d'expectative raisonnable de vie privée établi par la personne qui veut en bénéficier. La *Charte canadienne* ne protège personne contre les immixtions étatiques dans l'abstrait[144]. Nous le rappelons, la personne voulant bénéficier de la protection accordée par l'article 8 de la *Charte canadienne*, devra établir les paramètres qu'elle voudra voir être considérés lors de la détermination de l'application de la protection.

Nous venons de traiter de ce que l'on pourrait qualifier de protection « préalable» à l'immixtion accordée par l'article 8 de *la Charte canadienne*. Il existe par ailleurs une protection « *post* immixtion » qui découle de l'article 8 de la *Charte canadienne* et de la mécanique de l'application de celui-ci. Il convient donc maintenant d'en traiter.

Chapitre V - La protection « *post* immixtion » de la vie privée

La base de la présente étude est de déterminer s'il existe ou non une expectative raisonnable de vie privée eu égard aux divers contextes de communication offerts par Internet et les nouvelles TI. Comme nous l'avons vu, s'il existe une expectative raisonnable de vie privée à l'égard d'un contexte donné, cela aura pour effet d'obliger les représentants de l'État d'obtenir une autorisation judiciaire quelconque. C'est de cette manière que la vie privée d'un

---

137 *Wise*, *supra* note 46 aux pp. 533-34.

138 *Potash*, *supra* note 55 à la p. 416.

139 *R. c. Simmons*, [1988] 2 R.C.S. 495, 525 [ci-après *Simmons*]. Selon le contexte de la fouille, l'expectative raisonnable de vie privée à la frontière peut même être inexistante. Il suffit de retenir que, dans l'ensemble, l'expectative raisonnable de vie privée y est moindre. De plus, lorsque l'immixtion étatique ne porte pas atteinte à l'intégrité corporelle d'un individu ou ne fait pas en sorte que l'on obtienne de l'information qui provient de ses substances corporelles, l'atteinte à l'expectative raisonnable de vie privée sera également moindre. Voir *R. c. Monney,* [1999] 1 R.C.S. 652.

140 Article 492.2 du *Code criminel* et *Robillard*, *supra* note 114.

141 *M.R., supra* note 48 à la p. 421.

142 *Société Radio-Canada c. Lessard*, [1991] 3 R.C.S. 421.

143 *Weatherall c. Procureur Général du Canada*, [1993] 2 R.C.S. 872. Voir également *Gagnon c. Deslauriers* (1997), 141 F.T.R. 163 (C.F. (1ere inst.)), qui affirme que les visiteurs d'une institution carcérale ont également une expectative raisonnable de vie privée réduite sur les lieux de l'institution.

144 *Schreiber, supra* note 17 à la p. 860.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

individu est protégée : l'État doit obtenir une autorisation judiciaire avant de pouvoir s'immiscer dans une quelconque attente raisonnable en matière de vie privée.

On pourrait penser que l'obtention d'une autorisation judiciaire est suffisante pour qu'un représentant de l'État puisse agir légalement. Or, même lorsque l'État obtient une telle autorisation, il faut se demander si l'immixtion étatique n'est pas abusive et si la loi le permettant n'est pas elle-même abusive[145]. Lorsque l'appareil étatique effectue une fouille, perquisition ou saisie (c.-à-d. par une activité mettant en échec ou déjouant une quelconque expectative raisonnable de respect de la vie privée), il devient donc nécessaire d'en déterminer le caractère non abusif[146]. C'est ce que nous appelons la protection « *post* immixtion », découlant de l'article 8 de la *Charte canadienne*.

Une perquisition, fouille ou saisie ne sera pas abusive si elle est autorisée par la loi, si la loi elle-même n'a rien d'abusif et si son exécution n'est pas abusive[147]. Le fardeau d'établir le caractère abusif (ou son caractère déraisonnable), reposera sur les épaules de la personne voulant bénéficier de la protection[148].

Il s'agit donc en quelque sorte d'une protection de la vie privée résiduaire dont un individu peut se servir contre les immixtions injustifiées des représentants de l'État, même dans les cas où ceux-ci possédaient une autorisation judiciaire préalable. C'est pour cette raison que nous avons jugé approprié de traiter du sujet, même s'il peut dépasser le cadre de la présente étude. Par contre, nous ne traiterons pas des autres aspects de la procédure reliés aux critères de constitutionnalité. Nous traiterons donc du concept d'autorisation par la loi, du caractère non abusif ou raisonnable de l'autorisation légale et du caractère non abusif de l'immixtion dans une expectative raisonnable de vie privée.

Section I - L'autorisation par la loi

Pour être autorisée par la loi, une fouille, perquisition ou saisie doit être permise par une disposition législative spécifique ou par un principe de *common law*. Dans tous les autres cas, la fouille, perquisition ou saisie, n'est pas autorisée par la loi et devient abusive à sa face même et, par conséquent, viole l'article 8 de la *Charte canadienne*[149].

L'article 8 de la *Charte canadienne* n'est pas attributif de pouvoirs de fouille ou perquisition[150]. Ainsi, la seule existence de motifs raisonnables de croire qu'un lieu contient des renseignements ou même des éléments de preuve, n'autorise pas en soi une fouille, saisie ou perquisition. En principe, une activité étatique entraînant une immixtion dans la vie privée d'un individu devra être autorisée légalement, sinon elle sera présumée abusive.

Section II - Le caractère non abusif ou raisonnable de l'autorisation légale

---

145 *Collins*, *supra* note 18.
146 *Edwards*, *supra* note 15 à la p. 145.
147 *Collins*, *supra* note 18 à la p. 278.
148 Voir de façon générale *Collins*, *supra* note 18.
149 *Thompson*, *supra* note 51 à la p. 1153. Par contre, voir *M.R., supra* note 48 aux pp. 420, 422-23, où il a été décidé que lorsqu'un responsable d'école procède à une fouille ou à une saisie sur un élève, aucun mandat n'est requis. L'absence de mandat dans ces circonstances n'entraîne pas une présomption de fouille abusive.
150 *Hunter, supra* note 15 aux pp. 145, 157.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

Généralement, une loi permettant une immixtion sera jugée raisonnable si elle prévoit un mécanisme d'autorisation préalable, habituellement pour l'émission d'un mandat de perquisition[151] ou autre autorisation semblable. Le mécanisme doit consister en un tiers impartial agissant de façon judiciaire (généralement un juge). Le juge se fonde sur l'existence de motifs raisonnables de croire, établis généralement sous serment, à la commission d'une infraction avant d'émettre un mandat[152].

Cependant, certaines formes de fouille et perquisition sans mandat sont autorisées pourvu qu'elles se fondent sur une disposition législative ou sur le *common law*. Ces exceptions découlent généralement de la nécessité d'agir rapidement dans certaines catégories de situations[153], pour être en mesure de s'acquitter des responsabilités que la loi impose[154]. Nous ne traiterons pas davantage de cette question dans la présente étude.

Section III - La détermination du caractère non abusif de l'immixtion dans une expectative raisonnable de vie privée

Ce critère d'analyse a surtout été développé dans le contexte des fouilles, saisies ou perquisitions impliquant des individus, comme par exemple en matière de fouilles à nu, ou de fouilles dans les cavités corporelles[155]. Il a aussi été développé dans le contexte où des policiers munis d'un mandat, ont utilisé des moyens disproportionnés pour pénétrer sans avertissement à l'intérieur du domicile de l'accusé[156].

Cette question pourrait être d'importance dans le contexte d'une surveillance effectuée par le biais d'Internet et les nouvelles TI. C'est le cas d'une surveillance électronique qui, bien que fondée sur une autorisation légalement obtenue, est effectuée d'une manière déraisonnable. Par exemple, dans le contexte d'une communication effectuée à partir d'une cabine téléphonique, une minimisation de l'immixtion étatique est généralement requise[157]. Une certaine minimisation pourrait aussi être requise lors de l'interception de communications provenant d'un ordinateur situé dans un cybercafé[158] ou sur les lieux du travail où plusieurs utilisateurs ont accès au poste de travail ou réseau ciblé.

Les critères d'analyse liés à l'aspect déraisonnable des immixtions étatiques pourraient donc trouver application dans les environnements électroniques, dans l'évaluation de l'ampleur ou du degré d'immixtion de la technologie utilisée pour surveiller un individu ou ses communications

---

151 Voir par exemple l'article 487 du *Code criminel.*

152 *Hunter, supra* note 15 aux pp. 145, 160-68. Par contre dans certains cas les critères pour l'obtention d'une telle autorisation pourront être moindres, tels que l'exigence de motifs raisonnables de soupçonner au lieu des motifs raisonnables de croire. Voir à titre d'exemple l'article 492.2 du *Code criminel* traitant de l'obtention d'une autorisation pour enregistrer des numéros de téléphone.

153 *Grant*, *supra* note 124 aux pp. 240-43.

154 *M.R., supra* note 48 à la p. 423, où il a été déterminé qu'une loi et un règlement autorisaient, par « déduction nécessaire », les fouilles d'élèves.

155 *Greffe, supra* note 129 à la p. 795, où la Cour cite un passage de l'arrêt *Simmons, supra* note 139 à la p. 517 : « Il est évident que plus l'immixtion sur la vie privée est importante, plus sa justification et le degré de protection constitutionnelle accordés doivent être importants. »

156 *R. c. Genest,* [1989] 1 R.C.S. 59

157 *Thompson, supra* note 51aux pp. 1142, 1146.

158 Un cybercafé est défini comme étant un établissement commercial permettant aux clients de se restaurer tout en ayant accès à un ordinateur connecté à Internet. Office de la langue française, 2001, *s.v.* « cybercafé », en ligne : <http://www.olf.gouv.qc.ca/ressources/internet/fiches/2075030.htm> (date d'accès : 21 février 2001).

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

effectuées par le biais d'Internet et des nouvelles TI. Ce sera l'addition des différentes méthodes employées qui pourra faire en sorte que la surveillance ou l'immixtion étatique devient abusive.

Nous venons de traiter de la protection constitutionnelle accordée par la *Charte Canadienne* en matière de vie priée. Il convient maintenant de traiter de la protection statutaire de la vie privée en matière de communication et de correspondance. Il s'agit de la protection offerte principalement par le *Code criminel* à l'égard des « communications privées » et de la protection statutaire de la correspondance.

Chapitre VI - La protection statutaire de la vie privée en matière de « communication privée » et de correspondance

La vie privée est protégée en partie par le *Code criminel*. Cette protection découle du fait que le *Code criminel* interdit l'interception des « communications privées », sauf certaines exceptions[159]. On protège donc indirectement la vie privée des individus en interdisant à quiconque d'intercepter une communication privée. Nous n'entrerons pas dans le détail des diverses exceptions prévues à l'article 184 du *Code criminel*. Il suffit, pour les fins de la présente étude, de s'attarder à l'exception concernant le droit des organismes d'application de la loi d'obtenir une autorisation d'interception[160] et à l'exception concernant les personnes fournissant les services téléphoniques[161].

Nous avons déjà traité partiellement du premier cas d'exception. En effet, la *Charte canadienne* oblige les agents de l'État à obtenir une autorisation judiciaire avant de pouvoir s'immiscer dans une quelconque expectative raisonnable de vie privée. C'est ce que la partie VI du *Code criminel* prévoit[162]. Quant à l'exception concernant les personnes fournissant les services téléphoniques, nous en traiterons indirectement lorsque nous traiterons du rôle et des fonctions de l'administrateur de réseau ou fsI.

Les organismes d'application de la loi seront donc « empêchés » d'intercepter une communication privée à moins d'obtenir au préalable une autorisation en vertu du *Code criminel*. Quant aux fournisseurs de services téléphoniques, ils seront empêchés d'intercepter une communication privée, sauf s'ils se « qualifient » dans une des exceptions prévues au *Code criminel*.

Conséquemment nous traiterons dans un premier temps de la définition de « communication privée » qui est à la base de la protection accordée par le *Code criminel*. Nous traiterons ensuite de la distinction entre une communication bénéficiant d'une expectative raisonnable de vie privée et une « communication privée », et de la notion d'interception. Nous traiterons finalement de la protection accordée à la correspondance, étant donné sa nette ressemblance avec le courriel, dont nous traiterons plus loin en détail.

Section I - Les définitions à la base de la protection accordée par le *Code criminel*

[159] Voir à cet effet l'infraction prévue au paragraphe 184(1) du *Code criminel*. Les exceptions étant prévues au paragraphe 184(2).
[160] Voir plus spécifiquement le sous paragraphe 184(2)a) du *Code criminel*.
[161] Voir plus spécifiquement le sous paragraphe 184(2)c) du *Code criminel*.
[162] *Duarte*, *supra* note 51 ; *Michaud c. Québec (Procureur Général)*, [1996] 3 R.C.S. 3.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

Le *Code criminel* à sa partie VI, prévoit plusieurs définitions visant la protection offerte en matière de vie privée. Il s'agit en fait d'une protection indirecte de la vie privée, en ce sens qu'on y crée une infraction à l'égard de quiconque, au moyen d'un dispositif électromagnétique, acoustique, mécanique ou autre, intercepte volontairement une communication privée[163]. Pour mieux comprendre la portée de la protection offerte, il est nécessaire de bien saisir les concepts prévus aux définitions des notions de « communication privée », « communication radiotéléphonique », « dispositif électromagnétique, acoustique, mécanique ou autre » et « intercepter » qui sont définies à l'article 183 du *Code criminel* :

> « […] *« 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.*
>
> *« communication radiotéléphonique » S'entend de la radiocommunication, au sens de la Loi sur la radiocommunication, faite au moyen d'un appareil servant principalement à brancher la communication à un réseau téléphonique public commuté.*
>
> *«dispositif électromagnétique, acoustique, mécanique ou autre» Tout dispositif ou appareil utilisé ou pouvant être utilisé pour intercepter une communication privée. La présente définition exclut un appareil de correction auditive utilisé pour améliorer, sans dépasser la normale, l'audition de l'utilisateur lorsqu'elle est inférieure à la normale.*
>
> *[…] «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.*
>
> *« réseau téléphonique public commuté » Installation de télécommunication qui vise principalement à fournir au public un service téléphonique par lignes terrestres moyennant contrepartie*. »

Un autre concept dont on doit tenir compte dans la mécanique du *Code criminel* en matière de protection des communications privées, est la notion du terme « télécommunication » prévue à l'article 35 de la Loi d'interprétation :

> « *« télécommunication » La transmission, l'émission ou la réception de signes, signaux, écrits, images, sons ou renseignements de toute nature soit par*

[163] Paragraphe 184(1) du *Code criminel*. Certaines exceptions son prévues au paragraphe 184(2) du *Code criminel*, notamment une à l'égard d'une personne qui intercepte une communication privée en conformité avec une autorisation judiciaire à l'alinéa 184(2)b) du *Code criminel* et l'autre, à l'égard d'une personne qui fournit au public un service de communications téléphoniques, télégraphiques ou autres et qui intercepte une communication privée dans certaines circonstances. Cette exception est prévue à l'alinéa 184(2)c) du *Code criminel*.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

système électromagnétique, notamment par fil, câble ou système radio ou optique, soit par tout procédé technique semblable »[164].

C'est donc par ce jeu de définitions, que les communications privées sont protégées par le *Code criminel*. Le concept le plus important qui ressort de ces définitions, est celui d'expectative raisonnable de non-interception : « […] dans des circonstances telles que son auteur peut raisonnablement s'attendre à ce qu'elle ne soit pas interceptée par un tiers […] ». Bien que la mécanique de la protection offerte par le *Code criminel* diffère de celle accordée par la *Charte canadienne*, le concept d'attente raisonnable de non interception se rapproche, du moins dans sa formulation, du concept d'expectative raisonnable de vie privée traité précédemment en matière de protection accordée par la *Charte canadienne*[165]. Il convient donc de préciser la nature des deux concepts.

Section II - La distinction entre une « communication privée » et une communication bénéficiant d'une expectative raisonnable de vie privée est-elle académique?

L'interception d'une communication faite en privé constitue une immixtion de l'État sur une expectative raisonnable de vie privée[166]. Du point de vue de la protection constitutionnelle offerte par la *Charte canadienne* à l'article 8, il faudra donc, en principe, obtenir une autorisation judiciaire préalable avant de ce faire. À cet effet, le *Code criminel* prévoit à sa partie VI les exigences à respecter afin de pouvoir procéder légalement à l'interception d'une « communication privée ».

Dans *Duarte*[167], la Cour Suprême du Canada, par la plume du juge La Forest, a assimilé la détermination de ce qui constitue une « communication privée » à une communication bénéficiant d'une expectative raisonnable de vie privée. Une « communication privée » serait donc toujours une communication bénéficiant d'une expectative raisonnable de vie privée. Une communication bénéficiant d'une expectative raisonnable de vie privée constituerait par ailleurs une notion plus large qui engloberait la notion de « communication privée ».

Toujours dans *Duarte*, la Cour a déterminé qu'un enregistrement subreptice d'une conversation entre individus, faite en présence l'un de l'autre, par un agent de l'État, constituait une communication bénéficiant d'une expectative raisonnable de vie privée, même s'il ne s'agissait pas d'une « communication privée » au sens du *Code criminel*[168]. Le fait que

---

[164] Loi d'interprétation, L.R.C. 1985, c. I-21, art. 35.

[165] La jurisprudence traditionnelle traitant de la détermination de ce qui constitue une « communication privée », applique un critère évalué objectivement par la cour, soit celui de l'expectative raisonnable de non interception par un tiers. Une communication sera donc considérée « privée » au sens du *Code criminel,* seulement si elle est effectuée dans des circonstances telles que son auteur peut raisonnablement s'attendre à ce qu'elle ne soit pas interceptée par un tiers. Voir notamment : *R. v. Carothers,* [1978] 6 W.W.R. 571 (Co.Ct. C.-B.), *R. v. Goldman,* [1980] 1 R.C.S. 976, à la p. 994, *R. v. Rodney* (1984), 12 C.C.C. (3d) 195, à la p. 198 et *R. v. Richer* (1993), 82 C.C.C. (3d) 385, à la p. 408, où la question de l'attente subjective de l'auteur de la communication est soulevée, sans toutefois y répondre. On semble par ailleurs y appliquer implicitement une norme subjective. Confirmé par la Cour suprême du Canada à (1994), 90 C.C.C. (3d) 95.

[166] Voir généralement *Duarte*, *supra* note 51.

[167] *Duarte*, *Ibid*. aux pp. 42-43.

[168] Dans *Solomon*, *supra* note 114, confirmé par la Cour suprême sans référence à cette question spécifique à : [1997] 3 R.C.S. 696, la Cour d'appel du Québec a adopté cette approche pour déterminer si une communication effectuée par téléphone cellulaire analogique était une communication bénéficiant d'une expectative raisonnable de vie privée au sens de la *Charte canadienne.* En effet le juge Gendreau a utilisé le test de l'expectative raisonnable de vie privée élaboré dans les arrêts de la Cour suprême rendus dans *Wong*

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

la communication ait été enregistrée de façon permanente par un agent de l'État, dans des circonstances où l'on pouvait raisonnablement s'attendre à ce qu'elle soit confidentielle, semble avoir été le point déterminant pour en arriver à cette conclusion.

L'utilisation du concept de « communication privée » perd donc de son utilité lorsque vient le temps de déterminer s'il s'agit d'une communication devant bénéficier d'une protection contre les immixtions injustifiées de l'État. Le vrai test est celui de déterminer s'il s'agit d'une communication bénéficiant d'une expectative raisonnable de vie privée au sens de l'article 8 de la *Charte canadienne*. Dans la mesure où le concept de communication bénéficiant d'une expectative raisonnable de vie privée est plus large, le concept de « communication privée » devient obsolète pour les fins de la protection contre les immixtions de l'État.

À toute fin pratique, le concept de « communication privée » ne reste utile que pour établir un des éléments essentiels de l'infraction relative à une « communication privée »[169]. Ceci nous amène donc à traiter de la notion « d'interception ».

Section III - L'interception d'une « communication privée »

Tel que mentionné plus haut, l'article 183 du Code *criminel* définit le terme « intercepter » :

> « […] *« 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* »[170].

Cette définition est très large. En effet, elle comprend le concept de la « prise de connaissance » d'une communication.[171] Ce concept s'écarte de la définition traditionnelle

---

et *Duarte* pour conclure qu'il s'agissait effectivement d'une « communication privée », dans le sens de « communication bénéficiant d'une expectative raisonnable de vie privée », et ce, même si en première instance il avait été décidé qu'une communication effectuée par le biais d'un téléphone cellulaire, n'était pas une « communication privée » au sens du *Code criminel*. Cette décision de première instance n'était pas contestée devant la Cour d'appel, qui en a pris acte. Pour la décision de première instance relative à la qualification de ce qui constitue un communication privée, voir *R. c. Solomon* [1992] R.J.Q. 2631 (C.M. Mtl.). La Cour d'appel dans *Solomon*, par la plume du juge Gendreau, fait une distinction entre le fait que les ondes pouvaient assez facilement être interceptées par le public, ce qui ne constituait pas une infraction (absence d'expectative raisonnable de non interception de l'accusé à cet égard), par rapport au fait que des agents de l'État pouvaient les intercepter (expectative raisonnable de vie privée de l'accusé à cet égard). L'identité de la personne qui procède à l'interception (donc à l'immixtion) est donc déterminante. Voir également la décision *R. v. Cheung and Tam* (1995), 100 C.C.C. (3d) 441 (C.S. C.-B.) [ci-après *Cheung*], à la p. 447, où l'on assimile le test élaboré dans *Wong* pour la détermination en vertu de la *Charte canadienne* de ce qui constitue une expectative raisonnable de vie privée, et le test objectif de la détermination de ce qui constitue une « communication privée » bénéficiant d'une expectative raisonnable de non interception au sens du *Code criminel*.

[169] L'article 184 du *Code criminel* prévoit notamment qu'il est interdit, sauf certaines exceptions, d'intercepter volontairement une « *communication privée* », au moyen d'un dispositif électromagnétique, acoustique, mécanique ou autre.

[170] Il est intéressant de noter que la même définition du terme « intercepter » se retrouve au paragraphe 342.1(2) du *Code criminel*, l'infraction d'intercepter illégalement la fonction d'un ordinateur se trouvant à l'alinéa 342.1 (1)b) du *Code criminel.* Ceci tend une fois de plus à confirmer que la notion d'interception ne sert plus qu'à déterminer si une infraction est commise à l'égard d'une communication quelconque.

[171] Le terme « *communication* » doit être interprété ici dans le sens suggéré par la Partie VI. En effet les définitions apparaissant au début de la Partie VI ne s'appliquent qu'à cette partie. Le terme

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

voulant qu'un tiers soit présent sur la ligne au même moment où deux personnes sont en communication[172]. La distinction entre le fait « d'interférer » avec une communication et le fait de « prendre connaissance » d'une communication est inexistante dans cette définition. Nous sommes d'avis que le concept de prise de connaissance est plus large que le concept d'interférence. La question de savoir si l'immixtion étatique constitue une « interception » est d'intérêt, car si c'est le cas, il faudra procéder en vertu de la partie VI pour procéder à l'obtention des communications. Si l'immixtion n'est pas considérée comme une « interception », il faudra trouver ailleurs que dans la partie VI, la justification législative pour l'obtention de la communication, notamment en vertu des dispositions des articles 487 ou 487.01 du *Code criminel*.

Section IV - L'interception d'une communication privée dans le contexte de l'obtention de courriels en attente de livraison en droit américain

Le droit américain a été confronté à cette question dans la décision *Steve Jackson Games, Inc. c. The United States Secret Services*.[173] Il fallait déterminer si la saisie d'un ordinateur dans lequel étaient stockés des courriels privés qui avaient été envoyés à un babillard électronique, mais qui n'avaient pas encore été lus par leurs destinataires, constituait une « interception » interdite par le *Title* I du *Electronic Communication Privacy Act.*[174]

L'article 2510 (4) du Title 18 U.S.C. définit le concept d'interception comme suit :

> «*...means the aural or other acquisitions of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device*»

« *communication* » n'a de sens que dans le contexte des définitions proposées par la Partie VI : une communication, dans la définition du terme « *intercepter* », sera donc soit une communication orale, une « *télécommunication*» ou une « *communication radiotéléphonique* ». Une « télécommunication » est par ailleurs définie à l'article 35 de la *Loi d'interprétation* L.R.C. (1985), c. I-21 : « *La transmission, l'émission ou la réception de signes, de signaux, écrits, images, sons ou renseignements de toute nature que ce soit par système électromagnétique, notamment par câble ou système radio ou optique, soit par tout procédé technique semblable* ». Nous soumettons que cette définition est assez large du point de vue technique pour comprendre une communication effectuée par le biais d'Internet.

[172] La jurisprudence traditionnelle définit l'interception en référant au concept « d'interférence» entre la place d'origine et la place de destination de la communication : *Re Copeland and Adamson et al*. [1972] 3 O.R. 248 (Ont. H.C.) et *R v. Mc Queen* (1975), 25 C.C.C. (2d) 262 (Alta. C.A.). La décision *Re Copeland and Adamson et al*., a été rendue avant l'entrée en vigueur de la partie IV.1 (aujourd'hui la partie VI). On ne pouvait donc bénéficier de la définition de « *communication privée* » prévue à la loi depuis 1974. Quant à la décision *R v. Mc Queen*, elle a été rendue dans le contexte où un policier avait pris les appels destinés à la personne chez qui on exécutait un mandat de perquisition. Une décision semblable a été rendue dans *R. v. Singh* (1998), 127 C.C.C. (3d) 429, où une policière jouait le rôle de l'amie de l'accusé lors d'une conversation téléphonique avec M. Singh. Dans ces deux cas, aucun appareil n'a été utilisé pour enregistrer de façon permanente les propos recueillis. Il n'y avait donc ni interception au sens traditionnel, ni immixtion dans une quelconque expectative raisonnable de vie privée au sens de *Duarte*.

[173] 36 F.3d 457 (5th Cir. 1994) (Ci-après : « *Steve Jackson Games Inc.* »).

[174] Pub. L. No. 99-508, 100 Stat. 1848 (codifié tel qu'amendé de façon dispersée à 18 U.S.C.) (Ci-après : « *ECPA*») Le *ECPA* est entré en vigueur pour amender le *Federal Antiwiretapping Statute*. (Voir 18 U.S.C. §§ 2510-2520 (1994)) Le *ECPA* inclut deux catégories principales de protection : Le Title I qui interdit l'interception de message « *en transit*» (Voir 18 U.S.C. §§ 1367, 2521, 3117, 3121-3127 (1994)) et le Title II qui interdit l'accès et la divulgation d'information « *stockée*» (Voir 18 U.S.C. §§ 2701-2711)

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

La Cour a déterminé qu'une telle saisie ne constituait pas une interception parce que les courriels n'étaient pas en transit, mais étaient plutôt stockés en attente de transmission. Il est à noter que le droit américain fait la différence entre une communication stockée[175] et une communication en transit.[176]

De plus, le droit américain fait la distinction entre « *wire communication* »[177] et « *electronic communication* »,[178] ce qui n'est pas le cas au Canada. L'interprétation plus stricte du concept d'interception qui émane de la décision rendue dans *Steve Jackson Games Inc.* est, à notre avis, le résultat de l'existence de la distinction législative entre les concepts de communication en transit et communication stockée, ce qui n'est pas le cas au Canada[179].

Les concepts jurisprudentiels développés par le droit américain sur la notion d'interception et la législation s'y rapportant doivent conséquemment être considérés avec prudence en droit canadien. Par contre, nous sommes d'avis qu'ils nous donnent de bonnes indications sur la méthode d'analyse à utiliser lorsqu'il sera question de déterminer la nature de l'autorisation pour la prise de connaissance du contenu d'une communication faite par le biais d'un ordinateur, notamment dans le cas d'un courriel. Nous sommes d'avis que si la situation dans *Steve Jackson Games Inc*. étaient survenue au Canada, l'obtention des courriels stockés suite à la saisie de l'ordinateur, alors que ces courriels n'étaient pas rendus à destination, aurait constitué une « interception » au sens de la partie VI du *Code criminel*. À notre avis, une autorisation en vertu de cette partie aurait été rendue nécessaire pour l'obtention des courriels.

Compte tenu de la similitude entre le courriel, que nous aborderons plus en détail dans la deuxième partie, et la correspondance ordinaire, nous traiterons maintenant brièvement de la protection accordée à celle-ci en droit canadien.

---

[175] L'article 2510 (17) du 18 U.S.C. décrit la notion d'« *electronic storage*» comme suit : « *...means - (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication; and (C) "aural transfer" means a transfer containing the human voice at any point between and including the point of origin and the point of reception.* »

[176] La distinction s'opère entre communication stockée et en transit par le jeu des définitions de « *electronic communication* », « *wire communication* » (voir plus bas) et « *electronic storage* ».

[177] L'article 2510(1) du 18 U.S.C. définit « *wire communication*» comme suit : « *means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce and such term includes any electronic storage of such communication* ».

[178] L'article 2510(12) du 18 U.S.C. définit « *electronic communication*» comme suit : « *means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include : (A) any wire or oral communication; (B) any communication made through a tone-only paging device; (C) any communication from a tracking device (as defined in section of this title); or (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds* ».

[179] La décision rendue dans *Steve Jackson Games Inc,.supra* note 173 a été confirmée par les décisions rendues dans *Wesley College c. Pitts*, 974 F. Supp. 375, 384-390 (D. Del. 1997) ; *U.S. c. Moriarty*, 962 F. Supp. 217, 221 (D. Mass. 1997) ; *Bohach c. City of Reno*, 932 F. Supp 1232, 1235-36 (D. Nev. 1996). D'autres cours d'État sont arrivées à la même conclusion dans l'interprétation du terme « intercepter » tel qu'utilisée au *ECPA* : *Davis c. Gracey*, 111 F. 3d 1472 (Cir., 1997) ; *United States c. Reyes,* 922 F. Supp. 818 (S.D.N.Y. 1996). *Restuccia c. Burk Technology Inc.*, 5 Mass. L. Reptr. No 31,712 (1996) ; *Shoars c. Epson America*, No S.W.C. 112749 (Cal. Super C.T. 1990).

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

Section V - La protection de la correspondance

À l'instar des communications privées, la loi accorde une certaine protection en matière de vie privée à la correspondance[180]. Cette protection vise le courrier en cours de transmission postale[181]. La *Loi sur la Société canadienne des postes* affirme que malgré toute autre loi ou règle de droit, mais sous réserve de ses autres dispositions ou de ses règlements, de la *Loi sur le Service canadien du renseignement de sécurité* et de la *Loi sur les douanes*, rien de ce qui est en cours de transmission postale n'est susceptible de revendication, saisie ou rétention[182]. Les exceptions permettant l'ouverture du courrier sont généralement rattachées à des questions relatives à la conformité et sécurité du contenu des envois[183], au dédouanement[184] et à des questions relatives à la sécurité nationale[185]. Dans le cas des pénitenciers, l'ouverture du courrier par des agents est autorisée pour des raisons de sécurité[186] ou lorsqu'on a des motifs raisonnables de croire d'une part, que la communication contient ou contiendra des éléments de preuve relatifs soit à un acte qui compromettrait la sécurité du pénitencier ou de quiconque, soit à une infraction criminelle ou à un plan en vue de commettre une infraction criminelle, et d'autre part, que l'interception des communications est la solution la moins restrictive dans les circonstances[187]. Outre ces protections statutaires, nous sommes d'avis que la correspondance d'un individu, de par sa nature, bénéficie d'une expectative raisonnable de vie privée[188].

---

[180] Voir notamment les paragraphes 2(2) et (3) et les articles 40 à 42 et 48 de la *Loi sur la société canadienne des postes*, L.R.C. (1985), c. C-10, l'article 346 du *Code criminel*, le paragraphe 21(3) de la *Loi sur le service canadien de sécurité*, L.R.C. (1985), c. C-23, les articles 99, 110 et 111 de la *Loi sur les douanes*, L.C. 1986, c. 1, et de l'article 96 de la *Loi sur le service correctionnel et la mise en liberté sous condition*, L.C. 1992, c. 20, en relation avec les articles 88 et 94 du *Règlement sur le système carcéral et la mise en liberté sous condition*, D.O.R.S./92-620.

[181] Outre le service de courriel PosteCS[MC] de postes Canada, en ligne : Postes Canada <http://www.canadapost.ca/business/offerings/postecs/can/default-f.asp> (date d'accès : 8 novembre 2001), nous sommes d'avis que les dispositions de la *Loi sur la Société canadienne des postes* ne s'appliquent pas à l'envoi des courriels en général.

[182] Paragraphe 40(3) de la *Loi sur la société canadienne des postes*, L.R.C. (1985), c. C-10.

[183] Notamment dans le cas de l'article 41 de la *Loi sur la société canadienne des postes*.

[184] Notamment dans le cas de l'article 42 de la *Loi sur la société canadienne des postes* et de l'article 99 de la *Loi sur les douanes*.

[185] Notamment dans le cas de l'ouverture d'un objet par le biais d'une autorisation décernée en vertu du paragraphe 21(3) de la *Loi sur le service canadien de renseignement de sécurité*.

[186] L'article 88 du *Règlement sur le système carcéral et la mise en liberté sous condition*, permet à un agent d'ouvrir le colis ou l'enveloppe, afin de s'assurer qu'il ou elle ne contient pas d'objet interdit. L'agent ne pourra par contre, sous réserve du paragraphe 94(1) du *Règlement sur le système carcéral et la mise en liberté sous condition*, lire le contenu le cas échéant.

[187] Article 94 du *Règlement sur le système carcéral et la mise en liberté sous condition*.

[188] Voir à titre d'exemple *Re Postes Canada. et Canada (P.G.)* (1995), 95 C.C.C. (3d) 568, où on a déterminé que l'exécution d'un mandat émis en vertu de l'article 487.01 du *Code criminel*, autorisant la photocopie de l'extérieur des enveloppes des envois livrés dans la boîte postale de la cible, était valide et n'enfreignait pas la *Loi sur la Société canadienne des postes*. Voir également *R. c. Desilva*, [2000] O.J. No. 5107, (Ont. Ct. of J.) où l'on a décidé que l'accusé ne possédait pas l'intérêt pour invoquer la protection de l'article 8 de la *Charte canadienne*. Dans cette affaire, l'accusé se servait de la boîte postale d'un tiers innocent, pour recevoir du courrier contenant des chèques ou montants d'argent, provenant des victimes d'une fraude. La cour a considéré que l'accusé commettait une intrusion injustifiée dans la boîte postale du tiers innocent, commettant en quelque sorte un *trespass*. Cet intrus pouvait conséquemment invoquer la protection de la *charte canadienne* à l'égard de la boîte postale. Par ailleurs, la Cour, considérant que le courrier était arrivé à destination, a déterminé que les protections offertes par la *Loi sur la Société canadienne des postes* ne trouvaient plus application.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

Nous venons de traiter des différentes protections accordées en droit canadien en matière de vie privée, tant pour les communications privées, ou bénéficiant d'une expectative raisonnable de vie privée, que pour la correspondance. Il s'agit en quelque sorte d'un constat de l'état du droit canadien en la matière relativement à une multitude de contextes factuels. Par contre, ces constats ont principalement été faits dans des contextes du « monde réel » ou des contextes qui ne faisaient que s'apparenter techniquement aux contextes de communication apportés par Internet et les nouvelles TI.

Afin de mieux anticiper comment le droit tel que constaté précédemment s'appliquera aux nouveaux contextes de communication apportés par Internet et les nouvelles TI, il convient maintenant d'en traiter plus spécifiquement.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>

Partie II – Identification et explication des contextes techniques apportés par les nouvelles TI et Internet

Afin de bien identifier et comprendre les nouveaux contexte de communication apportés par Internet et les nouvelles TI, nous traiterons dans cette partie des contextes techniques généraux apportés par l'utilisation de l'informatique, d'Internet et des nouvelles TI au chapitre 1, des contextes particuliers de communication apportés par Internet et les nouvelles TI au chapitre 2 et des technologies particulières ayant une influence sur le caractère privé des communications effectuées dans les divers contextes apportés par Internet et les nouvelles TI au chapitre 3.

Chapitre I - Les contextes techniques généraux apportés par l'utilisation de l'informatique, d'Internet et des nouvelles TI

Les contextes de communication particuliers apportés par Internet et les nouvelles TI, s'insèrent indubitablement dans un contexte technique plus général, qu'est celui des réseaux de communication informatique. Afin de mieux comprendre le fonctionnement des contextes particuliers de communication apportés par Internet et les nouvelles TI, nous traiterons dans le présent chapitre du contexte de l'évolution des technologies en matière de communication, du contexte de l'utilisation de l'informatique, d'Internet et des nouvelles TI, de la définition d'Internet tel qu'avancée par la Cour suprême des États-Unis, du contexte technique d'Internet, du contexte du branchement à Internet et du contexte territorial ou juridictionnel d'Internet et de la notion d'ubiquité.

Section I - Le contexte de l'évolution des technologies en matière de communication

C'est grâce à la perspective historique que nous pouvons mieux saisir les raisons ayant mené à l'adoption des lois portant sur la protection des communications privées. C'est ce que nous avons appelé : « rationalités ».

Une meilleure compréhension à ce niveau nous aidera donc à mieux cerner l'étape suivante de cette évolution car, en fait, le phénomène de l'évolution jurisprudentielle ou législative en matière de fouille, saisie ou perquisition, suite à l'apparition d'une nouvelle technologie, n'est pas nouveau[189]. C'est plutôt la technologie qui est nouvelle, soit l'émergence d'Internet et des nouvelles TI. La loi ou la jurisprudence devra donc s'adapter le plus possible à cette nouvelle réalité technologique qui affectera dorénavant les comportements de la société.

Depuis le début des temps la plupart des communications entre les êtres humains étaient effectuées face à face. Depuis quelques milliers d'années certaines communications ont été effectuées par écrit. L'écrit constituait par contre un substitut de piètre qualité. En effet, le courrier pouvait prendre des semaines, des mois, voire des années avant de se rendre à

[189] Par exemple en 1878, la Cour Suprême américaine dans la cause *Ex Parte Jackson, 96 US 727, p. 733*, a rendu un jugement affirmant que le courrier de première classe ne pouvait être ouvert par des agents du gouvernement sans avoir préalablement obtenu un mandat de perquisition à cet effet. Par contre, l'invention du télégraphe a entraîné deux nouvelles manières d'écouter de façon indiscrète : mettre la ligne sous écoute et lire les messages plus tard à partir de copies conservées par la compagnie de télégraphe. La décision dans *Jackson* avait donc une application limitée dans ce nouveau contexte technologique. Conséquemment, la nécessité d'étendre la protection contre les fouilles saisies et perquisitions aux communications d'une personne découlait, du moins en partie, des avancées technologiques en matière de surveillance électronique.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

destination pour les grandes distances. La possibilité qu'une lettre puisse être ouverte lors du parcours, la rendant ainsi moins privée qu'un murmure, ne constituait qu'une des limites inhérentes à ce moyen de communication.

Pour un peu plus des cent dernières années, les communications humaines ont été effectuées de plus en plus par voie électronique, plus particulièrement par le biais du téléphone. Ce type de télécommunication s'apparentait le plus à la communication face à face.

La deuxième guerre mondiale a contribué à faire augmenter de façon significative les communications radio. Par contre, la majorité des télécommunications entre les personnes ordinaires s'effectuaient par le biais du téléphone, les communications radio étant utilisées principalement par les policiers, pompiers, ambulanciers, membres de la sécurité civile et par les militaires.

Aujourd'hui la qualité des communications continue de s'améliorer et la proportion de rapports interpersonnels ayant pour base les télécommunications continue d'augmenter. De plus, les distinctions traditionnelles entre téléphone et communications radio ont tendance à s'estomper[190].

Lorsque les télécommunications faisaient partie intégrante des communications en personne, il était toujours possible de pouvoir éventuellement se retirer pour bénéficier d'un peu plus d'intimité. Lorsque deux personnes se rencontrent aussi fréquemment qu'elles se parlent au téléphone, elles peuvent toujours garder leurs confidences pour leur rencontre en face-à-face.

Par contre, considérant que les télécommunications ont davantage tendance à devenir la règle plutôt que l'exception, cela devient plus difficile. Dans une société future, qui n'est peut-être plus très loin, dans laquelle la majorité des communications seront en fait des télécommunications et où plusieurs rapports sont entre des personnes qui ne se rencontrent jamais, cela devient impossible. L'émergence d'Internet et des nouvelles technologies, qui comportent de multiples moyens de communications, contribue à accentuer ce phénomène.

Aucune nation au monde n'est plus dépendante des communications électroniques que les États-Unis d'Amérique. Selon la professeure Susan Landau et le célèbre ingénieur et inventeur de la cryptographie asymétrique, Whitfield Diffie, un niveau de protection élevé est requis pour protéger les communications afin d'assurer la prospérité de la Nation[191].

Section II - Le contexte de l'utilisation de l'informatique, d'Internet et des nouvelles TI

Internet et les nouvelles technologies de l'information fonctionnent à la base avec des ordinateurs. C'est donc par les ordinateurs et leur mise en réseau que les technologies de l'information se sont développées. C'est dans le contexte de ces environnements

---

[190] On a qu'à penser aux divers types de téléphones cellulaires qui utilisent en partie divers types d'ondes radio et le réseau téléphonique commuté. Il y a même des téléphones cellulaires qui n'utilisent pas le réseau téléphonique commuté. Il s'agit d'un téléphone qui s'apparente plutôt à un walkie talkie. Voir notamment le téléphone « Mike » offert par la compagnie *Telus*, en ligne : <http://www.telusmobilite.com/qc/mike/mike_networks_home.shtml> (date d'accès : 2 juillet 2001)

[191] *Privacy on the Line, supra* note 23 aux pp. 104-05. Le Canada pourrait facilement se comparer aux États-Unis dans ce domaine, toute proportion gardée bien entendu.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

informatiques que de nouvelles rationalités ont pris naissance, augmentant du coup les possibilités d'immixtion dans la vie privée des individus[192].

Quatre raisons principales font en sorte que les individus vivant dans une société basée sur l'utilisation massive des ordinateurs ou des nouvelles TI, sont plus susceptibles d'être victimes d'immixtions dans leur vie privée[193]. Nous les avons adaptées à des exemples simples:

- Les ordinateurs seraient des «spécialistes» de la mémoire. Même si cette mémoire n'est pas aussi sophistiquée que la mémoire humaine, comme par exemple la mémoire du parfum d'une rose nous rappelant une période de notre existence, il n'en reste pas moins qu'un ordinateur a une capacité de stockage d'information quasi infinie. La mémoire informatique, surtout d'ordinateurs reliés en réseau, est quantitativement beaucoup plus puissante que la mémoire humaine.

- Les ordinateurs ne pardonnent pas. La capacité d'oublier et de pardonner fait partie intégrante de toute société civilisée. Il faut, pour avancer dans la vie être capable d'oublier, de pardonner, sinon on serait à tout jamais paralysé par de vieilles rancœurs ou par l'idée de vengeance. Étant donné que les ordinateurs «n'oublient» pas, ils ne peuvent *a fortiori* pardonner. Un simple vol à l'étalage commis à l'adolescence apparaissant au plumitif informatisé de la cour a, pour un ordinateur, la même valeur qu'un vol qualifié récent.

- Les ordinateurs et les technologies de l'information permettent d'effectuer des recherches en mémoire sophistiquées et exhaustives. On n'a qu'à penser aux différents logiciels de base de données qui comportent des capacités de recherche et de croisement de l'information inouïes. Et que penser des «meta outils» de recherche d'Internet permettant de fouiller le réseau au complet pour retrouver votre adresse de courriel et tous les sites où vous avez laissé votre trace ![194]

---

[192] Dans *R. c. McLaughlin,* [1980] 2 R.C.S. 331 [ci après *McLaughlin*], la cour Suprême a défini ce qu'était ordinateur, dans le contexte d'un réseau constitué d'un ordinateur central et d'environ trois cents terminaux dispersés sur le campus de l'université de l'Alberta à Edmonton, comme étant une installation de traitement de données, plutôt qu'une installation de télécommunication. Bien que dans cette affaire il y ait eu transmission de renseignements d'une partie de l'installation vers une autre, il n'y a pas eu réception par d'autres installations ni émission à partir de l'installation en cause. Il s'agissait donc en quelque sorte d'une communication en circuit fermé. Ce qui était visé par l'alinéa 287 (1) b) du *Code criminel* est le vol de renseignements d'une installation par laquelle on les canalise. La cour a considéré que la fonction d'un ordinateur dans ce contexte n'est pas la canalisation de renseignements vers des destinataires extérieurs, ce qui pourrait le rendre susceptible d'usage non autorisé; il sert plutôt à effectuer des calculs complexes, à traiter et à mettre en corrélation des renseignements et à les mettre en mémoire pour pouvoir les récupérer. Nous croyons que cette conception étroite de la fonction d'un ordinateur ne tiendrait plus aujourd'hui. En effet, la cour s'est notamment basée sur différentes définitions de ce qu'était un ordinateur de l'époque. La capacité des ordinateurs et leurs fonctions ayant évolués de façon fulgurante depuis la fin des années soixante dix, notamment quant à leur capacité de communication et de calcul, il est raisonnable d'affirmer que si elle avait été rendue aujourd'hui, la Cour aurait considéré un ordinateur comme étant quelque chose de plus sophistiqué qu'un simple calculateur à mémoire étendue ! À notre avis, il s'agit là d'un bon exemple où les rationalités sous-jacentes en matière informatique ont effectivement changé et évolué, rendant ce jugement totalement anachronique.

[193] *The Computer Privacy Handbook*, *supra* note 35 aux pp. 35-37.

[194] Voir notamment les fonctions *author profile* et *view thread*, du moteur de recherche *Deja.com* qui permettent de déterminer le profil d'un utilisateur en trouvant tous les articles publiés sur un sujet donné dans un groupe de discussion ou nouvelles *Usenet*, ou y faire des recherche par centre d'intérêt. *Deja.com*, en ligne :

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

- Les fichiers, répertoires et la mémoire informatique sont transférables. La mémoire humaine n'est pas transférable. Il est impossible pour un humain de transférer au complet tous ses souvenirs à un autre être humain. La mémoire informatique le peut d'une multitude de façons. Il va sans dire que le nombre de façons a augmenté significativement depuis l'avènement d'Internet.

Nous estimons que la mise en réseau multiplie de façon exponentielle l'occurrence des phénomènes décrits dans les quatre raisons énumérées ci-avant. Nous sommes bien loin des considérants du juge La Forest énoncés dans *Dyment*[195] relativement aux sphères d'intimité. La mise en réseau des ordinateurs a mené à l'apparition d'Internet et à l'utilisation des nouvelles TI. Il convient donc ici de traiter plus en détail de ce qu'est effectivement Internet.

Section III - La Cour suprême américaine décrit Internet

La Cour suprême américaine dans *Reno c. ACLU* décrit Internet de la manière suivante :

> « *The Internet is an international network of interconnected computers. It is the outgrowth of what began in 1969 as a military program called "ARPANET," which was designed to enable computers operated by the military, defense contractors, and universities conducting defense-related research to communicate with one another by redundant channels even if some portions of the network were damaged in a war. While the ARPANET no longer exists, it provided an example for the development of a number of civilian networks that, eventually linking with each other, now enable tens of millions of people to communicate with one another and to access vast amounts of information from around the world. The Internet is "a unique and wholly new medium of worldwide human communication."* » [notes omises] [196].

Cette décision ne porte pas sur la surveillance électronique ou sur le IV[e] amendement de la constitution américaine, l'équivalent américain de l'article 8 de la *Charte canadienne*. Elle porte plutôt sur l'étendue de la liberté d'expression telle que protégée par le I[er] amendement de la constitution américaine. On devait décider, notamment, si certaines dispositions du *Communication Decency Act* portaient atteinte au I[er] amendement[197].

<http://deja.com/*Usenet*> (date d'accès : 2 novembre 2000). *Meta Crawler*, en ligne : <http://www.metacrawler.com> (date d'accès : 24 avril 2001). Ils peuvent notamment servir à trouver une adresse de courriel d'une personne. Voir notamment *Alta Vista*, en ligne : <http://www.altavista.com> (date d'accès : 24 avril 2001), où il suffit d'entrer le nom d'une personne entre guillemets dans la case appropriée et de lancer la recherche sur le Web. On pourra également lancer une recherche *Usenet* à partir d'*Alta Vista*. Cette recherche permettra de retrouver le nom dans les groupes de discussion ou de nouvelles *Usenet*. Voir également le moteur de recherche *Lycos*, en ligne : <http://www.lycos.com> (date d'accès : 24 avril 2001).

[195] *Supra* note 38 aux pp. 428-30.

[196] *Supra* note 1, aux pp. 849-50. Nous utiliserons également la décision de première instance, dans laquelle on retrouvait un exposé conjoint, des faits relatifs aux divers contextes de communication apportés par Internet, des plus précis et exhaustif. Voir *ACLU c. Reno,* 929 F.Supp. 824 (E.D.Pa. 1996) [ci-après *ACLU c. Reno*]. Cet exposé a également été repris en partie par la Cour suprême. Nous référerons donc aux deux décisions indistinctement selon le besoin, compte tenu que l'exposé conjoint a servi de base factuelle aux deux cours pour rendre leur décision.

[197] Le *Communication Decency Act* (ci-après : *«CDA»)*, constitue le Titre V du Telecommunications Act of 1996 (Pub. L. 104-104, 110 Stat.56.) qui en comprend sept. La première disposition contestée, l'article 223a), interdit "*the knowing transmission of obscene or indecent messages to any recipient under 18 years of age*"

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

Le tribunal détermine qu'Internet n'est pas considéré comme un médium de même nature que la radio ou la télévision pour les fins d'application du I[er] Amendement. La majorité de la Cour, sous la plume du juge Stevens, reprend la conclusion de la Cour de district en précisant que la navigation dans Internet requiert un usager actif et des *«series of affirmative steps more deliberate and directed than merely turning a dial»*[198]. L'internaute n'est donc pas dans une position passive à l'instar du téléspectateur ou de l'auditeur. Il ne «subit» pas l'information, puisqu'il doit, au contraire, la chercher et la trouver pour en prendre connaissance ou l'utiliser. L'utilisateur «se place» donc dans un contexte particulier lorsqu'il communique dans Internet. Nous estimons que ce constat trouve application pour ce qui est de l'analyse de la protection offerte par l'article 8 de la *Charte canadienne*. En effet, l'utilisateur se place dans un contexte particulier lorsqu'il communique par le biais d'Internet. Internet comportant lui-même de multiples contextes de communication plus ou moins privés, il est raisonnable de penser qu'un utilisateur verra son expectative raisonnable de vie privée varier en conséquence.

Cette décision est également utile pour la détermination des contextes les plus fréquents dans Internet. En effet, dans le cadre de son analyse des faits, la Cour suprême américaine décrit les principaux paramètres de certains moyens de communication offerts dans Internet :

> « *Anyone with access to the Internet may take advantage of a wide variety of communication and information retrieval methods. These methods are constantly evolving and difficult to categorize precisely. But, as presently constituted, those most relevant to this case are electronic mail ("e-mail"), automatic mailing list services ("mail exploders," sometimes referred to as "listservs"), "newsgroups," "chat rooms," and the "World Wide Web." All of these methods can be used to transmit text; most can transmit sound, pictures, and moving video images. Taken together, these tools constitute a unique medium—known to its users as "cyberspace"—located in no particular geographical location but available to anyone, anywhere in the world, with access to the Internet* »[199].

Nous décrirons plus en détail ces différentes ressources, lors de la description des contextes particuliers de communication offerts dans Internet. Afin de mieux en saisir le fonctionnement, il convient maintenant de traiter de l'aspect technique d'Internet.

Section IV - Le contexte technique d'Internet

Sans trop de détails techniques, on peut affirmer qu'Internet constitue un réseau de réseaux d'ordinateurs interconnectés. Encore faut-il comprendre qu'est-ce qu'un réseau. Nous y reviendrons en détail un peu plus loin. Cette combinaison de réseaux en fait le plus grand réseau informatique de la planète. Il s'agit d'un réseau regroupant une multitude de réseaux régionaux, gouvernementaux et commerciaux. Tous ces réseaux, grands ou petits, se

---

("the indecent transmission provision"). La seconde disposition attaquée, l'article 223d), interdit, pour sa part, *"the knowing sending or displaying of patently offensive messages in a manner that is available to a person under 18 years of age" ("patently offensive display provision")*. Ces deux dispositions ont été déclarées contraire au premier amendement de la Constitution américaine.

198 *Reno c. ACLU, supra* note 1 à la p. 854.

199 *Ibid.* à la p. 851.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

« parlent » ou fonctionnent en utilisant les protocoles de communications TCP et IP[200]. La Cour de district de la Pennsylvanie a défini Internet de cette façon :

> « *1. The Internet is not a physical or tangible entity, but rather a giant network which interconnects innumerable smaller groups of linked computer networks. It is thus a network of networks. This is best understood if one considers what a linked group of computers -- referred to here as a "network" -is, and what it does. Small networks are now ubiquitous (and are often called "local area networks"). For example, in many United States Courthouses, computers are linked to each other for the purpose of exchanging files and messages (and to share equipment such as printers). These are networks.*
>
> *2. Some networks are "closed" networks, not linked to other computers or networks. Many networks, however, are connected to other networks, which are in turn connected to other networks in a manner which permits each computer in any network to communicate with computers on any other network in the system. This global Web of linked networks and computers is referred to as the Internet* » [notes omises][201].

Il y a également des réseaux commerciaux à grande échelle qui servent de porte d'entrée à Internet. Ces réseaux offrent l'accès à un contenu substantiel d'information et à des services en ligne, le tout organisé et présenté de façon très conviviale pour l'utilisateur. Bien que le réseau soit important et que l'information qui circule est importante, il s'agit en quelque sorte d'Internet à l'intérieur d'Internet. L'exposé conjoint de faits de la décision rendue par la Cour de District de la Pennsylvanie dans *ACLU c. Reno*, décrit le contexte de ces réseaux commerciaux à valeur rajoutée :

> « *19. Another common way for individuals to access the Internet is through one of the major national commercial "online services" such as America Online, CompuServe, the Microsoft Network, or Prodigy. These online services offer nationwide computer networks (so that subscribers can dial-in to a local telephone number), and the services provide extensive and well organized content within their own proprietary computer networks. In addition to allowing access to the extensive content available within each online service, the services also allow subscribers to link to the much larger resources of the Internet. Full access to the online service (including access to the Internet) can be obtained for modest monthly or hourly fees. The major commercial online services have almost twelve million individual subscribers across the United States* » [notes omises][202]

---

[200] *Le guide de l'internaute 2000, supra* note 136 à la p. 555 et *Droit du Cyberespace*, *supra* note 8 à la p. intr-2. Voir également : D. Johnston, S. Handa, et C. Morgan, *Cyber Law*, Toronto, Stoddart (1997), p. 16 [ci après *Cyber Law*].

[201] *ACLU c. Reno, supra* note 196, aux pp. 830-31. Nous croyons utile de référer à cette décision en raison de la description exhaustive qu'on y retrouve d'Internet et de ses ressources. Cette description a fait l'objet d'un exposé conjoint des faits de la part des parties, qui a été accepté en première instance et résumé par la suite par la Cour suprême. Voir *Reno c. ACLU, supra* note 1 à la p. 849.

[202] *ACLU c. Reno, supra* note 196, à la p. 833.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

Plusieurs ressources sont offertes dans ce réseau de réseaux tels le Web, courriel, le transfert de fichiers FTP, la session en mode *Telnet*, les groupes de discussion ou de nouvelles *Usenet*, le bavardage-clavier ou clavardage du service IRC, la téléphonie et vidéoconférence Internet et la messagerie instantanée. Nous traiterons de ces technologies plus loin. Il suffit de retenir pour l'instant qu'il s'agit de moyens différents ou complémentaires l'un de l'autre, utilisés pour communiquer par le biais d'Internet. Il convient maintenant de traiter plus en détail des aspects techniques d'Internet afin de mieux comprendre son fonctionnement. Nous traiterons de l'ordinateur, composante de base d'Internet et de certains de ses périphériques, de la notion de réseau en informatique, du rôle de l'administrateur de réseau, de la notion d'intranet et d'extranet, du protocole TCP/IP, des concepts d'adresse IP, d'adresse Internet d'un appareil ou nom logique, de paquet IP d'informations ou datagramme, du numéro de port IP et de port TCP/IP et de domaine et de serveur de nom de domaine.

A. Les composantes de base d'Internet

Nous avons vu qu'Internet est défini en fonction d'ordinateurs reliés en réseaux. Il convient donc ici de définir ce qu'est un ordinateur. Nous aurions pu retenir une multitude de définitions, mais compte tenu du contexte général de la présente étude nous avons choisi celle du *Code criminel* qui nous semble suffisante et contemporaine. Le paragraphe 342.1(2) du *Code criminel* propose donc la définition suivante :

> «*342.1(2) « ordinateur » Dispositif ou ensemble de dispositifs connectés ou reliés les uns aux autres, dont l'un ou plusieurs d'entre eux :*
> *a) contiennent des programmes d'ordinateur ou d'autres données;*
> *b) conformément à des programmes d'ordinateur :*
> *(i) soit exécutent des fonctions logiques de commande,*
> *(ii) soit peuvent exécuter toute autre fonction*. »

Il découle de cette définition qu'un ordinateur se caractérise principalement par une composante matérielle et une composante logicielle. Nous ne nous attarderons pas spécifiquement à l'aspect logiciel propre au fonctionnement d'un ordinateur. Nous traiterons indirectement de plusieurs logiciels ou applications lors de notre étude des contextes particuliers de communication. Nous nous attarderons ici à quelques composantes matérielles ou périphériques, autres que celles rattachées au concept de réseau dont nous traiterons plus loin, susceptibles d'influer sur le niveau d'expectative raisonnable de vie privée. Nous traiterons donc du microprocesseur, du clavier, de l'écran et de l'imprimante.

– Le microprocesseur

Défini de façon simpliste, le microprocesseur ou processeur est une composante matérielle d'un ordinateur qui sert à le faire fonctionner. Il s'agit en quelque sorte du cerveau de l'ordinateur capable d'effectuer des opérations arithmétiques et logiques sur des données, et donc de commander d'autres unités de l'ordinateur[203]. Plusieurs sociétés offrent des microprocesseurs sur le marché dont le MAC de la société *Apple*. Une des plus importante est la société *Intel*[204]. Successeur du processeur *Pentium* II, le processeur *Pentium* III d'*Intel*, est

---

[203] A. Voss, *Dictionnaire de l'informatique et de l'Internet 2001*, Paris, Micro Application, 2000, à la p. 712 [ci après *Dictionnaire de l'informatique*].

[204] Voir Intel, en ligne : <http://www.intel.com> (date d'accès :5 septembre 2001).

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

apparu en février 1999. Celui-ci comporte une innovation importante, soit la présence d'un numéro de série interne, ou *Processor Serial Number* (*PSN*). Il a pour but de faciliter l'identification d'un utilisateur, notamment en matière de commerce électronique. Par contre, ce numéro peut, en théorie, permettre à des fsI d'identifier immédiatement l'ordinateur branché au réseau. Ainsi, tout utilisateur laisserait en quelque sorte une empreinte numérique lors de l'utilisation d'Internet[205].

Compte tenu des problèmes que cette technologie peut entraîner pour les utilisateurs, notamment en matière de vie privée, la société *Intel* a décidé en avril 2000, de désactiver cette fonction d'identification[206]. L'efficacité de cette mesure n'est toutefois pas certaine, notamment en ce qui concerne les processeurs vendus avec le numéro de série interne. Il reviendrait en effet aux utilisateurs de désactiver eux-mêmes la fonction, ce qui n'est pas une mince affaire. En conséquence, l'expectative raisonnable de vie privée d'un utilisateur muni d'un ordinateur équipé d'un processeur d'*Intel Pentium III,* dont le numéro de série n'a pas été désactivé convenablement, pourrait être compromise. La connaissance de l'existence de la fonction d'identification et de la possibilité de désactivation sera déterminante dans l'évaluation subjective du niveau d'expectative raisonnable de vie privée d'un individu.

– Le clavier

Le clavier est généralement le périphérique d'entrée le plus utilisé. Il sert à entrer l'information dans l'ordinateur[207]. Il s'agit de l'intermédiaire entre la machine et l'être humain assis devant l'écran de l'ordinateur. Dans certaines circonstances, il est possible de savoir exactement quelles touches ont été tapées par l'utilisateur. On reproduira ainsi le contenu exact de tout ce qui a été tapé au clavier par un utilisateur.

Pour ce faire on utilise un enregistreur de touche. Cet enregistreur peut prendre la forme d'une composante matérielle rajoutée au clavier ou ailleurs dans l'ordinateur visé, ou il peut prendre la forme d'un logiciel inséré dans la mémoire de l'ordinateur visé[208]. Dans les deux cas, on peut exactement savoir ce qui a été tapé depuis un moment déterminé d'avance. Un enregistreur de touche est souvent utilisé dans les cas où un employeur veut effectuer un certain suivi des activités de ses employés, notamment dans le contexte où l'entrée de données fait partie intégrante des tâches reliées au travail. Nous référons le lecteur à la section traitant du branchement à partir des lieux du travail pour une discussion plus approfondie sur l'expectative raisonnable de vie privée dans ce contexte. Dans ce cas, la personne installant l'enregistreur de touche pourra, le plus souvent, le faire légitimement. Dans d'autres cas il peut y avoir installation illégitime, soit par des tiers malveillants. Nous ne traiterons pas de cet aspect.

Le dernier cas d'intérêt est celui de l'installation d'un enregistreur de touches par un agent de l'État. Il pourrait en effet être intéressant pour l'État d'utiliser cette technique pour obtenir les

---

[205] *Dictionnaire de l'informatique, supra* note 203 à la p. 678.

[206] Voir Big Brother Inside, en ligne : <http://www.bigbrotherinside.com> (date d'accès : 6 septembre 2001). Il n'est pas clair si la fonction d'identification de la nouvelle génération de microprocesseur Pentium IV, Pentium IV-m et Pentium Xeon existera ou sera désactivée.

[207] B. Fabrot, *Protégez-vous sur Internet : Anonymat et sécurité*, Paris, Marabout Informatique, 1999, à la p. 52 [ci après *Protégez-vous sur Internet*].

[208] *Ibid.* Voir aussi (Anonyme), *Sécurité Optimale,* 2e éd., Paris, Campus Press France, 1999, aux pp. 308-09 [ci après . *Sécurité Optimale*].

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

communications privées d'un individu. Pour ce faire il faudra, dans la majorité des cas, obtenir une autorisation judiciaire préalable, dont la nature sera à déterminer dans chaque cas.

– L'écran

L'écran sert bien entendu à voir ce qui se passe dans l'ordinateur. Sans l'écran, il est impossible d'interagir efficacement avec un ordinateur. L'écran comporte généralement un tube cathodique. Les écrans plats bénéficient quant à eux d'une technologie basée sur l'utilisation de cristaux liquides, tout comme les ordinateurs portables, agendas électroniques, calculatrices, etc.[209]

L'utilisation d'un écran à la vue de tous est susceptible d'entraîner une diminution de l'expectative raisonnable de vie privée. Cette diminution sera notamment tributaire du lieu où se trouve l'ordinateur, des mesures prises par l'utilisateur pour en dissimuler le contenu et du nombre de personnes ayant un accès visuel à l'écran.

Par ailleurs, même dans les cas où l'utilisateur est en retrait dans un lieu plus « privé », il se peut que son expectative raisonnable de vie privée soit tout de même réduite. En effet, le tube cathodique d'un écran traditionnel émet des ondes relativement puissantes. Avec un balayeur d'ondes approprié, il est possible, à distance, de suivre absolument tout ce qui se passe sur l'écran d'un utilisateur ciblé[210]. Plus l'écran est récent, moins les émissions seront fortes. De plus, les écrans à cristaux n'émettent pas d'ondes susceptibles d'interception[211]. Dans les cas où des ondes sont émises, il est recommandé pour en éviter l'interception par un récepteur de type Van Eck, d'utiliser une mesure de protection rencontrant la norme TEMPEST. Il s'agit notamment d'utiliser un dispositif placé autour de l'écran qui empêchera les informations d'être captées par un tiers se trouvant à proximité. Cette protection sera appelée cage de Faraday[212]. Donc selon le type d'écran utilisé et les dispositions techniques prises par l'utilisateur, les informations apparaissant à l'écran seront susceptibles ou non de diffusion sur une distance qui pourra dans certains cas être assez importante. Le problème soulevé ici ressemble beaucoup à la problématique entourant les ondes émises par les téléphones cellulaires, captées à l'aide de balayeur d'ondes, que nous avons déjà abordé plus haut.

– L'imprimante

L'imprimante est un périphérique qui sert à imprimer sur papier les informations se trouvant électroniquement dans la mémoire d'un ordinateur[213]. Or, dans bien des cas, l'imprimante est partagée avec d'autres utilisateurs, notamment pour diminuer les coûts d'achat et maximiser

---

209 *Protégez-vous sur Internet, supra* note 207 à la p. 54.

210 Un récepteur de type Van Eck, peut capter des signaux émanant d'un moniteur jusqu'à une distance de 1 kilomètre. Voir D.E. Denning, *Information Warfare and Security*, Reading (Mass.), Addison-Wesley, 1999, à la p. 189 [ci après *Information Warfare*] ; W. Gieske, *Sécurité et protection*, Düsseldorf, Data Becker GmbH & co., 1998, à la p. 126 [ci après *Sécurité et protection*].

211 *Protégez-vous sur Internet, supra* note 207 à la p. 55.

212 *Sécurité et protection*, *supra* note 210 aux pp. 126-27. Voir aussi *Information Warfare, supra* note 210 aux pp. 318-19. L'acronyme TEMPEST signifierait Transcient Electromagnetic Pulse Emanation System. Nous indiquons sciemment cette signification au conditionnel, compte tenu qu'il s'agit d'un nom de code de l'armée américaine qui doit rester, en principe, secret. Voir également : J. Mc Namara, « *The complete, Unofficial TEMPEST Information Page* », (2001), en ligne : <http://www.eskimo.com/~joelm/tempest.html> (dernière modification : 3 août 2001)

213 *Dictionnaire de l'informatique, supra* note 203 à la p. 428.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

son utilisation. Dans les cas où elle est partagée, l'imprimante se trouvera généralement en un lieu autre que celui où se trouve l'utilisateur. L'imprimante pourra se trouver dans un autre bureau, dans une aire commune, sur un autre étage, etc. Le lieu où se trouve l'imprimante influera donc, dans bien des cas, sur le niveau d'expectative raisonnable de vie privée qu'un utilisateur aura dans l'information qu'il imprime. Le nombre d'utilisateurs d'une même imprimante et le nombre de personnes y ayant accès pourra également influer sur le niveau d'expectative raisonnable de vie privée. Nous verrons un exemple de cette problématique dans la section traitant du branchement à Internet à partir du lieu de travail.

La notion de réseau en informatique

Un réseau est un ensemble de matériels informatiques interconnectés[214]. Il existe plusieurs types de réseaux ou configurations. Il y a les LAN[215], MAN[216], WAN[217], CAN [218]et TAN[219]. La principale fonction d'un réseau informatique est de relier des objets identiques en utilisant en ensemble de règles garantissant un service fiable[220].

Les réseaux comportent une partie matérielle (ordinateurs, terminaux, carte d'interface réseau, câblage, etc.), une partie logicielle (applications, programmes de gestion du réseau, systèmes de sécurité, etc.) et une composante « humaine », constituée d'une part des techniciens et des gestionnaires chargés de la mise en œuvre du réseau, d'autre part des clients du réseau, c'est-à-dire des utilisateurs bénéficiaires des services offerts par le réseau[221]. Il va sans dire que les

---

[214] A. Dufour, *Internet*, Paris, Presses Universitaires de France, coll. « Que sais-je? », 1998, à la p. 4 [ci après *Internet*].

[215] LAN pour *Local Area Network*. Même s'il s'agit des réseaux les plus simples, ils ne sont pas nécessairement les plus rudimentaires. En effet, certains LAN peuvent compter quelques milliers d'utilisateurs. *Les réseaux*, *supra* note 136 aux pp. 15, 375.

[216] MAN pour *Metropolitain Area Network*. Il s'agit du niveau immédiatement supérieur au LAN en matière de complexité. Si l'expansion d'un LAN est telle qu'il doive par exemple occuper deux immeubles situés géographiquement très près l'un de l'autre, il est fréquent de fractionner le réseau en plusieurs petits réseaux et de les relier à un MAN, en utilisant des liaisons téléphoniques spécialisées à haut débit ou des équipements spéciaux, (unités de transmission de données utilisant la radio, les micro-ondes ou le laser) permettant des vitesses de transfert équivalentes à celles des LAN. Les MAN permettent donc à des utilisateurs situés à plusieurs endroits géographiques, de partager des ressources réseau comme s'ils étaient reliés au même réseau local. Voir *Les réseaux*, *supra* note 136 aux pp. 16-17, 376.

[217] WAN pour *Wide Area Network*. Les WAN sont constitués de LAN ou de MAN distants géographiquement reliés par des lignes téléphoniques à haut débit. Les WAN sont souvent mis en place lorsqu'il est important pour tous les utilisateurs d'avoir la possibilité d'accéder à des informations communes telles que les bases de données de produits ou des serveurs locaux bancaires. Contrairement au LAN et au MAN, les WAN utilisent presque toujours des routeurs, c'est-à-dire un équipement qui gère les flots de données entre les réseaux. Puisque la majeure partie du trafic d'un WAN se situe dans les LAN et les MAN, le constituant, les routeurs jouent un rôle important : ils s'assurent que les LAN et les MAN ne reçoivent que les données qui leur sont destinées. *Les réseaux*, *supra* note 136 aux pp. 17-18, 382.

[218] CAN pour *Campus Area Network*. Les CAN sont pratiquement identiques au MAN. Ils sont constitués d'un seul réseau distribué dans une zone géographique limitée, un campus, par exemple. La configuration technique d'un CAN est différente de celle d'un MAN mais, pour l'essentiel, l'utilisateur ne se rend pas compte si le serveur auquel il accède est de l'autre côté de la pièce ou du campus. Les CAN sont très utilisés dans des organisations grandes consommatrices d'informations, notamment les éditeurs de logiciels et les universités. *Les réseaux*, supra note 136 aux pp. 20-21.

[219] TAN pour *Tiny Area Network*. Les TAN sont des «réseaux domestiques». Ils sont composés de deux ou trois ordinateurs installés à la maison ou dans d'autres locaux «non professionnels». *Les réseaux*, *supra* note 136 à la p. 20.

[220] *Ibid*. à la p. 6.

[221] *Internet*, *supra* note 214 à la p.4. Il y aurait également l'aspect organisationnel d'un réseau. Un réseau serait

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

composantes matérielles et logicielles peuvent, à l'intérieur de certains réseaux, être partagées par les utilisateurs. Dans ce contexte, on pourra partager des applications ou programmes, un disque dur ou espace mémoire, ou partager l'utilisation de périphériques, comme par exemple une imprimante. Ce partage pourra survenir en un même lieu ou dans des lieux différents.

Internet est donc constitué, en partie, d'un ensemble de réseaux informatiques privés, publics et gouvernementaux (LAN, MAN et WAN) reliés les uns aux autres. Chaque réseau privé individuel est composé d'un ensemble d'ordinateurs au sein d'une entité. Dans la décision de première instance rendue dans *ACLU c. Reno*, on y décrit comment les réseaux sont reliés entre eux pour former Internet :

> « *4. Some of the computers and computer networks that make up the Internet are owned by governmental and public institutions, some are owned by non-profit organizations, and some are privately owned. The resulting whole is a decentralized, global medium of communications -- or "cyberspace" -- that links people, institutions, corporations, and governments around the world. The Internet is an international system. This communications medium allows any of the literally tens of millions of people with access to the Internet to exchange information. These communications can occur almost instantaneously, and can be directed either to specific individuals, to a broader group of people interested in a particular subject, or to the world as a whole* » [note omise][222]

Chaque entité n'est responsable que des ordinateurs situés dans sa sphère d'influence. Généralement, les réseaux individuels sont connectés par des équipements spéciaux appelés routeurs qui doivent déterminer quelles sont les données devant rester dans le réseau local et celles devant être transmises à d'autres réseaux[223]. Il n'existe pas d'organisation centrale qui gère Internet, ce qui fait que son contrôle est pratiquement impossible :

> « *11. No single entity -- academic, corporate, governmental, or non-profit -- administers the Internet. It exists and functions as a result of the fact that hundreds of thousands of separate operators of computers and computer networks independently decided to use common data transfer protocols to exchange communications and information with other computers (which in turn exchange communications and information with still other computers). There is no centralized storage location, control point, or communications channel for the Internet, and it would not be technically feasible for a single entity to control all of the information conveyed on the Internet* »[224].

Il est raisonnable d'affirmer, qu'en principe, plus le réseau sera grand, plus un utilisateur sera susceptible de voir son expectative raisonnable de vie privée compromise. Bien entendu, cette affirmation n'est pas absolue. Plusieurs autres facteurs viendront moduler cette affirmation. Nous ne nous attarderons pas sur la partie logicielle du fonctionnement d'un réseau, ce qui déborderait grandement du cadre de l'étude. Quant à la partie matérielle, nous l'aborderons

---

en fait un ensemble d'éléments réunis par différents liens de nature organisationnelle. Voir *Droit du Cyberespace*, *supra* note 8 à la p. 2-3.

222 *ACLU c. Reno, supra* note 196 à la p. 831.

223 *Les réseaux*, *supra* note 136 aux pp. 20-21.

224 *ACLU c. Reno, supra* note 196 à la p. 832.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

indirectement lorsque nous traiterons des différentes ressources utilisées dans Internet. Il convient par contre de traiter de la partie humaine d'un réseau, plus particulièrement de l'administrateur de réseau, notamment en raison du rôle qu'il peut jouer au niveau de l'expectative raisonnable de vie privée.

L'administrateur de réseau

Pour pouvoir fonctionner, un réseau et ses composantes doivent être gérés et entretenus. Par exemple, dans le contexte d'un réseau de type WAN, LAN ou MAN, l'administrateur de réseau devra être capable de résoudre les problèmes matériels et logiciels liés au réseau[225]. Pour ce faire, il devra notamment être en mesure de conserver des fichiers de journalisation du système, de procéder au stockage sécurisé des données, de créer et gérer les comptes des utilisateurs du réseau et de faire en sorte que les données puissent être récupérées en cas de catastrophe[226]. L'administrateur de réseau pourra également effectuer une surveillance en direct du réseau, notamment par le biais d'un analyseur de réseau ou *sniffer*, dont l'objectif principal est d'analyser le trafic et d'identifier les zones potentielles de problèmes. Comme nous le verrons plus en détail, l'information qui circule dans un réseau fonctionnant sur la base du protocole *TCP/IP*, est divisée en paquet d'information ou datagramme. On peut se servir d'un analyseur de réseau pour déterminer l'origine exacte d'un problème affectant un segment du réseau, comme par exemple dans le cas où la livraison de certains paquets d'informations s'effectue trop lentement. Cette opération implique qu'un administrateur de réseau ou un de ses employés pourra avoir accès à des mots de passe ou informations personnelles et confidentielles des utilisateurs du réseau[227].

Toutes ces tâches sont susceptibles de porter atteinte à une quelconque expectative raisonnable de vie privée d'un utilisateur du réseau. En effet, dans le cadre de la conservation des fichiers de journalisation, un administrateur de réseau conservera un journal des heures et des dates de tous les événements du réseau, de toutes les interactions de la machine avec son environnement et de tous les ajouts, déplacements et modifications du système[228].

Cette conservation est rendue nécessaire, notamment pour limiter les effets pervers de la négligence dont on pourrait blâmer une organisation; en effet, pour des raisons de sécurité, elle permet de savoir ce qui se passe en tout moment dans son réseau, et qui s'est branché au réseau ou qui a tenté de le faire. Pour permettre la détection d'anomalies dans le réseau, elle permet également la capture de paquets d'informations qui révéleront la mauvaise configuration du réseau et le trafic excessif[229]. Elle est également nécessaire pour garder la trace des ajouts, déplacements et modifications du système, puisqu'elle permet de conserver une liste exhaustive des ressources et fichiers spécifiques auxquels chaque utilisateur a accès, et de tous leurs mots de passe. L'accès au mot de passe est également utile à l'administrateur de réseau lorsqu'il devra avoir accès aux fichiers d'un utilisateur[230].

---

[225] *Internet*, *supra* note 214 à la p. 20. Voir aussi *Les réseaux*, *supra* note 136 à la p. 331. Dans le contexte d'un individu branché à Internet par le biais d'un fournisseur de service Internet, l'administrateur de réseau sera représenté par le service à la clientèle du fournisseur de service. *Le guide de l'internaute 2000, supra* note 136 à la p. 551.

[226] *Les réseaux*, *supra* note 136 à la p. 332.

[227] *Sécurité Optimale, supra* note 208 aux pp. 241-43.

[228] *Les réseaux supra* note 136 aux pp. 337-38, 343.

[229] *Ibid*. aux pp. 338-39.

[230] *Ibid*. à la p. 342.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

La fonction première d'un réseau est l'échange d'informations[231]. Dans ce contexte, il faut plusieurs utilisateurs pour que le réseau ait une raison d'être. Dans le cadre de la gestion d'un réseau, un administrateur doit voir à la création et à la gestion des comptes des utilisateurs du réseau[232]. Cette tâche implique nécessairement une atteinte à une quelconque attente en matière de vie privée, notamment à cause du système d'attribution et de modification des mots de passe et à cause du système d'attribution des accès aux ressources et fichiers auxquels un utilisateur a accès. L'administrateur de réseau détient conséquemment des informations privilégiées sur le compte d'un utilisateur.

Pour une gestion responsable d'un réseau, un administrateur doit également être en mesure de récupérer les données stockées du réseau en cas de panne ou de catastrophe. Pour ce faire, il doit au préalable établir un système de stockage approprié des données ou de sauvegarde. Cela implique donc une copie systématique de toutes les informations contenues dans le réseau, comme par exemple le disque dur d'un serveur sur lequel seront enregistrées toutes les données des utilisateurs[233]. Ces enregistrements seront généralement systématisés, automatisés et effectués sur des supports indépendants du réseau, tels des bandes ou disques à haute capacité, ou tout simplement sur un autre ordinateur qui se trouvera idéalement ailleurs que sur les lieux où le matériel du réseau à protéger se trouve[234]. Ces enregistrements feront parfois l'objet d'audits effectués par l'administrateur de réseau pour y détecter les anomalies[235].

Dans le contexte où un réseau de type WAN, LAN ou TAN est branché à Internet, le serveur Web, servant de passerelle pour passer du réseau à Internet, fera également l'objet d'audits, afin d'y détecter des fichiers placés par les utilisateurs qui pourraient compromettre la sécurité du réseau[236].

L'administrateur de réseau d'un fsI, aura la même position privilégiée par rapport à l'information fournie par les abonnés. Ces informations seront également accessibles par l'administrateur de réseau de la même manière que dans le cadre d'un réseau plus petit, avec les adaptations nécessaires bien entendu. Dans *United States c. Hambrick*[237], il a été décidé

---

[231] *Ibid*. à la p. 352.
[232] *Ibid*. à la p.346.
[233] En effet dans le contexte de l'utilisation d'un réseau, il est recommandé que les utilisateurs enregistrent leurs données sur le serveur du réseau. *Les réseaux*, *supra* note 136 à la p. 343.
[234] *Ibid*. aux pp. 348-53.
[235] *Ibid*. à la p. 352.
[236] *Ibid*.
[237] No. 99-4793 (4th Cir. 08/03/2000) [ci après *Hambrick*], aux para. 21-22. Il est à notre avis périlleux d'appliquer cette décision en droit canadien. En effet, elle est en partie basée sur les principes juridiques développés dans *United States c. Miller*, 425 U.S. 435 (1976) [ci après *Miller*], qui n'ont pas été « importés » en droit canadien par la Cour suprême dans *Plant, supra* note 34. Donc l'information détenue par un fsI au Canada, pourrait devoir être obtenue quand même par le biais d'un mandat ou d'un autre type d'ordonnance qui exige des standards plus élevés que pour l'obtention par simple *subpoena*. De plus, au Canada, la *Loi sur la protection des renseignements personnels et les documents électroniques*, L.R.C. 1985, c. P-8.6, en ligne : Ministère de la justice <http://lois.justice.gc.ca/fr/P-8.6/74408.html> (date d'accès : 30 août 2001) et au Québec, les articles 35 à 40 inclusivement, du *Code civil du Québec*, L.Q. 1991, c. 64, en ligne : Les publications du Québec <http://publicationsduquebec.gouv.qc.ca/fr/cgi/frameset.cgi?url=/documents/lr/CCQ/CCQ_1.html> (date d'accès : 30 août 2001) et la *Loi sur la protection des renseignements personnels dans le secteur privé*, L.R.Q. c. P-39.1, en ligne : Les publications du Québec

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

que l'information non reliée au contenu fournie par un abonné au fsI, ne bénéficiait pas d'une expectative raisonnable de vie privée. Selon cette décision, il serait possible d'obtenir l'information relative au nom, à l'adresse de facturation, aux numéros de téléphone de la résidence et du travail, au numéro de télécopieur et autres informations relatives à la facturation, par un simple *subpoena*. Même si dans certaines circonstances, une personne peut avoir une expectative raisonnable de vie privée à l'égard de l'information non reliée au contenu d'une communication transmise par le biais d'Internet, elle n'aura pas l'intérêt suffisant pour prétendre à une expectative raisonnable de vie privée à l'égard de l'information non reliée au contenu.

L'administrateur de réseau doit aussi décider s'il autorise les requêtes de type *finger* sur son système. *Finger* est un service couramment implanté sur divers systèmes d'exploitation dont l'objectif est de fournir des informations sur les utilisateurs d'un hôte distant donné[238]. À l'instar des services TCP/IP, *finger* fonctionne selon le modèle client-serveur. De nombreux administrateurs de réseau autorisent sur leur serveur un accès *finger* illimité en provenance de l'extérieur. *Finger* utilise le port TCP/IP numéro 79[239]. Des utilisateurs distants sont ainsi en mesure d'identifier tous les utilisateurs d'un système. Pour cela, il suffit d'émettre la commande : « *finger* @hôtecible.com », à partir d'un logiciel client correspondant au système du serveur de la cible. Bien entendu, le terme « hôtecible » dans la commande correspond au serveur visé par la requête et sera différent selon le serveur visé. Cette commande demande de fournir des informations sur tous les utilisateurs actuellement branchés à Internet. Le genre de liste générée par ce type de requête permet dans presque tous les cas de révéler le véritable nom de l'utilisateur branché, soit directement ou indirectement. On connaîtra directement le nom réel de l'utilisateur dans la mesure où celui-ci a fourni les bons renseignements à son administrateur de réseau. On connaîtra indirectement l'identité réelle d'un utilisateur en se servant de l'information recueillie comme base pour une recherche lancée sur un autre service. On utilisera souvent *Alta Vista*[240] et *World Pages*[241] pour confirmer l'identité, connaître l'adresse résidentielle et le numéro de téléphone d'un utilisateur. Dans Internet, *World Pages* et *Alta Vista* font office de bottins téléphoniques géants, accessibles à tous. Un service comme *America Online* ne permet pas les requêtes de type *finger* sur ses utilisateurs[242]. Dans le cas où un administrateur de réseau autorise les requêtes de type *finger*, nous soumettons qu'un utilisateur n'a pas ou peu d'expectative raisonnable de vie privée sur sa réelle identité et sur le fait qu'il soit branché dans Internet à un moment donné. Un utilisateur distant plus sophistiqué pourrait même lancer automatiquement des requêtes successives de type *finger*, afin de savoir si l'utilisateur ciblé est branché, combien de fois il

---

<http://publicationsduquebec.gouv.qc.ca/fr/cgi/frameset.cgi?url=/documents/lr/P_39_1/P39_1.html> (date d'accès 30 août 2001), offrent des protections aux renseignements personnels d'individus, détenus par des tiers, principalement dans le cadre d'activités commerciales. Les fournisseurs d'accès Internet sont à notre avis visés, en tout ou en partie, par ces lois.

238 De multiples systèmes sont susceptibles de requêtes de type *finger*, dont les systèmes ou serveurs fonctionnant à partir d'Unix, Windows NT, Windows 95, MacOs, OS/2, etc. Voir *Sécurité Optimale, supra* note 208 aux pp. 578-79. Pour un exemple d'informations données lors d'une session Unix, voir : E. Amoroso, *Intrusion Detection*, Sparta (NJ), Intrusion.Net Books, 1999, aux pp. 136, 139-40 [ci après *Intrusion Detection*].

239 *Sécurité Optimale, supra* note 208 à la p. 59.

240 Voir le service de recherche par nom de personne d'Alta Vista, en ligne : <http://www.altavista.com> (date d'accès : 24 avril 2001).

241 Voir le service de recherche par nom de personne de World Pages, en ligne : <http://www.worldpages.com> (date d'accès : 24 avril 2001).

242 *Sécurité Optimale, supra* note 208 à la p. 580.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

vérifie son courriel et à partir d'où le branchement est établi. Il sera ainsi possible de connaître le profil d'utilisation d'Internet d'un utilisateur[243]. Le service *finger* peut entraîner des risques considérables pour la sécurité et servir à compromettre des informations relatives aux utilisateurs. Par conséquent, il est recommandé de ne pas offrir ce service au monde extérieur[244].

Intranet et extranet sont-ils des petits frères d'Internet?

Étant donné le développement important d'Internet, il devient de plus en plus logique d'utiliser ses ressources lorsqu'on veut établir un réseau de type LAN, MAN ou WAN, ne serait-ce que pour la réduction des coûts d'exploitation et d'implantation. Cela évite notamment de devoir bâtir un réseau de toute pièce, impliquant la mise en place d'une infrastructure composée de câbles, d'ordinateurs, de routeurs etc.

Lorsqu'on construit un réseau de type LAN, MAN ou WAN, c'est-à-dire un réseau privé selon les normes d'Internet, on construit un « Internet interne », intra réseautage, ou intranet. Contrairement à Internet, seuls les membres autorisés ont le droit d'exploiter les ressources d'un intranet[245].

Les extranets sont des intranets qui utilisent Internet comme support pour interagir avec le monde extérieur, comme par exemple avec leurs clients, leurs fournisseurs et leurs partenaires commerciaux. Seuls les membres autorisés ont le droit d'exploiter les ressources d'un extranet[246]. Un intranet et un extranet ne correspondent finalement qu'à une façon d'utiliser Internet comme ressource réseau ou infrastructure.

B. Le protocole TCP/IP

Les ordinateurs branchés à Internet dialoguent en utilisant un langage de communication commun appelé TCP/IP (*Transmission Control Protocol/Internet Protocol*). Les protocoles[247] de communication de la famille TCP/IP assurent l'interopérabilité entre les ordinateurs hétérogènes qui sont reliés à Internet. En fait, TCP/IP supporte un grand nombre de protocoles de communication spécialisés dans différentes applications, tels FTP (*File Transfer Protocol*), SMTP (*Simple Mail Transfer Protocol*), NNTP (*Net News Transfer Protocol*), PPP/SLIP (*Point-to-Point Protocol/Serial Line Internet Protocol*), HTTP (*Hyper Text Transfer Protocol*), POP3 (*Post Office Protocol*, version 3), *Telnet*, *finger*, etc. TCP/IP est également implémenté dans les systèmes d'exploitation tels Windows 95-98, etc[248]. Nous verrons plus en détail les différents protocoles de communication lorsque nous traiterons des contextes particuliers de communication.

La partie TCP du protocole offre aux applications, décrites plus haut, un service de transport de données fiable entre deux ordinateurs branchés à Internet. Il reçoit les données que des

---

[243] *Ibid*. aux pp. 581-82.
[244] *Ibid*. à la p. 363. Voir aussi *Intrusion Detection*, *supra* note 238 à la p. 140.
[245] *Les réseaux*, *supra* note 136 à la p. 23 ; *Le guide de l'internaute, supra* note 136 aux pp. 61, 556.
[246] *Les réseaux*, *supra* note 136 aux pp. 24-25 ; *Le guide de l'internaute 2000*, *supra* note 136 aux pp. 61, 554.
[247] Un protocole de communication est une convention qui spécifie les règles d'échange d'information entre deux machines. Il existe un grand nombre de protocoles, dont certains sont normalisés au niveau international par des organismes spécialisés de normalisation. Voir *Internet*, *supra* note 214 à la p. 12.
[248] *Internet*, *supra* note 214 aux pp. 11-12, 19-20.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

applications, telles que FTP ou SMTP souhaitent transférer. Il segmente ces données en une série de paquets appelés datagrammes ou paquets IP. Il comporte également une somme de contrôle d'erreur qui permettra de vérifier que le datagramme n'est pas transmis par erreur[249]. Le protocole IP offre un service d'acheminement des paquets d'informations. Il assure la livraison des paquets pour toutes les applications nommées plus haut.[250] Le protocole IP gère en quelque sorte le routage des paquets dans Internet. Il s'agit en fait de ce qui constitue l'activité principale d'Internet :

> « *Recall, in particular, that Internet activity consists of IP packets arranged into streams that are routed in connectionless manner between clients and servers* »[251].

Lorsque le protocole IP reçoit des datagrammes, il leur ajoute son en-tête IP qui contient l'adresse des deux machines , soit la source et la cible, ainsi qu'une somme de contrôles qui permettra de vérifier que l'en-tête IP n'est pas altérée en cours de transmission. Lorsque le paquet IP est transmis dans le réseau, il est aiguillé par les ordinateurs faisant office de routeurs IP dans la base de l'adresse de la station de destination[252]. Cela signifie, notamment, que le protocole IP permettra la recherche du meilleur chemin à emprunter pour accéder à l'ordinateur cible. Si un ordinateur disparaît du réseau, les informations trouveront un autre chemin pour parvenir à leur destination[253].

Le protocole ICMP (*Internet Control Message Protocol*) gère les messages d'erreur et de contrôle qui sont transmis entre deux ordinateurs ou plus durant le processus de transfert de paquets d'informations sous TCP/IP. Il leur permet de partager ces informations. À cet égard, ICMP est essentiel pour diagnostiquer les problèmes réseau, comme l'arrêt d'un ordinateur hôte, et la congestion ou panne d'une passerelle Internet. Un utilitaire appelé *ping* utilise le protocole ICMP pour déterminer si une machine distante est opérationnelle. Lorsque l'utilisateur effectue un *ping*, une série de paquets est transmise depuis sa machine vers celle de l'hôte distant. Ces paquets sont ensuite renvoyés à l'émetteur. Si aucun retour n'est enregistré, l'utilitaire affiche généralement un message d'erreur indiquant que l'hôte distant

---

249 *Ibid*. à la p. 13. Voir aussi *Protégez-vous sur Internet, supra* note 207 aux pp. 70-72, 74.

250 *Sécurité Optimale, supra* note 208 à la p. 55.

251 *Intrusion Detection*, *supra* note 238 à la p. 123.

252 *Internet*, *supra* note 214 à la p. 13. Le programme Unix *TCP/IP traceroute*, indique la route entre une adresse IP d'une machine et l'adresse IP d'un hôte distant. Il sera donc possible de connaître toutes les adresses IP empruntées par un ou des paquets d'informations entre deux points. Plusieurs systèmes d'exploitation contiennent un programme pour effectuer des requêtes de type *traceroute*. Dans Windows de Microsoft, le programme se nomme *tracert*. Il sera ensuite possible, à l'aide du service WHOIS, de connaître le nom des hôtes correspondants aux adresses IP révélées. On obtiendra ainsi l'identité de tous les domaines américains non militaires, les noms des propriétaires de domaine, le nom du contact technique pour chaque domaine et les adresses de serveurs de noms pour chaque domaine. Ceci pourrait notamment être utile pour connaître les différentes juridictions empruntées par le paquet d'information. Voir *Sécurité Optimale, supra* note 208 aux pp. 496, 596, 763. Voir aussi E. Casey, *Digital Evidence and Computer Crime*, San Diego (CA), Academic Press, 2000, aux pp. 104, 128 [ci après *Digital Evidence*]. Voir finalement *Intrusion Detection*, *supra* note 238 aux pp. 136-37. Un utilisateur pourra facilement procéder à une requête de type WHOIS, notamment par le biais des sites Web suivants : *ARIN*, en ligne : <http://www.whois.arin.net/whois/arinwhois.html> (date d'accès : 5 septembre 2001) et *Network Information Center*, en ligne : <http://www.internic.net> (date d'accès :5 septembre 2001).

253 *Protégez-vous sur Internet, supra* note 207 à la p. 72. Voir aussi *Sécurité Optimale, supra* note 208 aux pp. 55-56.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

n'est pas opérationnel[254]. Cette fonction pourrait notamment servir à savoir si un utilisateur est branché ou non à Internet et quel service il utilise.

C. L'adresse IP

Pour être en mesure d'identifier un ordinateur dans Internet, celui-ci doit posséder une adresse unique. Comme nous l'avons vu, le protocole TCP/IP sert à effectuer cet adressage. C'est ce que l'on appelle l'adresse IP. Sans entrer trop à fond dans les détails techniques, il suffit de retenir que chaque ordinateur lié à Internet possède une adresse IP numérique unique. Il est nécessaire de posséder une adresse IP afin de le distinguer des autres ordinateurs connectés au réseau et d'être en mesure d'échanger n'importe quelle sorte d'information dans le réseau[255]. L'adresse IP est à la base de l'utilisation des ressources Internet[256], même si on fait présentement face à une pénurie d'adresses[257]. L'adresse IP d'un ordinateur est reconnue pour être le point de départ de l'établissement de l'identité d'un utilisateur d'Internet[258]. Dans ce contexte, un fsI pourra notamment procéder à la surveillance des différentes adresses IP visitées par un abonné ou de celles dont il a reçu une communication. Cette surveillance s'apparente à la surveillance des numéros composés et reçus de la part d'un abonné, effectuée par une compagnie de téléphone[259].

L'adresse Internet d'un appareil ou nom logique

En plus de l'adresse IP numérique, les ordinateurs branchés à Internet possèdent également un nom logique[260]. Il en est ainsi parce qu'il est plus aisé de se souvenir d'un nom que d'un numéro. L'adresse Internet d'un ordinateur est composée du nom de domaine, du nom du ou des réseaux, le cas échéant, et du nom propre de l'appareil. L'adresse Internet pourrait ressembler à ceci : « abc.justice.gc.ca » où « abc » serait le nom donné à l'ordinateur, « Justice » serait le nom de réseau (ministère fédéral de la justice), « gc » serait le nom du

---

254 *Sécurité Optimale, supra* note 208 à la p. 55.

255 A. Bélanger et J.-H. Roy, *Internet le guide 2000*, 5e éd., Montréal, Québec Science, 2000, à la p. 80 [ci après *Internet le guide 2000*] ; *Le guide de l'internaute 2000*, *supra* note 136 aux pp. 69-70 ; *Internet*, *supra* note 214 à la p. 15.

256 Les utilisateurs branchés à Internet par modem téléphonique à un fournisseur de Services Internet se voient assigner dynamiquement une adresse *IP* chaque fois qu'ils se branchent sur le réseau, c'est-à-dire une adresse IP différente à chaque connexion. C'est la plupart du temps ce qui se produit lorsqu'il y à connexion à haute vitesse par modem câblé. Par contre, dans le cas des ordinateurs qui sont reliés en permanence à Internet, dans des réseaux d'entreprise notamment, ou dans des universités, il y a de fortes probabilités que l'adresse IP soit toujours la même. Il s'agit alors d'une adresse IP statique ou fixe. Voir *Le guide de l'internaute 2000, supra* note 136, à la p. 60 ; *Les réseaux*, *supra* note 136 aux pp. 259-60 ; *Internet le guide 2000*, *supra* note 255 à la p. 80.

257 En effet, lorsque le schéma d'adressage à 32 bits, permettant un peu plus de 4 milliards d'adresses, a été créé, personne n'avait entrevu que l'on viendrait à en manquer. Il semble que *IPng* (*IP next generation*), permettra de régler le problème du manque d'adresse par un schéma d'adressage à 128 bits, soit 2^{128} adresses, comparativement à 2^{32} adresses. *Les réseaux*, *supra* note 136 aux pp. 51-55 ; *Internet*, *supra* note 214 à la p. 37. L'augmentation du nombre d'adresses *IP* possibles fait en sorte qu'elles ne serviront plus nécessairement à identifier un ordinateur. Donc dans le cas d'une adresse *IP* à 128 bits, il sera moins clair qu'elle correspond à un ordinateur en particulier. Pour cette dernière question, voir *Intrusion Detection*, *supra* note 238 à la p. 126.

258 *Ibid*. à la p. 125.

259 *Ibid*.

260 *Internet*, *supra* note 214 aux pp. 15-16.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

domaine (gouvernement fédéral canadien) et « ca » le nom de domaine de dernier niveau localisant l'ordinateur au Canada[261].

Quant aux utilisateurs qui accèdent à Internet par le biais d'un fsI, les ordinateurs possèdent une adresse générique qui peut changer à chaque entrée dans le réseau. L'adresse attribuée pourrait ressembler à ceci : « ppp-021 » fournisseur Internet où « ppp-021 » serait le numéro séquentiel du modem qu'utilise le fournisseur[262].

Le paquet IP d'information ou datagramme

Le paquet d'informations est ce qui circule dans les fils de télécommunication[263]. On appelle également le paquet d'informations un datagramme qui contient des en-têtes qui gèrent l'adressage, la correction d'erreurs, les sommes de contrôles et des données à transmettre dans le réseau[264].

L'analogie de l'envoi d'une lettre est utilisée pour mieux comprendre le fonctionnement de l'envoi d'un paquet d'informations. Il convient ici de reprendre les propos de Sohier :

> « *Après avoir rédigé la lettre, vous l'insérez dans une enveloppe que vous cachetez. Vous prenez bien soin d'écrire l'adresse du destinataire au recto, et finalement, vous inscrivez votre propre adresse au verso. Un paquet d'information fonctionne selon le même principe. Lorsque vous faites parvenir un fichier à un collègue dans une autre entreprise, des paquets sont formés. Chaque paquet contient les deux adresses et un morceau du fichier* »[265].

L'information qui circule dans les réseaux est découpée parce qu'elle permet à plus d'un flot de données de parcourir le même support au même moment. Elle permet également la correction des erreurs et l'envoi des données d'un ordinateur à un autre en empruntant des routes multiples en fonction de l'ouverture de celle-ci à un instant précis[266].

Hayden précise le fonctionnement de l'empaquetage des données :

> « *L'empaquetage des données consiste à les scinder en parts égales, afin de les transmettre sur un réseau. La somme de contrôle permet de déterminer si toutes les données sont bien dirigées. Lorsque celles-ci sont empaquetées, l'ordinateur compte le nombre de « 1 » et de « 0 » qu'elles contiennent et attribue leur numéro qu'il inclut au paquet.*
>
> *La route qu'empruntent les données ainsi que l'ordre dans lequel elles arrivent n'ont donc aucune importance, pourvu qu'elles parviennent toutes à destination. L'ordinateur peut les assembler à partir de la somme de contrôle*

---

[261] *Le guide de l'internaute 2000, supra* note 136, aux pp. 61-62 et *Droit du Cyberespace*, *supra* note 8 aux pp. 17-1 à 17-3.
[262] *Ibid*. à la p. 62.
[263] *Ibid*. à la p. 63.
[264] *Les réseaux*, *supra* note 136 à la p. 377.
[265] *Le guide de l'internaute 2000, supra* note 136 aux pp. 63-64 ; *Intrusion Detection*, *supra* note 238 à la p. 129.
[266] *Les réseaux*, *supra* note 136 à la p. 27.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

et des numéros de séquence qui ont été attribués à chaque paquet de données »[267].

Un ordinateur peut conséquemment traiter un grand nombre de paquets de données en provenance de plusieurs machines, parce que chaque paquet, un peu comme l'analogie de l'envoi postal précédent, dispose d'une adresse de retour, c'est-à-dire de l'adresse d'origine des paquets, d'une adresse de destination et d'un numéro de séquence qui assure que les données sont exemptes d'erreurs[268]. De plus, on retrouvera dans le paquet d'information IP le numéro de port IP utilisé pour le transfert de fichier[269].

L'analogie du courrier est importante pour la bonne compréhension du fonctionnement du protocole TCP/IP. Compte tenu de la protection en matière de vie privée généralement offerte en matière de communication effectuée par le biais du téléphone, il convient de faire la distinction entre une communication téléphonique traditionnelle et une communication informatique réseau. Une communication téléphonique utiliserait un réseau à circuits commutés alors qu'une communication TCP/IP utiliserait un réseau à paquets d'information commutés. Il convient ici de reprendre une citation de D.E. Comer, reprise dans l'ouvrage de Casey :

> « *Circuit-switched networks operate by forming a dedicated connection (circuit) between two points. The US telephone system uses circuit switching technology – a telephone call establishes a circuit from the originating phone through the local switching office, across trunk lines, to a remote switching office, and finally to the destination telephone. […] The advantage of circuit switching lies in its garanteed capacity : once a circuit is established, no other network activity will decrease the capacity of the circuit. One disadvantage of circuit switching is cost : circuit costs are fixed, independent to traffic. For example, one pays a fixed rate for a phone call, even when the two parties do not talk.*
>
> *Packet-switched networks, the type used to connect computers, take an entirely different approach […] The network hardware delivers the packets to the specified destination, where software reassembles them into a single file again. The chief advantage of packet-switching is that multiple communications among computers can proceed concurrently, with intermachine connections shared by all pairs of machines that are communicating. The disadvantage, of course, is that as activity increases, a given pair of communicating computers receives less of the network capacity. That is, whenever a packet-switched network becomes overloaded, computers using network must wait before they can send additional packets* »[270]

La communication téléphonique établirait en quelque sorte un canal de communication (un circuit), alors que celle effectuée par le biais du protocole TCP/IP n'en établirait pas. Ces distinctions étant faites, il convient donc maintenant de traiter du port IP. On pourrait

---

[267] *Ibid*. aux pp. 27-28.
[268] *Ibid*. à la p. 28.
[269] *Le guide de l'internaute 2000, supra* note 136 aux pp. 64-65.

[270] *Digital Evidence*, *supra* note 252 à la p. 123.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

conséquemment avancer qu'une communication, transitant par un réseau à circuit commuté (par ex. le téléphone), favoriserait plus l'existence d'une quelconque expectative raisonnable de vie privée, qu'une communication transitant par un réseau à paquets commutés (par ex. Internet). Par contre, dans biens des cas, il y aura confusion entre les deux types de réseaux lors de l'établissement d'un branchement Internet. Ce sera notamment le cas lors d'un branchement à Internet à partir d'une ligne téléphonique. Nous en reparlerons plus loin.

Le numéro de port IP et le port TCP/IP

Le numéro de port IP sert à différencier le trafic dans le réseau. Sohier reprend l'analogie des ondes radio pour mieux illustrer le concept :

> « […] *Pensez à un poste de radio qui a la capacité de recevoir toutes les ondes radio. De la même façon, un serveur peut offrir plusieurs services à la fois. Chacun de ces services écoute son propre port IP. Il répond seulement lorsque des paquets marqués du port approprié lui sont acheminés. Les autres services ignoreront ces paquets d'information* »[271].

Nous verrons plus loin, lors de l'étude des contextes particuliers, plusieurs applications TCP/IP ou moyens de communication. Chacun de ces moyens de communication utilise des ports IP de communication spécifique[272]. Il s'agit donc d'un chiffre indiquant le canal logique utilisé par une transmission TCP/IP entre deux ordinateurs. Ce numéro est utilisé pour identifier le type d'application exploité[273]. Chaque datagramme ou paquet IP contiendra donc, d'abord, le numéro de port auquel il est destiné et ensuite, les informations à transmettre à ce port[274].

Beaucoup d'applications TCP/IP peuvent être utilisées dans Internet. La plupart d'entre elles fonctionnent selon le mode client-serveur. À chaque demande de connexion par une machine client, un programme serveur ou application, qui communique ensuite avec la machine client, est démarré. Pour faciliter ce processus, chaque application, comme par exemple FTP ou SMTP, reçoit un numéro de port IP unique. Nous avons vu précédemment les numéros de port correspondant à chaque application. L'application est donc liée à ce numéro. Lorsqu'une demande de connexion est faite, le serveur vérifiera le numéro de port IP demandé par le client. Ce numéro, comme nous l'avons vu, fait partie intégrante du paquet d'information IP transmis par la machine client distante. Lorsqu'une requête est faite sur un port, l'application correspondante se trouvant sur le serveur est lancée. Inetd est le programme se trouvant sur le serveur qui a la charge de lancer les applications demandées par les ordinateurs clients. Inetd attend donc les requêtes de connexion provenant du réseau. Lorsqu'il en reçoit une, il l'évalue. Cela lui permet de déterminer le service concerné par la requête et si la machine distante souhaite, par exemple communiquer avec FTP, soit le port de communication TCP/IP

---

[271] *Le guide de l'internaute 2000, supra* note 136 à la p. 64.

[272] Les numéros de port IP seront généralement les suivants : le numéro 21 pour *FTP*, 23 pour Telnet, 25 pour *SMTP* (envoi de courriel), 79 pour *finger*, 80 ou 81 pour *HTTP* (Web), 110 pour *POP3* (réception de courriel), 119 pour *NNTP* (groupes de nouvelles *Usenet*), la session de bavardage *IRC*, les 6667 6670 et le service ICQ, le port 4000. S. McClure, *et al.*, *Hacking Exposed : Network Security Secrets and Solutions*, 2e ed., Berkeley (CA), Osborne/McGraw-Hill, 2001, aux pp. 658-60 [ci après . *Hacking Exposed*]

[273] *Le guide de l'internaute 2000, supra* note 136 à la p. 558.

[274] *Protégez-vous sur Internet, supra* note 207 à la p. 74.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

numéro 21 ou SMTP, soit le port de communication TCP/IP numéro 25. Si c'est le cas, inetd démarre le processus serveur FTP ou SMTP, selon le cas, qui peut ainsi traiter la demande[275].

Il est important de bien saisir toute cette mécanique pour mieux comprendre le fonctionnement d'un scanner de port TCP/IP à l'égard des services exécutés à un moment précis sur un serveur. À l'instar des balayeurs d'ondes permettant d'écouter les conversations téléphoniques cellulaires ou les ondes radio, le scanner permet à un utilisateur de connaître à distance certaines informations à propos de tiers qui communiquent. Là s'arrête la comparaison. Outre la fréquence utilisée pour communiquer, les scanners d'ondes radio permettent de connaître le contenu d'une conversation, si celle-ci est effectuée en clair. Le scanner de port TCP/IP permet plutôt d'interroger à distance les ports TCP/IP de l'hôte cible et enregistre les réponses de celui-ci. De cette façon on ne prend pas connaissance du contenu même de la communication, on recueille plutôt des informations relativement aux services exécutés au moment du « *scanning* », aux utilisateurs propriétaires de ces services, à la disponibilité des connexions anonymes et si certains services réseaux requièrent une authentification[276].

Outre le fait qu'il soit en mesure d'indiquer quel service est utilisé à un moment donné par un ordinateur distant, le scanner est utile pour les administrateurs de réseaux car il permet notamment de détecter les faiblesses d'un réseau. Par contre, pour une personne malveillante, le scanner pourra faciliter une intrusion non autorisée dans un système. Quant aux organismes d'application de la loi, il pourrait leur fournir des informations utiles pour une enquête sur une multitude d'entités exploitant un serveur notamment quant à l'identité de ses membres et les applications TCP/IP disponibles et/ou en fonction. Il va sans dire que cet outil permet de *scanner* efficacement une multitude d'adresses IP à la fois. Il convient ici de citer un passage de l'ouvrage d'un *hacker* anonyme qui reprend une analogie qui décrit bien l'utilisation d'un scanner :

> « *La question de la légalité des scanners fait l'objet de débats incessants. Certains avancent que « scanner » une cible revient à utiliser un pied de biche pour tenter d'ouvrir les portes et fenêtres d'une maison. Il compare cette activité à une intrusion illégale. D'autres pensent que le simple fait de maintenir un site est une forme de consentement implicite à une attaque, si l'on considère qu'une adresse de réseau suit le même principe qu'un numéro de téléphone, à savoir que n'importe qui est en droit de la composer* »[277].

Deux concepts émanant de cette analogie rejoignent le droit pénal en matière d'expectative raisonnable de vie privée : l'intrusion illégale et l'invitation implicite. Dans *Kokesch*, la Cour suprême du Canada a déterminé que les observations visuelles, olfactives et auditives effectuées par des policiers sur le terrain d'une propriété constituaient une perquisition périphérique. Cette intrusion non justifiée de la police a été considérée comme une perquisition abusive, et ce, même si on ne s'était pas introduit dans la maison d'habitation de l'accusé se trouvant sur le terrain[278]. Des agents de l'État utilisant un *scanner* sur un serveur ou ordinateur distant pourraient, théoriquement, commettre une perquisition périphérique illégale au sens de l'arrêt *Kokesch*, si l'analogie de l'intrusion est retenue.

---

[275] *Sécurité Optimale, supra* note 208 aux pp. 58-59 ; *Digital Evidence, supra* note 252 aux pp. 122-24.
[276] *Sécurité Optimale, supra* note 208 à la p. 167.
[277] *Ibid*. aux pp. 168-69.
[278] *Supra* note 57.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

Dans l'arrêt *Evans*[279], la Cour suprême du Canada a dû se pencher également sur la question de la fouille olfactive effectuée par un policier, mais dans un contexte différent de celui de l'arrêt *Kokesch*. Suite à une enquête jusque-là infructueuse, qu'ils avaient entreprise à la suite de renseignements obtenus d'un informateur anonyme, des policiers en tenue civile ont frappé à la porte des appelants, se sont identifiés, ont senti une odeur de marijuana et ont immédiatement arrêté les appelants. Ils ont gardé les lieux, où se trouvaient plusieurs plants de marijuana. Un mandat de perquisition a ensuite été demandé, puis exécuté. Les appelants ont été déclarés coupables de possession de marijuana en vue d'en faire le trafic et leur appel a été rejeté. Une des questions en litige était de savoir si la conduite des policiers, qui étaient à la recherche d'une odeur de marijuana lorsqu'ils ont frappé à la porte des appelants, constituait une «fouille ou perquisition» au sens de l'art. 8 de la *Charte canadienne*.

Le juge Sopinka pour la majorité a déterminé que les gens ont une attente raisonnable en matière de vie privée qu'ils peuvent opposer aux personnes qui s'approchent de leur demeure. Ils peuvent également y renoncer dans le but de faciliter la communication avec le public. Quiconque, y compris les agents de l'État, viole les conditions de cette renonciation et s'approche de la porte dans un but non autorisé, outrepasse les conditions de l'invitation implicite à frapper à la porte et devient un intrus. Par conséquent, lorsque des policiers s'approchent d'une maison d'habitation dans le but de recueillir des éléments de preuve contre l'occupant, ils procèdent alors à une «fouille ou perquisition» dans la demeure de l'occupant. Des agents de l'État utilisant un *scanner* sur un serveur ou un ordinateur distant pourraient, théoriquement, commettre une fouille ou perquisition illégale au sens de l'arrêt *Evans*, si l'analogie de l'invitation implicite est retenue.

Le domaine et le serveur de noms de domaine

Le domaine est l'ensemble des utilisateurs d'un site Internet ou d'une organisation. Toutes les adresses IP des utilisateurs de cette organisation possèdent les deux mêmes premiers nombres. Si le domaine du gouvernement canadien est « gc.ca », toutes les adresses des utilisateurs et des ordinateurs auront ce suffixe comme premiers chiffres. Donc si « gc.ca » correspond à « 123.456 », l'adresse IP d'un ordinateur se trouvant au gouvernement canadien sera « 123.456.XXX.XXX ». Toutes les adresses IP du domaine « gc.ca » commenceront donc par « 123.456 »

Dans « gc.ca », « gc. » indique gouvernement canadien et « ca » indique qu'il s'agit d'une ressource canadienne. Il s'agit du nom de domaine que l'on doit traduire ou lire de droite à gauche[280].

Le serveur de noms de domaine est un ordinateur contenant la liste de tous les domaines principaux d'Internet, la table des adresses Internet ainsi que les adresses IP correspondantes de tous les utilisateurs de ce site[281].

On retrouve un serveur de noms de domaine dans la majorité des sites Internet. Ce serveur agit en quelque sorte comme un portier du site[282]. Il aidera notamment à trouver une adresse

[279] *Evans*, *supra* note 59.
[280] *Le guide de l'internaute 2000, supra* note 136 aux pp. 65-67, 553. Il existerait présentement plus de 9 millions de noms de domaine dans Internet.
[281] *Ibid*. à la p. 66.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

d'un ordinateur se trouvant dans son domaine lorsqu'une requête lui parviendra d'un autre serveur de noms de domaine. Dans la mesure où le domaine est identifié, toutes les adresses IP correspondantes pourront facilement y être reliées. Dans ce contexte, le niveau d'expectative raisonnable de vie privée à l'égard de l'adresse IP se trouvant dans un domaine, sera elle-même tributaire de celle du domaine. Il en est de même pour les numéros correspondants au nom de domaine.

Section IV - Le contexte du branchement à Internet

Il existe plusieurs façons de se brancher à Internet. Les moyens techniques pour s'y brancher varieront grandement ainsi que les lieux à partir desquels on s'y branchera. La décision de la Cour suprême américaine dans *Reno c. ACLU*, traite de la notion de l'accès ou branchement à Internet :

> « *Individuals can obtain access to the Internet from many different sources, generally hosts themselves or entities with a host affiliation. Most colleges and universities provide access for their students and faculty; many corporations provide their employees with access through an office network; many communities and local libraries provide free access; and an increasing number of storefront "computer coffee shops" provide access for a small hourly fee. Several major national "online services" such as America Online, CompuServe, the Microsoft Network, and Prodigy offer access to their own extensive proprietary networks as well as a link to the much larger resources of the Internet. These commercial online services had almost 12 million individual subscribers at the time of trial* »[283].

L'énoncé conjoint des faits en première instance dans *ACLU c. Reno*, décrit deux méthodes principales de branchement à Internet qui seraient sous-jacentes à tout autre type de branchement :

> « *12. Individuals have a wide variety of avenues to access cyberspace in general, and the Internet in particular. In terms of physical access, there are two common methods to establish an actual link to the Internet. First, one can use a computer or computer terminal that is directly (and usually permanently) connected to a computer network that is itself directly or indirectly connected to the Internet. Second, one can use a "personal computer" with a "modem" to connect over a telephone line to a larger computer or computer network that is itself directly or indirectly connected to the Internet. As detailed below, both direct and modem connections are made available to people by a wide variety of academic, governmental, or commercial entities* » [note omise][284].

Dans certains cas, les moyens techniques utilisés pour se brancher à Internet seront tributaires des lieux de branchement; dans d'autres cas, ils en seront indépendants. La technique utilisée pour le branchement pourra influencer le niveau d'expectative raisonnable de vie privée d'un

---

[282] *Ibid*.
[283] *Supra* note 1 à la p. 850.
[284] *ACLU c. Reno, supra* note 196 à la p. 832.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

utilisateur. Nous traiterons plus loin des détails des diverses techniques ou modes de branchement.

L'endroit à partir duquel le branchement sera effectué influera également sur le niveau d'expectative raisonnable de vie privée, en ce sens qu'il faudra s'interroger à chaque fois sur la nature de l'interaction entre un utilisateur et le lieu de l'ordinateur utilisé pour effectuer le branchement. Plus ce lieu est public ou échappe au contrôle de l'utilisateur, moins la connexion sera privée. Il convient donc de traiter du branchement à Internet par rapport à la technique utilisée et par rapport au lieu de l'établissement de la connexion.

Le branchement à Internet par rapport à la technique utilisée

– Accès à Internet par le biais d'un réseau TCP/IP

Il s'agit du type de connexion à Internet le plus répandu. Chaque ordinateur d'un réseau à Internet a la possibilité de s'y brancher. La connexion au réseau s'effectuera par le biais d'une carte réseau installée dans chaque ordinateur. Le lien avec Internet se fait par un aiguilleur qui se trouve quelque part dans le réseau. La localisation géographique ou logique de l'aiguilleur n'a pas d'importance[285].

Ce n'est donc pas l'utilisateur qui est relié à Internet, mais le réseau dans lequel il se trouve. Ce branchement est effectué par l'aiguilleur.

Le type de connexion pour relier l'aiguilleur à Internet peut varier. Il pourra s'agir d'une connexion téléphonique haute vitesse ou d'une liaison par câble haute vitesse. La connexion utilisée supportera normalement un haut débit et sera capable de traiter un volume élevé de données compte tenu du nombre élevé d'utilisateurs.

Cette configuration et cet accès seront généralement mis en œuvre dans une organisation quelconque, telle une société ou une institution d'enseignement.

– Accès à Internet par le biais du réseau téléphonique

Dans la majorité des cas, il s'agit simplement de posséder un ordinateur et un modem pour communiquer avec un fsI[286]. Le fsI sera branché à Internet par le biais d'un fournisseur d'accès régional plus important. L'exposé conjoint des faits dans *ACLU c. Reno* décrit le contexte général d'un branchement fait par le biais du réseau téléphonique :

> « *18. Individuals can also access the Internet through commercial and non-commercial "Internet service providers" that typically offer modem telephone access to a computer or computer network linked to the Internet. Many such providers -- including the members of plaintiff Commercial Internet Exchange*

[285] *Le guide de l'internaute 2000, supra* note 136 aux pp. 70-71 ; *Les réseaux*, *supra* note 136 aux pp. 256-57.

[286] Nous le rappelons, un fsI ou fournisseur de service Internet, est une entreprise qui vend des accès à Internet. On dit aussi fournisseur d'accès Internet. *Les réseaux*, *supra* note 136 à la p. 254. Les accès seront offerts sous forme d'abonnements de types différents à des particuliers ou des entreprises. Voir aussi *Le guide de l'internaute 2000, supra* note 136 à la p.71.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

Association -- are commercial entities offering Internet access for a monthly or hourly fee. […] »[287]

L'utilisateur se sert donc d'une ligne téléphonique normale ou réservée aux communications effectuées par le biais d'Internet. Il s'agit ici d'une approche client-serveur. L'utilisateur (client) entrera en communication avec le fournisseur de service Internet (serveur) en utilisant un logiciel de connexion qui communiquera à l'aide du protocole SLIP/PPP (*Serial Line Internet Protocol/Point to Point Protocol*)[288]. Le serveur qui reconnaîtra le client lui attribuera une adresse IP pour la session demandée. Il s'agit d'une attribution dynamique d'adresse IP, en ce sens qu'elle variera à chaque nouvelle demande de connexion[289]. Le protocole SLIP/PPP fait partie des protocoles utilisés ou reconnus par le protocole TCP/IP[290].

L'utilisateur utilisera généralement un modem pour être en mesure d'établir la connexion client-serveur par l'entremise du réseau téléphonique. Il s'agira d'une connexion Internet normale ou à basse vitesse[291]. La connexion avec le fsI étant établie, un utilisateur pourra se servir des ressources offertes par Internet.

Dans tous les cas où une communication est établie entre un client et un serveur par l'entremise d'une ligne téléphonique, l'aiguilleur ou le serveur de lien Internet se trouvera ailleurs qu'au domicile de l'utilisateur. Le serveur se retrouvera le plus souvent chez le fsI. L'accès par le fsI à Internet même s'effectuera de différentes manières, selon le fsI et selon le lien entre celui-ci et le fournisseur régional d'accès Internet.

– Accès à Internet par le biais du câble

Pour ce type d'accès, on utilise le réseau de câblodistribution pour accéder à Internet. Le réseau téléphonique n'a donc pas à être utilisé. L'avantage principal de l'utilisation de ce type

---

[287] *ACLU c. Reno, supra* note 196 à la p. 833.

[288] *Le guide de l'internaute 2000, supra* note 136 aux pp. 69, 71-72.

[289] *Ibid*. à la p. 72 ; *Les réseaux, supra* note 136 aux pp. 255-60.

[290] *Le guide de l'internaute 2000, supra* note 136 à la p. 7 ; *Les réseaux*, *supra* note 136 à la p. 255. L'assignation dynamique d'adresse IP rend, en principe, l'identification de la personne se trouvant derrière celle-ci plus difficile. *Intrusion Detection*, *supra* note 238 à la p. 124.

[291] Il existe d'autres utilisations possibles du réseau téléphonique pour accéder à Internet, mais cette fois à haute vitesse. La façon d'y accéder sera semblable à la connexion SLIP/PPP où l'on utilise un modem pour entrer en communication avec un fsI. Dans le cas des connexions à haute vitesse, une carte réseau supplémentaire sera généralement requise en plus du modem. Il s'agit des accès par lien DSL (Digital Subscriber Line) ou ADSL (Asymetric Digital Subscriber Line) ou en français un lien LNPA (Ligne numérique à paire asymétrique). Voir notamment Sympatico édition haute vitesse, en ligne : <http://www.whv.sympatico.ca> (date d'accès : 20 juillet 2001). Ces services à haute vitesse permettent notamment d'utiliser Internet au même moment où, sur la même ligne téléphonique, on l'utilise pour parler. Dans d'autres cas on aura besoin, en plus d'un modem, d'une seconde ligne téléphonique entièrement dédiée à l'accès Internet. Il s'agira d'une ligne téléphonique numérique à haute vitesse de transmission plus rapide. On aura également besoin dans ce cas d'un autre périphérique en plus d'un modem, soit un routeur. Il semble par contre que cette dernière technologie soit en déclin pour le service résidentiel, notamment en raison des coûts rattachés à son implémentation à grande échelle. Sohier, Danny J., *Le guide de l'internaute 2000,* Montréal, Les éditions logiques, 2000 aux pp. 71-72, 80-81 ; *Internet le guide 2000, supra* note 255 aux pp. 10-11. De plus, dans la plupart des cas, vue la relative étendue des services haute-vitesse, on pourra tirer une inférence de proximité entre le lieu du serveur Internet du Fournisseur de Service Internet et le lieu où se trouve l'ordinateur du client. Ce sera notamment le cas du service LNPA, où il est recommandé d'avoir un serveur près du commutateur téléphonique. Sur la question de la proximité du commutateur téléphonique. *Internet le guide 2000, supra* note 255 à la p. 10.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

d'accès est le fait que la ligne téléphonique n'a pas à être utilisée lors d'une connexion à Internet[292]. L'accès par câble est également généralement plus rapide et plus stable que l'accès téléphonique ordinaire et à haute vitesse[293].

Pour se brancher au réseau, une communication est établie entre l'ordinateur de l'utilisateur (client) et l'ordinateur du fsI (serveur). La communication est établie par le biais d'un modem et d'une carte réseau installés sur l'ordinateur du client[294]. Il s'agit de la connexion haute vitesse la plus populaire[295].

L'ordinateur du client est doté d'une adresse Internet pour la durée de la connexion par le fsI. Il s'agit de l'attribution dynamique d'une adresse *IP*, c'est-à-dire qu'elle changera à chaque connexion par opposition à une connexion à adresse *IP* fixe qui sera toujours la même[296].

Comme dans le cas d'une connexion par le biais d'une ligne téléphonique, l'aiguilleur Internet se trouvera généralement sur les lieux du fsI[297].

– Accès à Internet par le biais d'un satellite

L'accès à Internet est également accessible par le biais d'un satellite. Il y a la connexion unidirectionnelle et bidirectionnelle[298]. La connexion unidirectionnelle utilise une technologie hybride. Nous disons hybride en ce sens qu'elle utilisera en partie un satellite et en partie le réseau téléphonique pour communiquer avec Internet.

Il faudra, pour avoir accès au satellite, pointer vers le ciel une petite antenne parabolique fixée sur un toit ou sur un balcon, un peu comme les antennes pour la télévision numérique par satellite[299].

L'antenne ne fonctionnera qu'à sens unique, c'est-à-dire qu'elle recevra les signaux en provenance d'Internet, mais ce n'est pas elle qui acheminera les requêtes ou messages vers le réseau. Il faudra, pour acheminer les requêtes, utiliser un modem et se connecter par le biais du réseau téléphonique au fournisseur de service offrant la technologie[300].

---

[292] *Le guide de l'internaute 2000, supra* note 136 aux pp. 78-79.

[293] *Internet le guide 2000, supra* note 255 aux pp. 8-14. Voir également J.-J. Meyer, *Les réseaux*, Paris, Osman Eyrolles Multimédia, 2000 aux pp. 160-61.

[294] *Le guide de l'internaute 2000, supra* note 136 à la p. 79.

[295] *Internet le guide 2000, supra* note 255 à la p. 8. Voir notamment les services offerts par Cogeco câble, en ligne : <http://www.cogeco.ca> (date d'accès : 20 juillet 2001) et de Vidéotron Ltée., en ligne : <http://www.videotron.com> (date d'accès : 20 juillet 2001). Compte tenu de l'étendue géographique relative de ces services, il sera possible d'inférer la proximité entre le lieu où se trouve le serveur et le lieu où se trouve l'ordinateur du client.

[296] *Le guide de l'internaute 2000, supra* note 136 à la p. 79 ; *Les réseaux*, *supra* note 136 aux pp. 259-60. En général, les adresses IP fixes seront utilisées dans certains réseaux locaux. Par contre, dans certains cas, un réseau de type LAN/*TCP/IP*, pourra utiliser l'assignation dynamique, rendant en principe l'identification d'un utilisateur plus difficile que dans le cas où une adresse IP fixe est utilisée. Voir aussi *Intrusion Detection*, *supra* note 238 à la p. 124.

[297] *Le guide de l'internaute 2000, supra* note 136 à la p. 79.

[298] Voir les technologies « *DirecPC Two-way System* » et « *DirecPC One-way System* », *de DirecPC, en ligne :* <http://www.direcpc.com> *(date d'accès : 5 août 2001).*

[299] *Internet le guide 2000, supra* note 255 à la p. 13. Voir aussi *DIRECTV*, en ligne : <http://www.directv.com> (date d'accès : 5août 2001), pour un aperçu des services offerts par la télévision par satellite.

[300] *Internet le guide 2000, supra* note 255 à la p. 13.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

Quant au volet téléphonique de l'accès par satellite, nous référons le lecteur à la section traitant des connexions à Internet par le biais du réseau téléphonique. Quant au volet satellite de l'accès, un serveur ou aiguilleur Internet se trouvera sur les lieux du fsI offrant la technologie. C'est par là que se feront les liens entre l'utilisateur, le fournisseur d'accès offrant la technologie, Internet, le satellite et, en fin de piste, l'utilisateur[301].

La connexion bidirectionnelle permettra de communiquer dans Internet seulement par le biais de l'antenne et du satellite. Bien entendu, le satellite est relié au serveur du fournisseur d'accès offrant la technologie, qui lui-même est relié à un fournisseur d'accès Internet régional. Ce type de connexion est accessible à toute personne se trouvant suffisamment près de l'Équateur. Une personne au Canada se trouvant trop au Nord ne pourra bénéficier de ce service[302].

Le niveau d'expectative raisonnable de vie privée quant au contenu du message dans un tel environnement sera tributaire du niveau de protection de vie privée qu'offre la communication par satellite[303]. Comme dans les cas de l'accès à Internet par le réseau de câblodistribution et par le réseau téléphonique, la partie serveur de l'accès se trouvera toujours chez un tiers.

– Le phénomène de la convergence des technologies

Comme nous l'avons vu, plusieurs méthodes et technologies existent pour se brancher à Internet. Le branchement, du point de vue de l'utilisateur, s'effectue généralement à partir de son ordinateur, lui-même branché au réseau par un type de connexion quelconque. Il peut être relativement compliqué de qualifier l'expectative raisonnable de vie privée par rapport à un environnement technique donné. Cela devient encore plus compliqué lorsque plusieurs technologies sont utilisées pour communiquer par le biais d'Internet. En fait, il s'agit de moyens technologiques utilisés normalement à d'autres fins qu'une communication Internet, qui sont désormais utilisés pour y communiquer. Ce sera le cas d'un téléphone cellulaire qui comprend un service de courriel auquel on aura accès en mode texte à même un petit écran sur le téléphone[304]. Ce sera également le cas du service de télévision par câble[305] qui offre les

---

[301] Pour des détails sur les services Internet offerts par le biais d'un satellite, voir *DirecPC*, en ligne : <http://www.direcpc.com> ou <http://www.directpc.com> (dates d'accès : 5 août 2001).

[302] Dans le cas d'un accès unidirectionnel il sera toujours possible d'inférer une certaine proximité entre le serveur du fournisseur Internet offrant la technologie et l'utilisateur du service, notamment à cause de la nécessité d'avoir un lien téléphonique. Dans le cas de l'accès bidirectionnel, l'inférence de proximité est pratiquement impossible : l'individu peut se trouver n'importe où sur la Terre, dans la mesure où il n'est pas trop au nord. *Internet le guide 2000, supra* note 255 aux pp. 12-13.

[303] Quant au volet téléphonique, se référer à la section traitant de l'accès Internet par le biais du réseau téléphonique. Il est intéressant de noter que l'antenne offerte par le service de DirecPC indique « DirecPC » en caractères gras, noirs et rouges. Dans la mesure où cette antenne est visible d'un endroit public, l'expectative raisonnable de vie privée à l'égard du type d'accès à Internet utilisé est grandement diminuée, voire inexistante. Il est également possible d'avoir les services de la télévision par satellite et d'accès à Internet par le biais de la même antenne. Le mot « DirecDuo » en caractères gras, noirs et rouges se trouve inscrits sur l'antenne indiquant que l'utilisateur bénéficie des deux types de services.

[304] Voir Fido, accès mobile à Internet, en ligne : <http://www.fido.ca/NASApp/info/Discover/WhyFido04.jsp?lang=fr> (date d'accès :8 novembre 2001), Telus Mobilité et son service Internet sans fil Net en main, en ligne : <http://www.fido.ca/NASApp/info/Discover/WhyFido04.jsp?lang=fr> (date d'accès : 8 novembre 2001), Bell Mobilité Internet mobile, en ligne :

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

services Internet et le cas des services de télévision par satellite[306]. Dans chaque cas il faudra déterminer le niveau d'expectative raisonnable de vie privée pour chacune des technologies utilisées. Il ne faut pas oublier non plus les différentes technologies qui sont utilisées entres elles de façon complémentaire. Dans certains cas le segment de communication sera par le biais d'une ligne téléphonique ordinaire, qui acheminera le tout à un réseau d'antennes pour téléphones cellulaires ou téléphones satellites, etc.[307] Ce sera, encore une fois, une analyse fondée sur l'ensemble des circonstances, donc sur l'ensemble des fonctionnalités des technologies utilisées et de la nature des services offerts par celles-ci, qui déterminera le niveau ou degré d'expectative raisonnable de vie privée.

Le branchement à Internet par rapport au lieu de l'établissement de la connexion

Il peut y avoir une multitude de lieux à partir desquels un branchement à Internet pourra être effectué. Il ne s'agit pas ici de traiter de tous les lieux possibles. À l'instar de la Cour suprême américaine dans *Reno c. ACLU* [308] et de la décision de première instance dans *ACLU c. Reno*[309], il s'agit plutôt de traiter des principaux[310]. Nous verrons qu'ils peuvent avoir un effet significatif sur le niveau d'expectative raisonnable de vie privée d'un utilisateur. Par exemple, la nature des lieux de l'établissement du branchement à Internet affectera les relations entre les divers individus qui s'y trouvent. Nous traiterons donc du branchement à partir du domicile de l'utilisateur, de son lieu de travail et de son institution d'enseignement. Nous traiterons également du branchement effectué à partir d'un cybercafé et du branchement par accès mobile.

– Au domicile de l'utilisateur

Bien des entreprises offrent le branchement à Internet à partir du domicile. Il s'agit généralement des fsI. Plusieurs types de branchement sont possibles. Les branchements établis par le biais du réseau téléphonique sont sans aucun doute, les plus communs[311]. Il y a également les branchements effectués par le biais du câble qui sont assez populaires, notamment en raison de l'accès haute vitesse très efficace[312]. Dans les régions plus éloignées des grands centres, l'accès par satellite peut également s'avérer être une bonne solution, notamment en raison de l'absence de service du câble pour un accès haute vitesse.

<http://www.bellmobilite.ca/ps/wiredat/browser/overview/default.asp> (date d'accès : 8novembre 2001) et finalement le service de navigation sans fil sur le Web de Rogers, en ligne : <http://www.boutiquerogers.com/store/wireless/services/web_browsing/overview.asp?shopperID=DUE7N58MSCS92P2G00J74HSV311V1M76> (date d'accès : 8 novembre 2001).

305 Voir Cogeco câble, en ligne : <http://www.cogeco.ca> (date d'accès : 20 juillet 2001).et Vidéotron Ltée., en ligne : <http://www.videotron.com> (date d'accès : 20 juillet 2001).

306 Voir *DirecPC*, en ligne : <http://www.direcpc.com> ou <http://www.directpc.com> (dates d'accès : 5 août 2001). et *DIRECTV*, en ligne : <http://www.directv.com> (date d'accès : 5août 2001).

307 U.S. Congress, Office of Technology Assessment, *Electronic Surveillance in a Digital Age*, OTA-BP-ITC-149, Washington DC, U.S. Government Printing Office, 1995, en ligne : <http://www.wws.princeton.edu/cgi-bin/byteserv.prl/~ota/disk1/1995/9513/9513.PDF> (date d'accès : 10 août 2001).

308 *Supra* note 1.

309 *Supra* note 196.

310 Nous référons le lecteur à la section traitant des divers niveaux d'expectative raisonnable de vie privée en fonction du lieu. Généralement, plus les lieux seront publics, moins l'expectative raisonnable de vie privée sera élevée à leur égard.

311 *Internet le guide 2000, supra* note 255 à la p. 8 ; *Cyber Law*, *supra* note 200 aux pp. 13-14.

312 *Internet le guide 2000, supra* note 255 aux pp. 8-10 ; *Cyber Law*, *supra* note 200 aux pp. 14-15.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

Par rapport à l'utilisateur, les branchements effectués à partir du domicile sont les plus susceptibles de générer une attente raisonnable de vie privée élevée. En effet les communications s'établissent à partir d'un lieu (le domicile) en utilisant une technologie (le téléphone) qui bénéficie généralement d'une attente élevée en matière de vie privée[313].

Dans *Gauthier*[314], il fallait déterminer si les fichiers contenus dans la mémoire de l'ordinateur de l'accusé, bénéficiaient d'une expectative raisonnable de vie privée. L'ordinateur avait initialement été saisi à son domicile par les agents de l'État, dans le contexte d'une enquête sur la commission d'infractions en matière de droits d'auteur. En l'espèce, les agents de l'État n'ont pas accédé au contenu de la mémoire de l'ordinateur par le bais d'un réseau. Il est tout de même intéressant de constater la conclusion de la Cour quant au sujet de l'expectative raisonnable de vie privée rattachée au contenu de la mémoire d'un ordinateur. Nous le verrons en détail plus loin.

Toujours dans *Gauthier*, suite à une fouille du contenu de la mémoire de l'ordinateur, un rapport de saisie a été fait au juge de paix, et des accusations de possession de matériel contrefait ont été déposées, en vertu du paragraphe 42(1) de la *Loi sur le droit d'auteur*[315].

Dans le cadre du règlement de l'affaire, un agent de l'État a fouillé de nouveau la mémoire de l'ordinateur de l'accusé dans le but de déterminer si l'ordinateur saisi constituait une « planche » au sens de la *Loi sur le droit d'auteur*. Il est à noter que l'ordinateur était à ce moment en possession des agents de l'État. Cet exercice a été effectué sans autre autorisation que celle du procureur de la Couronne de l'époque et a permis de découvrir une multitude de fichiers contenant de la pornographie infantile. Ces fichiers ont ensuite été transmis aux autorités provinciales, d'où le dépôt d'accusations de possession de pornographie juvénile, en vertu du paragraphe 163.1(4) du *Code criminel*.

La Cour a déterminé que, dans ces circonstances, l'accusé bénéficiait d'une expectative raisonnable de vie privée à l'égard au contenu de son ordinateur. Les raisons invoquées par la Cour ne sont pas très exhaustives. Par souci de précision, nous reprenons le texte du jugement :

> « *C'est à la lumière des arrêts la R. c. Edwards (1996) 1 RCS p. 128; la R. c. Silveira (1995) 2 RCS p. 297 et la R. c. Evans (1996) 1 RCS p. 8, qui parlent de l'expectative raisonnable de vie privée, que le présent Tribunal peut conclure que le contenu d'un ordinateur, particulièrement les courriels ou E-Mail, les images, les news group, les news rider, [sic] sont du*

---

313 Voir notamment *Feeney, supra* note 20 et *Silveira*, *supra* note 20, *Duarte*, *supra* note 51 et la protection offerte par la partie VI du *Code criminel* en matière de protection contre l'interception des communications privées. Nous soumettons que les communications effectuées par le biais du câble bénéficient également d'une protection contre les interceptions illégales. En effet, une communication effectuée par le biais du câble, constitue une « télécommunication » au sens de l'article 35 de la loi d'interprétation ou une « communication privée » au sens des définitions prévues à l'article 183 du *Code criminel*. Voir également la section de la présente étude traitant de cette question. Quant aux communications effectuées par le biais d'un satellite, il est moins clair qu'elles se qualifient de la même façon sauf, bien entendu, quant au volet téléphonique d'une telle communication, le cas échéant.

314 *Supra* note 135.

315 *Loi sur le droit d'auteur* L.R.C. 1985, c. C-42, en ligne : Ministère de la justice <http://lois.justice.gc.ca/fr/C-42/texte.html> (date d'accès : 30 août 2001).

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

> *domaine de la vie privée où il y a «a reasonable expectation of privacy», selon les termes de l'arrêt Hunter c. Southam (1984) 2 RCS p. 145* »[316].

Vu le manque de précisions quant aux motifs, nous nous permettons d'avancer que c'est probablement parce que l'accusé était propriétaire de l'ordinateur, que celui-ci se trouvait dans son domicile et que l'enquêteur a consulté le contenu des courriels, des images et messages de groupes de nouvelles *Usenet*, qui pouvaient être considérés comme des fichiers contenant des informations de nature personnelle et confidentielle. Cette décision est donc susceptible d'application dans presque tous les cas où l'ordinateur de la personne visée par l'immixtion étatique se trouvera dans son domicile.

La Cour ne traite malheureusement pas en détail de la question relative à l'expectative raisonnable de vie privée lorsqu'un ordinateur est effectivement entre les mains des agents. On semble donc prendre pour acquis qu'il en subsisterait une, compte tenu que l'exécution du mandat initial était terminée. À la lumière des critères élaborés par la Cour suprême du Canada dans les arrêts *Plant* et *Edwards*, nous sommes plutôt d'avis que l'expectative raisonnable de vie privée dans ce contexte était inexistante. En effet, les données recherchées se trouvaient dans un ordinateur qui était entre les mains du même organisme d'application de la loi qui avait initialement obtenu l'ordinateur. Le *standing* de M. Gauthier pour contester l'immixtion étatique dans les circonstance était donc à toute fin pratique nul.

– Sur les lieux du travail de l'utilisateur

Ce type de branchement est probablement le plus répandu au Canada. C'est également sur les lieux du travail que les ordinateurs branchés à Internet sont le plus susceptibles de faire partie d'un réseau[317]. L'exposé conjoint des faits dans *ACLU c. Reno*, traite du contexte général d'un branchement fait à partir des lieux du travail :

> « *14. Similarly, Internet resources and access are sufficiently important to many corporations and other employers that those employers link their office computer networks to the Internet and provide employees with direct or modem access to the office network (and thus to the Internet). Such access might be used by, for example, a corporation involved in scientific or medical research or manufacturing to enable corporate employees to exchange information and ideas with academic researchers in their fields* » [note omise][318].

Nous avons vu qu'une multitude de topographies ou configurations sont possibles. Ce qu'il faut retenir, c'est que généralement, l'employeur est un intermédiaire entre le fsI et

---

316 *Gauthier*, *supra* note 135 au para. 29. La décision américaine rendue dans *United States c. Chan,* 830 F. Supp. 531 (N.D.Cal. 1993), confirme également, qu'en principe, le contenu d'un appareil où sont stockées des données, en l'espèce un téléavertisseur, bénéficie d'une expectative raisonnable de vie privée. En effet à la page 534, la Cour affirme ce qui suit: « *The expectation of privacy in an electronic repository for personal data is therefore analogous to that in a personal address book or other repository for such information* ». Voir au même effet *United States c. Reyes, supra* note 179; *United States c. Maxwell,* 45 M.J. 406 (Air Force Crim. App.1996), à la p. 417 [ci après *Maxwell 2*].

317 Nous renvoyons le lecteur à la section traitant des types de réseaux. Le niveau d'expectative raisonnable de vie privée sur les lieux du travail sera notamment tributaire de l'étendue et de la configuration ou topologie du réseau utilisé.

318 *Supra* note 196, aux pp. 832-33.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

l'utilisateur. Le niveau d'attente raisonnable de vie privée sera donc tributaire de la relation de confidentialité existant entre l'utilisateur (employé) et le propriétaire (employeur) du réseau et de ses composantes matérielles et logicielles.

Sans entrer en détail dans les questions reliées au droit du travail, il est raisonnable d'affirmer que les ordinateurs disponibles pour les employés ne devraient servir que pour les fins du travail. Dans ce contexte, une certaine surveillance des activités d'un utilisateur pourrait être effectuée par l'employeur[319], ce qui diminuerait d'autant l'expectative raisonnable de vie privée de l'utilisateur. Dans certains cas, même la productivité de certains employés utilisant les ordinateurs de l'employeur peut être surveillée et contrôlée[320]. Toute surveillance de l'employeur devrait par contre être annoncée clairement aux utilisateurs par le biais d'un avis. Cet avis devrait généralement faire partie des conditions d'emploi[321].

Idéalement, la surveillance devrait faire l'objet d'un consentement qui pourrait être donné par l'employé au début de chaque session initiale de branchement au réseau de l'employeur. En pratique, pour accéder au réseau de l'employeur, il faudra consentir à une surveillance pour fins de vérification d'utilisation conforme en cliquant « oui » à une question apparaissant à l'écran lors du branchement initial. En cliquant « non » on ne pourrait accéder au réseau. Conséquemment, une personne qui accède au réseau accepterait en quelque sorte que l'utilisation de son ordinateur soit surveillée et que ses communications soient interceptées[322].

Un bon exemple illustre bien toute la problématique de l'expectative raisonnable de vie privée en milieu de travail. Dans *Tremblay*[323], l'accusé était policier à l'emploi de la Ville de Trois-Rivières Ouest. Dans le cadre de ses fonctions il utilisait, à partir de son bureau, un ordinateur faisant partie d'un réseau. Le réseau et le matériel informatique se trouvaient sur les lieux du travail et appartenaient à la Ville de Trois-Rivières Ouest. L'ordinateur de Tremblay devait être utilisé pour les fins du travail. Une politique d'utilisation de la Ville, dont l'accusé était censé avoir pris connaissance, allait dans ce sens.

---

319 *Cyber Law*, *supra* note 200 à la p. 69.

320 Ce sera le cas de l'utilisation d'un enregistreur de touches qui aura été placé dans l'ordinateur de l'employé pour savoir quelle est son efficacité au clavier. De plus, on pourra enregistrer le contenu de ce qui est tapé au clavier par l'employé.

321 Des politiques d'utilisation d'Internet sont souvent adoptées par les employeurs. Elles sont par la suite intégrées aux conditions de travail. *Cyber Law*, *supra* note 200 à la p. 76. Elles confèrent généralement très peu de protection en matière d'expectative raisonnable de vie privée quant au contenu de ce qui y circule, notamment les courriels, compte tenu que l'utilisation qui en est faite, doit être reliée au travail. Par contre, dans la décision américaine rendue dans *Smyth c. Pillsbury Company,* 914 F. Supp. 97 (E.D.Pa. 1996), un employeur s'était engagé à ne pas intercepter les courriels de ses employés. Malgré cette politique, on a quand-même congédié un employé en raison d'un usage inapproprié du système de courriel de l'employeur. La Cour a déterminé qu'il n'existait pas d'expectative raisonnable de vie privée à l'égard du contenu d'un courriel envoyé, par le biais du système de courriel, à un superviseur de la compagnie, même si le courriel avait à première vue, été intercepté contrairement à la politique de l'employeur. Le fait que l'employé ait communiqué volontairement son message à un superviseur, par le biais du système de l'employeur, semble avoir été déterminant pour en arriver à cette décision.

322 Il est préférable pour un employeur d'obtenir le consentement d'un employé utilisateur avant de procéder à toute surveillance ou interception. En effet, le *Code criminel* prévoit à l'alinéa 184(2)a), que l'interception d'une communication privée constitue une infraction, à moins que l'on obtienne le consentement 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.

323 *Supra* note 122.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

De la surveillance visuelle du contenu de l'écran, de la surveillance électronique du contenu de l'ordinateur et des accès à l'ordinateur de Tremblay qui se trouvait dans son bureau, ont permis à des collègues de travail d'obtenir des informations compromettantes relativement à de la pornographie infantile. Celles-ci sont transmises à un agent de la paix qui les utilisera pour obtenir un mandat de perquisition. Les fruits de la perquisition justifieront plus tard des accusations de possession de pornographie juvénile, le tout en vertu de l'alinéa 163.1 (4)a) du *Code criminel*.

La question fondamentale était de savoir si Tremblay bénéficiait, dans les circonstances, d'une expectative raisonnable de vie privée eu égard aux fichiers contenus dans l'ordinateur de la Ville de Trois-Rivières Ouest. Le cas échéant, on risquait de ne pas pouvoir utiliser les fruits de la perquisition en preuve contre lui.

La Cour a déterminé que Tremblay ne bénéficiait pas d'une expectative raisonnable de vie privée eu égard aux fichiers contenus dans l'ordinateur de la ville de Trois-Rivières Ouest. Reprenant les critères des arrêts *Edwards*, *Colarusso*, *Wong*, *Gauthier* et *Weir*, la Cour décide que Tremblay ne pouvait s'attendre raisonnablement à bénéficier d'une expectative raisonnable de vie privée dans les circonstances. La Cour fait d'abord une distinction entre le contenu d'un ordinateur personnel et le contenu d'un ordinateur se trouvant sur les lieux du travail :

> « *Les arrêts Gauthier et Weir sont clairs à ce sujet : Le contenu d'un ordinateur, en particulier les courriels sont du domaine de la vie privée où il y a une attente raisonnable de vie privée. Mais ces arrêts traitent d'ordinateurs personnels. L'environnement dans lequel est situé l'ordinateur peut aussi avoir une influence sur l'expectative de vie privée au travail ou à la maison* »[324].

Les raisons suivantes sont avancées, pour supporter la conclusion voulant que Tremblay n'ait pas d'expectative raisonnable de vie privée dans les circonstances :

- Tremblay utilise un ordinateur propriété de la Ville de Trois-Rivières Ouest;
- L'ordinateur doit servir pour les fins du travail;
- Une politique émise par la Ville de Trois-Rivières Ouest en ce sens était supposée être connue de Tremblay;
- Tremblay tolère que son ordinateur soit utilisé par d'autres employés, et ce, même en son absence;
- Pendant les heures de travail, le bureau de Tremblay est ouvert ainsi que son ordinateur qui, lui, est ouvert en permanence;
- Des collègues de travail ont pu avoir accès très librement à l'ordinateur de Tremblay;
- Le technicien en informatique de la Ville de Trois-Rivières Ouest a pu avoir accès à cet ordinateur par le biais de son propre ordinateur sans pénétrer dans le bureau de Tremblay;
- Un collègue de travail a eu connaissance, à de nombreuses occasions, que durant les heures ouvrables de bureau, Tremblay se servait de son ordinateur pour visionner de la pornographie et qu'à certaines occasions, il s'en serait aperçu, changeant de programme à ce moment-là;

[324] *Ibid*. à la p. 10.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

- Tremblay n'a pas témoigné au soutien des allégations de sa requête;

Une multitude de facteurs spécifiques aux environnements de travail devront conséquemment être soupesés lors de la détermination du caractère privé des informations se trouvant dans un ordinateur faisant partie d'un réseau appartenant à l'employeur. De plus, se référant à *Godbout c. Ville de Longueuil*[325], la Cour considère que les actions effectuées par la Ville de Trois-Rivières Ouest sont visées par la *Charte canadienne*. Cela implique que la surveillance initiale, effectuée par les employés, aurait constitué une immixtion étatique, dans le cas où une expectative raisonnable de vie privée aurait été reconnue en faveur de Tremblay.

En conséquence, il est raisonnable d'affirmer qu'un employeur privé ne sera pas soumis aux mêmes conditions qu'un employeur gouvernemental. Dans le cas d'un employeur privé, la *Charte canadienne* ne s'applique pas, alors que c'est le contraire pour un employeur gouvernemental. Ceci a notamment pour conséquence que le niveau de renonciation au droit de voir son ordinateur fouillé, surveillé ou accédé, par un employeur gouvernemental ou ses mandataires, pourrait devoir respecter les critères de renonciation constitutionnels[326]. Un employeur privé ne serait donc pas soumis aux mêmes standards pour qu'un employé renonce validement.

– Dans une institution d'enseignement

L'exposé conjoint des faits dans *ACLU c. Reno*, décrit le contexte général du branchement à Internet par le biais d'une institution d'enseignement :

> « *13. Students, faculty, researchers, and others affiliated with the vast majority of colleges and universities in the United States can access the Internet through their educational institutions. Such access is often via direct connection using computers located in campus libraries, offices, or computer centers, or may be through telephone access using a modem from a student's or professor's campus or off-campus location. Some colleges and universities*

---

[325] *Godbout c. Ville de Longueuil*, [1997] 3 R.C.S. 844 [ci après *Godbout*].

[326] D'ailleurs dans *Godbout, Ibid*. il a été déterminé qu'il ne pouvait y avoir de renonciation valide a un droit constitutionnel, puisque l'individu n'avait d'autres choix que de se plier à l'obligation imposée par l'employeur, s'il voulait bénéficier de son statut d'employé permanent. Or pour être valide du point de vue constitutionnel, la renonciation doit être exprimée librement et volontairement, ce qui n'était pas le cas en l'espèce. Ceci implique que l'imposition d'une renonciation, par un employeur gouvernemental, eu égard à l'utilisation d'un ordinateur pour fins de travail seulement, sera rarement constitutionnelle, à moins qu'elle ne soit pas rattachée aux conditions obligatoires d'emplois, ce qui est, en pratique, peu probable. Voir à ce sujet D. Veilleux, « Le droit à la vie privée-sa portée face à la surveillance de l'employeur » (2000) 60 R. du B. 1. Voir également pour les États-Unis d'Amérique L.O. Natt Grantt, II, « An Affront to Human Dignity : Electronic Mail Monitoring in the Workplace » 8 (1995) Harv. J.L. & Tech 345 ; S.A. Sundstrom, « You've Got Mail! (And the Government Knows It) : Applying the Fourth Amendment to Workplace E-mail Monitoring » 72 (1998) N.Y.U. L. Rev. 2064. J. J. White, « E-mail@Work.Com : Employer Monitoring of Employee E-mail » 48 (1997) Ala. L. R. 1079 ; S. Winters, « The New Privacy Interest : Electronic Mail in the Workplace » (1993) 8 High Tech L.J. 197. Voir finalement *United States c. Simons*, No. 99-4238 (4th Cir. 02/28/2000), où il a été déterminé qu'un employé du *Foreign Bureau of Information Services* (*FBIS*), une division de la *Central Intelligence Agency* (*CIA*), ne bénéficiait d'aucune expectative raisonnable de vie privée à l'égard de fichiers stockés dans un ordinateur de son employeur. Une politique de l'employeur, énonçant notamment que des vérifications, une surveillance et des audits pouvaient être réalisés, a été déterminante dans l'évaluation de l'attente subjective de l'accusé par rapport au caractère privé des fichiers contenus dans son ordinateur et de sa navigation dans Internet.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

> *install "ports" or outlets for direct network connections in each dormitory room or provide access via computers located in common areas in dormitories. Such access enables students and professors to use information and content provided by the college or university itself, and to use the vast amount of research resources and other information available on the Internet worldwide* » [note omise][327].

Généralement, deux types de relations surviennent lors du branchement à Internet dans le contexte d'une institution d'enseignement. La première relation est du type employeur/employé. La deuxième est du type institution/écolier, élève ou étudiant. Nous ne nous attarderons qu'à la deuxième, la première ayant déjà été traitée.

Un branchement à Internet effectué à partir d'une institution d'enseignement se fait généralement à partir d'un ordinateur faisant partie d'un réseau appartenant à l'institution d'enseignement. Bien entendu, l'existence, l'étendue et la topographie du réseau dépendront de l'importance de l'institution.

L'utilisation des ordinateurs fait généralement l'objet d'une politique d'utilisation qui est imposée par l'institution. Le niveau d'expectative raisonnable de vie privée dans le contexte d'un tel branchement sera donc tributaire des limites imposées par l'institution.

Les ordinateurs utilisés dans un tel contexte sont généralement accessibles à plus d'un utilisateur. Les ressources sont donc partagées. Même si chaque étudiant possède généralement son propre code, ou mot de passe, pour accéder au réseau de l'institution, il se peut que dans certaines circonstances, un seul et même code ou mot de passe soit utilisé par plusieurs personnes, ce qui réduit l'expectative raisonnable de vie privée eu égard à certains secteurs de la mémoire de l'ordinateur partagé.

Une politique de surveillance de l'utilisation peut également être mise en place par l'institution qui veut s'assurer que les ordinateurs ne sont utilisés qu'à des fins compatibles avec l'enseignement. Nous référons le lecteur à la section traitant de ce sujet dans le contexte d'un branchement effectué à partir des lieux de travail.

– Dans un cybercafé

L'exposé conjoint des faits dans *ACLU c. Reno*, décrit le contexte général d'un branchement fait à partir d'un cybercafé :

> « *17. Individuals can also access the Internet by patronizing an increasing number of storefront "computer coffee shops," where customers -- while they drink their coffee -- can use computers provided by the shop to access the Internet. Such Internet access is typically provided by the shop for a small hourly fee* » [note omise][328].

Le cybercafé est en quelque sorte un lieu ou endroit commercial, dont un individu ou une personne morale, est propriétaire. Des ordinateurs y sont branchés à Internet et mis à la

[327] *Supra* note 196, à la p. 832.
[328] *Ibid.* à la p. 833.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

disposition des clients de l'établissement pour utilisation. Certains établissements offrent des abonnements. D'autres n'offrent que l'accès à l'utilisation. Bien entendu, il faut payer une contrepartie pour pouvoir utiliser les ordinateurs. Dans le cas où aucun abonnement n'est requis pour se brancher, on qualifie le cybercafé de point d'entrée « anonyme » dans Internet. On le considère « anonyme » en ce sens qu'il sera très difficile de relier un utilisateur à une adresse IP[329].

Le type de branchement à Internet dans ce genre d'établissement peut varier. Pour plus d'efficacité, les branchements y sont généralement à haute vitesse, soit par lignes téléphoniques, soit par câble.

La nature commerciale et publique d'un tel lieu fait d'emblée obstacle à une expectative raisonnable de vie privée élevée. Le simple fait d'être dans un lieu public et commercial ne fait pas en soi obstacle à toute expectative raisonnable de vie privée. Par contre, un individu s'y trouvant devra prendre les mesures nécessaires pour ne pas être à la vue ou entendu de tous.

Dans le contexte de l'utilisation d'un cybercafé, des mesures particulières devront être prises par l'utilisateur pour cacher ou faire disparaître certaines traces qui apparaissent dans la mémoire d'un ordinateur, qu'un utilisateur ordinaire subséquent pourrait facilement consulter. Ces traces sont laissées suite à une utilisation normale de tout navigateur Web, à moins qu'on utilise un ou des logiciels spécialisés dans le nettoyage des secteurs appropriés de la mémoire. Ces traces peuvent également être effacées « manuellement » à même le logiciel. Nous y reviendrons plus en détail dans la section traitant des navigateurs Web.

Par ailleurs, dans la mesure où l'État veut procéder à une surveillance électronique quelconque, on devra s'assurer d'une certaine minimisation de l'atteinte, notamment en raison du caractère public de l'endroit. Cela aura pour but d'empêcher que les communications de tiers, par rapport à l'individu visé, ne fassent l'objet d'une surveillance injustifiée[330].

– L'accès mobile à Internet

Il est maintenant possible de se brancher à Internet, peu importe le lieu où on se trouve. En effet, il est possible de se brancher au réseau à l'aide d'un téléphone cellulaire. Bien entendu, il faut que l'endroit dans lequel on se trouve soit desservi par le service téléphonique offrant la technologie. On branchera donc un ordinateur à Internet par le biais d'un modem, contenu dans une petite carte insérée généralement dans l'ordinateur portatif, qui sera branché au téléphone cellulaire par un câble approprié. Le lien avec le fournisseur de service Internet sera donc établi par le biais du réseau d'antennes de la compagnie offrant le service de téléphonie cellulaire au réseau téléphonique public commuté.

Donc, dans la mesure où l'on peut se brancher pratiquement dans n'importe quel lieu, l'expectative raisonnable de vie privée reliée à un tel branchement, sera tributaire du lieu dans lequel on se trouve et des dispositions que l'on aura prises, pour garder notre communication

---

[329] *Intrusion Detection*, *supra* note 238 à la p. 130. On considère également les bibliothèques, les aéroports, les gares ferroviaires, ou d'autres lieux semblables offrant une connexion au public, comme des points anonymes d'entrée à Internet.

[330] Sur la question de la minimisation, voir *Thompson*, supra note 51.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

confidentielle. Par ailleurs, une « communication radiotéléphonique » sera une communication privée au sens de l'article 183 du *Code criminel*, si elle est traitée électroniquement ou autrement en vue d'empêcher sa réception en clair par une personne autre que la personne à laquelle son auteur la destine. Les communications cellulaires analogiques ne seront donc pas considérées comme une communication privée au sens du *Code criminel*. Par contre, elle, bénéficieront en principe de la protection de la *Charte canadienne*, parce qu'elles constitueront, à l'égard des agents de l'État, des communications bénéficiant d'une expectative raisonnable de vie privée, le tout, encore une fois, sujet aux dispositions prises pour préserver le caractère confidentiel de la communication.

Lors de l'accès mobile à Internet on sera effectivement en mouvement. Conséquemment, l'expectative raisonnable de vie privée pourrait devenir tributaire du niveau d'expectative raisonnable de vie privée rattaché au moyen utilisé. La Cour suprême du Canada a notamment décidé dans *Wise* et *Belnavis*, qu'il y avait une expectative raisonnable de vie privée réduite lors des déplacements en automobile et à l'intérieur d'un véhicule.

Section VI - Le contexte territorial ou juridictionnel d'Internet et la notion d'ubiquité

La notion d'ubiquité

L'ubiquité est définie comme la faculté d'être présent partout dans un même instant. Il s'agit de la possibilité d'être présent en plusieurs lieux à la fois[331]. Ce concept peut être élargi pour inclure également certains aspects de la nouvelle réalité des réseaux informatiques :

> « [...] *le fonctionnement des réseaux ouverts et l'accès à des sites d'information sont facilités lorsque le même contenu informationnel est disponible à plusieurs endroits sur le réseau, permettant à l'usager de toujours accéder au site le moins occupé. [...] Cette ubiquité est également apparente lorsque l'information va d'un fournisseur de service à un usager et que pour cela, elle doive être temporairement fixée sur certains sites, appelée [sic] «passerelles d'interconnexion». Par ailleurs, dans ce cas, l'information n'existe pas nécessairement à plusieurs endroits à la fois mais est plutôt subdivisée en plusieurs segments répartis en plusieurs lieux. En ce sens, on craint parfois que la seule utilisation du réseau génère une importante quantité d'informations, pouvant être récupérée par des tiers négligents, et cela, sans que l'usager n'en soit nécessairement conscient* »[332].

L'ubiquité découlant du protocole TCP/IP

Les communications effectuées par le biais d'Internet nécessitent en principe un déplacement de l'information dans des directions non contrôlées, dans un état de fragmentation non contrôlée, ou les deux à la fois. L'exposé conjoint des faits dans *ACLU c. Reno*, traite de cet aspect :

---

[331] *Le Robert*, *supra* note 4, *s.v.* « ubiquité ».

[332] *Droit du Cyberespace*, *supra* note 8 à la p. 1-17. Voir également sur la création de site miroir A. M. Gathan, M. P. J. Kratz, et J. F. Mann, *Internet Law*, Scarborough (ONT), Carswell, 1998, aux pp. 138-39 [ci après *Internet Law*].

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

> « *9. Messages between computers on the Internet do not necessarily travel entirely along the same path. The Internet uses "packet switching" communication protocols that allow individual messages to be subdivided into smaller "packets" that are then sent independently to the destination, and are then automatically reassembled by the receiving computer. While all packets of a given message often travel along the same path to the destination, if computers along the route become overloaded, then packets can be re-routed to less loaded computers* »[333].

Cette caractéristique de la technologie peut faire en sorte que le degré d'immixtion dans une quelconque expectative raisonnable de vie privée d'un individu pourrait être moindre, dans le cas de l'obtention ou la récupération de l'information, faite par inadvertance, ou dans le cours normal de l'entretien du réseau. La communication est donc partout et nulle part à la fois. Il convient ici de reprendre les propos de Gieske :

> «*Ni l'expéditeur, ni le destinataire n'ont d'influence sur le choix du chemin emprunté. Ils ne peuvent donc pas davantage contrôler ce qui peut advenir des paquets de données sur les différentes passerelles par lesquelles ils transitent. Les paquets IP ne sont pas cryptés, ce qui permet à n'importe quel ordinateur participant à l'acheminement de les enregistrer et donc de reconstituer les informations d'origine. Pire encore, un ordinateur peut manipuler les paquets de données, en les remplaçant par ses propres paquets, et modifier ainsi le contenu des informations transmises* »[334].

En effet, si l'information est obtenue ou récupérée ailleurs que chez l'accusé ou dans un ordinateur autre que le sien ou celui de son fsI, on pourrait invoquer que l'expectative raisonnable de vie privée est moindre dans ces circonstances. Le degré de contrôle sur l'information se trouvant tout azimut étant moindre, le degré d'attente raisonnable peut être réduit d'autant[335].

De plus, considérant que l'information fragmentée, provenant d'un serveur ou d'un ordinateur au Canada peut, théoriquement, se retrouver dans un serveur ou un ordinateur aux États-Unis, il en découle que le citoyen canadien n'aurait, à l'égard de l'information s'y trouvant, aucune protection constitutionnelle en vertu de l'article 8 de la *Charte canadienne* contre les agissements des autorités étrangères[336].

L'ubiquité est-elle une notion prévue au *Code criminel* ?

Les paragraphes 487(2.1) et (2.2) du *Code criminel* s'attaquent à la problématique de l'ubiquité découlant de l'utilisation d'un réseau informatique. En effet, si les données recherchées ne se trouvent pas dans la mémoire de l'ordinateur fouillé, celui-ci n'étant qu'un poste de travail faisant partie d'un réseau, l'officier exécutant peut exiger d'une personne se trouvant sur les lieux de faciliter l'obtention de celles-ci. Ce qui veut dire, en pratique, qu'une personne se trouvant sur les lieux de la fouille devra faire en sorte que les données soient rendues accessibles à l'officier qui les réclame. Les données pourraient être téléchargées de

---

[333] *Supra* note 196, à la p.832.
[334] *Sécurité et protection*, *supra* note 210 à la p. 398.
[335] Voir notamment *Edwards*, *supra* note 15; *Plant, supra* note 34.
[336] *Schreiber, supra* note 17.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

l'ordinateur distant afin que l'ordinateur y donnant accès permette d'en tirer une copie. Il n'est pas clair cependant si cette disposition permet de forcer un individu se trouvant sur les lieux de la fouille, de révéler les mots de passe ou de fournir les clés pour procéder au déchiffrement de données. C'est donc le sens du mot « accès » qui n'est pas tout à fait clair. S'agit-il d'un accès « absolu », auquel cas il faudrait fournir les mots de passe et les clés appropriés, en plus de donner accès aux données, ou d'un accès « relatif », auquel cas il ne faudrait fournir que les données qui sont à distance ? Dans ce dernier cas, des données chiffrées, ou n'étant accessibles que par mot de passe, resteraient inaccessibles, sauf dans la mesure où les agents de l'État pourraient briser les codes ou clés, ce qui n'est pas une mince affaire. La jurisprudence canadienne n'a pas tranché cette question à ce jour.[337] Nous

[337] Il n'est pas clair si le paragraphe 487 (2.1) du *Code criminel*, crée une présomption de proximité de l'information ou des données. Dans la mesure où les données sont accessibles par l'ordinateur se trouvant dans le lieu de la fouille, on permet d'obtenir les données recherchées, même si elles se trouvent électroniquement dans un autre lieu. Cette disposition déroge au principe voulant qu'un mandat de perquisition vise un lieu et non plusieurs lieux. Dans la mesure où le lieu où se trouvent les données distantes est dans une autre circonscription territoriale ou une autre province canadienne, il pourrait toujours être possible d'argumenter que le mandat est invalide, notamment en raison du fait que la disposition permet une perquisition pour laquelle un visa est généralement requis. De plus, il n'est pas clair si ce paragraphe permet d'avoir accès à des données ou des informations qui pourraient se trouver à l'extérieur du Canada. Cela irait à l'encontre du principe fondamental d'interprétation voulant qu'une Loi n'est applicable en principe que sur son territoire. Vu la nature d'Internet et les multiples configurations possibles d'un réseau, il est raisonnable d'envisager la problématique où des données se trouvent à l'étranger. Par contre la mécanique des navigateurs Web peut faire en sorte qu'une information apparaissant se trouver à l'étranger, soit en réalité dans la mémoire cache de l'ordinateur fouillé au Canada. Dans ce cas, il faudrait une présomption claire indiquant que l'information accessible est présumée se trouver au Canada. Dans l'éventualité où le paragraphe 487(2.1) du *Code criminel* était interprété par les tribunaux comme ne permettant pas d'accéder à des données se trouvant à l'étranger, il faudrait vraisemblablement procéder à une demande d'entraide juridique à l'autorité centrale du pays en question, soit par le biais d'un traité d'entraide juridique, soit par le biais de la Convention de Vienne ou d'une demande *ad hoc* qui n'aura aucune base légale formelle, autre que la bonne volonté des parties. Dans le cas où le paragraphe 487(2.1) du *Code criminel* est interprété comme permettant d'obtenir des données de l'étranger, on pourrait notamment invoquer en défense que l'on tente de faire indirectement ce qu'on ne peut faire directement, à savoir, fouiller ou perquisitionner à l'étranger avec un mandat ou autorisation canadien. *Loi sur l'entraide juridique en matière criminelle* L.R.C. 1985 (4e Supp.), c. M-13.6, en ligne : Ministère de la justice <http://lois.justice.gc.ca/fr/M-13.6/31941.html> (date d'accès : 30 août 2001) ; *Traité d'entraide juridique en matière pénale entre le gouvernement du Canada et le gouvernement des États-Unis d'Amérique,* 18 mars 1985, R.T. Can. 1990/19 (entrée en vigueur : 24 janvier 1990), en ligne : Lexum <http://www2.lexum.umontreal.ca/ca_us/fr/CTS.1990.19.fr.cfm> (date d'accès 13 septembre 2001); *Convention des Nations Unies contre le trafic illicite des stupéfiants et des substances psychotropes*, 20 décembre 1988, R.T.N.U. (entrée en vigueur : 11 novembre 1990), en ligne : Traités multilatéraux déposés auprès du secrétaire général des Nations Unies <http://untreaty.un.org/FRENCH/bible/frenchinternetbible/partI/chapterVI/treaty22.asp> (date d'accès : 13 septembre 2001). Le communiqué émanant de la conférence ministérielle du G-8, dont le Canada fait partie, tenue à Moscou les 19 et 20 octobre 1999, confirme que l'accès transfrontalier aux données informatiques stockées dans un pays étranger doit faire l'objet d'une ordonnance judiciaire de ce pays avant de pouvoir y accéder. Il faudrait donc en principe procéder par le biais des mécanismes d'entraide traditionnels pour y accéder. Seules les données accessibles au public en général, peuvent faire l'objet d'une obtention sans autorisation judiciaire, et ce, indépendamment de leur localisation géographique. Canada, Communiqué « *Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime* » (Moscou, 19-20 octobre 1999), en ligne : Ministère des affaires étrangères et du commerce international <http://www.g8.gc.ca/1999/moscow1-f.htm> (date d'accès : 9 novembre 2001). La *Convention sur la cybercriminalité*, 23 novembre 2001, S.T.E. 185 (ouvert pour signature : 23 novembre 2001), en ligne : Conseil de l'Europe <http://conventions.coe.int/Treaty/fr/Treaties/Html/185.htm> (date d'accès : 24 novembre 2001), prévoit également des dispositions d'entraide et de mesures provisoires, plus particulièrement des mesures relatives à la conservation rapide des données informatiques stockées, la divulgation rapide de données conservées. Il prévoit également aux articles 29-34 inclusivement, des dispositions d'entraide concernant les pouvoirs d'investigation, plus particulièrement concernant l'accès aux

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

traiterons plus en détail des principaux aspects de la cryptographie, dont les difficultés à briser les clés cryptographiques.

L'ubiquité d'Internet diminue indirectement le niveau d'expectative raisonnable de vie privée des utilisateurs au Canada.

Internet favorise l'émergence d'une nouvelle criminalité informatique[338]. Il s'agit en général d'une criminalité impliquant des questions d'ordre public[339]. Nous estimons que l'ubiquité qui caractérise Internet favorise également l'émergence d'une criminalité impliquant des questions de sécurité nationale[340]. En effet, par sa configuration, Internet favorise une criminalité transfrontalière, d'où l'augmentation potentielle de la criminalité impliquant des

---

données stockées, l'accès transfrontalier à des données stockées, avec le consentement ou lorsqu'elles sont accessibles au public, la collecte en temps réel de données relatives au trafic et d'interception de données en matière de contenu. Le gouvernement canadien a annoncé que cette convention sera ratifiée et adoptée par le Canada. Canada, Communiqué « Points saillants de la Loi antiterroriste » (Ottawa, 15 octobre 2001), en ligne, Ministère de la Justice <http://Canada.justice.gc.ca/fr/nouv/cp/2001/doc_27786.html> (date d'accès : 18 octobre 2001). La convention a effectivement été signée le 23 novembre 2001 par le Canada. Conseil de l'Europe, état des signatures et ratifications, en ligne : <http://conventions.coe.int/Treaty/FR/searching.asp?NT=185&DF=> (date d'accès : 24 novembre 2001).

338 Internet peut faciliter directement la commission d'une infraction. Dans ce cas, l'infraction est commise dans un environnement informatique. Internet peut également faciliter la commission d'infractions qui ne sont pas commises dans un environnement informatique. Dans ce cas, Internet servira souvent de moyen de communication entre complices qui s'en serviront dans la poursuite de leur but commun.

339 Au sujet de la criminalité informatique impliquant des questions d'ordre public, voir notamment : R. W. K. Davis et S.C. Hutchison, *Computer Crime in Canada*, Toronto, Carswell, 1997 ; J. De Maillard, *Un monde sans loi*, Paris, Stock, 1998 [ci après *Un monde sans loi*] ; D. Dufresne et F. Latrive, *Pirates et flics du Net*, Seuil, Paris, 2000 ; P.N. Grabosky et R.G. Smith, *Crime in the Digital Age*, New Brunswick (NJ), Transaction Publishers, 1998; J.-L. Hérail, et P. Ramael, *Blanchiment d'argent et crime organisé, la dimension juridique*, Paris, PUF, 1996 [ci après *Blanchiment d'argent et crime organisé*] ; D. Icove *et al*., *Computer Crime, A Crime Fighter's Handbook*, Sebastopol (CA), O'Reilly & Associates, 1995 ; D. Martin, *La criminalité informatique*, Paris, Presses Universitaires de France, 1997 [ci après *La criminalité informatique*] ; F.-J. Pansier, et E. Jez, *La criminalité sur l'Internet,* Paris, Presses Universitaires de France, coll. « Que sais-je? », 2000 [ci après *La criminalité sur l'Internet*] ; D. B. Parker, *Fighting Computer Crime, A new framework for protecting information*, New-York, John Wiley and Sons, 1998; J. R. Richards, *Transnational Criminal organizations, Cybercrime, and Money Laundering*, New-York, CRC Press, 1999 [ci après *Transnational Criminal organizations*].

340 Au sujet de la criminalité informatique impliquant des questions de sécurité nationale, voir notamment *Information Warfare, supra* note 210; F. J. Cillufo *et al.*, *Cybercrime... Cyberterrorism... Cyberwarfare... Averting an Electronic Waterloo,* Washington D.C., CSIS Press (The Center for Strategic and International Studies), 1998. Au Canada la sécurité nationale est protégée par l'application complémentaire de deux lois, soit *Loi sur le Service canadien du renseignement de sécurité* L.R.C. 1985, c. C-23, en ligne : Ministère de la justice <http://lois.justice.gc.ca/fr/c-23/texte.html> (date d'accès : 30 août 2001) et la *Loi sur les infractions en matière de sécurité*, L.R.C. 1985, c. S-7, en ligne : Ministère de la justice <http://lois.justice.gc.ca/fr/S-7/47206.html> (date d'accès : 30 août 2001). Selon l'article 2 de la *Loi sur le Service canadien du renseignement de sécurité*, constituent des menaces envers la sécurité du Canada les activités suivantes : «[…] *a*) l'espionnage ou le sabotage visant le Canada ou préjudiciables à ses intérêts, ainsi que les activités tendant à favoriser ce genre d'espionnage ou de sabotage; *b*) les activités influencées par l'étranger qui touchent le Canada ou s'y déroulent et sont préjudiciables à ses intérêts, et qui sont d'une nature clandestine ou trompeuse ou comportent des menaces envers quiconque; *c*) les activités qui touchent le Canada ou s'y déroulent et visent à favoriser l'usage de la violence grave ou de menaces de violence contre des personnes ou des biens dans le but d'atteindre un objectif politique au Canada ou dans un État étranger; *d*) les activités qui, par des actions cachées et illicites, visent à saper le régime de gouvernement constitutionnellement établi au Canada ou dont le but immédiat ou ultime est sa destruction ou son renversement, par la violence. La présente définition ne vise toutefois pas les activités licites de défense d'une cause, de protestation ou de manifestation d'un désaccord qui n'ont aucun lien avec les activités mentionnées aux alinéas *a*) à *d*) ».

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

questions de sécurité nationale. C'est la répression de ce dernier type de criminalité qui est le plus susceptible d'entraîner des atteintes au niveau de l'expectative raisonnable de vie privée des utilisateurs d'Internet.

Dans son rapport public de 1997, le Service canadien du renseignement de sécurité (SCRS), traite de la problématique de la guerre informatique et semble en faire une priorité dans ses objectifs de surveillance, la considérant du coup comme une menace envers la sécurité du Canada :

> « *Pour fonctionner efficacement, le gouvernement et le secteur public doivent utiliser des systèmes informatiques reliés en réseaux internationaux. Cependant, en raison de ces liens et de la dépendance qui en résulte, il existe des points vulnérables qui peuvent être exploités si les systèmes et les données ne sont pas convenablement protégés. Des tests de pénétration menés aux États-Unis ont révélé que 65% des tentatives avaient été couronnées de succès et que la plupart d'entre elles n'avaient pas été détectées.*
>
> *Des services de renseignements étrangers, tout comme certaines organisations criminelles, des groupes terroristes et même des passionnés d'ordinateurs, peuvent effectuer des pénétrations similaires et donc menacer la sécurité au Canada. Le SCRS coopère avec plusieurs ministères et organismes gouvernementaux pour lutter contre la menace posée par les opérations informatiques et pour fournir des évaluations sur la vulnérabilité du Canada et sur les compétences des personnes susceptibles d'exploiter cette vulnérabilité* »[341].

Le rapport public de 1999 est tout aussi éloquent sur la question et confirme que le SCRS ne ménagera pas les efforts pour continuer la surveillance en matière de nouvelles TI et d'Internet. Le SCRS semble également s'inquiéter de l'utilisation accrue des techniques de chiffrement, dont nous traiterons plus loin :

> *« La technologie moderne a une incidence déterminante sur nos méthodes actuelles de travail. Tout en ayant été très utiles pour de nombreuses personnes, les percées réalisées à l'égard des méthodes de télécommunication et de chiffrement ont aussi ouvert de nouvelles voies pour les opérations de renseignements et de terrorisme, ce qui représente de nouveaux défis pour les services de renseignements et de sécurité qui tentent de surveiller les activités représentant une menace. Par ailleurs, les télécommunications modernes ont fait apparaître de nouveaux joueurs dans le contexte de la menace, des pirates informatiques aux extrémistes solitaires ayant des motifs politiques. Les progrès technologiques ont fourni des moyens de développer des armes innovatrices, ce qui accroît le pouvoir destructeur des outils mis à la disposition de ceux qui cherchent à faire du tort.*
>
> *Le service s'efforce de rester à la fine pointe de l'évolution technologique, grâce à des échanges avec des institutions gouvernementales et des services alliés, et à*

[341] Canada, Service canadien du renseignement de sécurité, *Rapport public de 1997*, Ottawa, Approvisionnements et Services, 1998, aux pp. 7-8.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

> *ses propres projets de recherche et de développement. Pour mener des enquêtes opportunes sur les menaces pour la sécurité nationale, il faut pouvoir compter* sur une collecte et une analyse efficaces. […] Pour être en mesure d'évaluer et de contrer la menace dans le contexte actuel, le service consentira des investissements considérables dans le développement technologique afin de suivre le rythme des changements dans ce domaine »[342]

Il s'agit donc de cas où la criminalité est directement reliée aux environnements informatiques.

Au Canada, la norme de protection constitutionnelle requise pour procéder à la surveillance électronique d'un individu en matière de sécurité nationale, est moindre qu'en matière d'ordre public[343]. En effet, pour obtenir une autorisation d'intercepter des « communications privées », les agents du SCRS n'ont besoin que d'avoir des motifs raisonnables de soupçonner qu'une activité constitue une menace envers la sécurité du Canada, ce qui peut sembler déroger aux critères énoncés dans *Hunter*, qui prévoient au minimum l'existence de motifs raisonnables de croire[344]. De plus il n'est pas nécessaire qu'il y ait commission d'une infraction criminelle pour obtenir une autorisation d'intercepter. Il suffit qu'une menace envers la sécurité du Canada soit établie. La partie VI du *Code criminel* ne s'applique pas à une interception de « communications privées », autorisée par un mandat décerné en vertu de l'article 21 de la *Loi sur le Service canadien du renseignement de sécurité*, ni à la communication elle-même[345]. Conséquemment, le SCRS peut intercepter des communications privées reliées à des comportements de nature criminelle, dans la mesure où l'interception se produit dans le cours d'une enquête visant une menace envers la sécurité du Canada.

---

[342] Canada, Service canadien du renseignement de sécurité, *Rapport public de 1999*, Ottawa, Approvisionnements et Services, 2000, aux pp. 15-16.

[343] En effet l'article 12 de la *Loi sur le Service canadien du renseignement de sécurité* L.R.C. 1985, c. C-23, permet notamment l'obtention d'une autorisation judiciaire, prévue à l'article 21, pour procéder à l'interception des communications d'un individu. L'article 12 prévoit : « […] *Le Service recueille, au moyen d'enquêtes ou autrement, dans la mesure strictement nécessaire, et analyse et conserve les informations et renseignements sur les activités dont il existe des motifs raisonnables de soupçonner qu'elles constituent des menaces envers la sécurité du Canada; il en fait rapport au gouvernement du Canada et le conseille à cet égard* ». Le paragraphe 21(1) prévoit : 21. (1) « *Le directeur ou un employé désigné à cette fin par le ministre peut, après avoir obtenu l'approbation du ministre, demander à un juge de décerner un mandat en conformité avec le présent article s'il a des motifs raisonnables de croire que le mandat est nécessaire pour permettre au Service de faire enquête sur des menaces envers la sécurité du Canada ou d'exercer les fonctions qui lui sont conférées en vertu de l'article 16* ».

[344] Ce critère a tout de même été jugé conforme à l'article 8 de la *Charte canadienne* dans : *Atwal c. Canada*, [1988] 1 C.F. 107. Le juge Dickson dans *Hunter, supra* note 15 aux pp. 167-68, annonçait déjà qu'une norme moindre que celle des motifs raisonnables de croire pourrait trouver application dans des situations où la sécurité nationale serait en jeu :

> « *Le droit de l'état de déceler et de prévenir le crime commence à l'emporter sur le droit du particulier de ne pas être importuné lorsque les soupçons font place à la probabilité fondée sur la crédibilité. L'histoire confirme la justesse de cette exigence comme point à partir duquel les attentes en matière de la vie privée doivent céder le pas à la nécessité d'appliquer la loi. Si le droit de l'état ne consistait pas simplement à appliquer la loi comme, par exemple, lorsque la sécurité de l'état est en cause, ou si le droit du particulier ne correspondait pas simplement à ses attentes en matière de vie privée comme, par exemple, lorsque la fouille ou la perquisition menace son intégrité physique, le critère pertinent pourrait fort bien être différent* ».

[345] *Loi sur le Service canadien du renseignement de sécurité* L.R.C. 1985, c. C-23, art. 23, en ligne : Ministère de la justice <http://lois.justice.gc.ca/fr/c-23/texte.html> (date d'accès : 30 août 2001)

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

L'information ainsi obtenue pourra être transmise aux organismes d'application de la loi appropriés[346].

L'actualité récente nous donne malheureusement deux bons exemples de cas où Internet aurait été utilisé pour faciliter la commission d'infractions impliquant des questions de sécurité nationale[347].

Nous venons de décrire les contextes techniques généraux apportés par l'utilisation de l'informatique, d'Internet et des nouvelles TI. Ce sont dans ces contextes plus généraux que s'insèrent des contextes techniques particuliers de communication. Ces contextes apporteront leurs différentes caractéristiques qui moduleront, dans un sens ou dans l'autre, le niveau d'expectative raisonnable de vie privée auquel un utilisateur sera en droit de s'attendre. Il convient donc de traiter des contextes techniques particuliers de communication apportés par Internet et les nouvelles TI.

Chapitre II - Les contextes techniques particuliers de communication apportés par Internet et les nouvelles TI

Nous traiterons dans le présent chapitre du Web, du courriel, du transfert de fichiers *FTP*, des groupes de discussions ou de nouvelles *Usenet*, des sessions en mode terminal *Telnet*, des sessions de bavardage-clavier ou clavardage du service IRC, de la téléphonie et de la vidéoconférence Internet et, finalement, de la messagerie instantanée.

Section I - Le Web

---

[346] *Loi sur le Service canadien du renseignement de sécurité* L.R.C. 1985, c. C-23, arts. 17(1) et 19(1), (2)a), en ligne : Ministère de la justice <http://lois.justice.gc.ca/fr/c-23/texte.html> (date d'accès : 30 août 2001) et *Loi sur les infractions en matière de sécurité*, L.R.C. 1985, c. S-7, art. 6, en ligne : Ministère de la justice <http://lois.justice.gc.ca/fr/S-7/47206.html> (date d'accès : 30 août 2001).

[347] En effet, des groupes terroristes islamistes ont mis en place deux sites Web, utilisés notamment pour recruter des terroristes, lever des fonds et prôner la violence envers les communautés juives. Ces sites étaient enregistrés au Canada et auraient été l'objet d'enquête du SCRS et de la GRC. Stewart Bell, « RCMP Probing 'Jihad' Websites » *National Post* (18 août 2001) A-1 et A-4. De plus, suite aux attaques terroristes survenues aux États-Unis d'Amérique contre le World Trade Center et le Pentagone, une surveillance presque généralisée a été lancée dans Internet. On pourrait notamment se servir du système Carnivore pour surveiller systématiquement tous les courriels des jours précédant les attentats. Le FBI a requis auprès de fsI majeurs, d'effectuer cette surveillance générale de leur système, dont America Online et Earthlink. Eng, Paul, « Scouring Cyberspace. Tapping the Internet for Clues on the Attack on America » ABC News.com (13 septembre 2001) en ligne : <http://www.abcnews.go.com/sections/scitech/DailyNews/WTC_netsearch010913.html>. Voir également *Carnivore*, en ligne : <http://www.fbi.gov/hq/lab/carnivore/carnivore.htm> (date d'accès :24 août 2001) et United Sates, Department of Justice, *Independant Technical Review of the Carnivore System Draft Report*, ITT Research Institute, 2000 (auteurs : Smith, Stephen P., Perrit, Jr., Henry, *et al.*), en ligne : <http://www.usdoj.gov/jmd/publications/carnivore_draft_1.pdf> (date d'accès : 24 août 2001). Plus récemment encore, le Canada a déposé le P.L. C-36, *Loi antiterroriste*, 1ère sess., 37e, 2001, qui prévoit notamment l'élargissement des pouvoirs d'interception des communications privées lorsque des questions reliées à des activités terroriste sont en cause, en ligne : Parlement du Canada <http://www.parl.gc.ca/common/Bills_House_Government.asp?Language=F&Parl=37&Ses=1#C-36> (date d'accès : 12 novembre 2001). Le gouvernement des Etats-Unis d'Amérique veut également augmenter les pouvoirs d'interception des communications privées traditionnelles et par le biais d'Internet. Voir le *USA Patriot Act of 2001*, Bill H.R. 3162, 107th Cong. (2001), en ligne : *FindLaw* <http://news.findLaw.com/cnn/docs/terrorism/hr3162.pdf> (date d'accès : 12 novembre 2001).

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

Nous commencerons cette section en décrivant le Web. Nous traiterons ensuite des navigateurs et de leur utilité. Nous traiterons finalement des *cookies* de la mémoire cache et des *log files* qui sont rattachés à l'utilisation des navigateurs.

Description générale de la technologie

Le Web fonctionne avec une approche client-serveur. La partie client de cette relation est formée de l'utilisateur, de son ordinateur et de son logiciel de navigation (*Browser*) ou navigateur. La partie « serveur » de cette relation est constituée également d'un ordinateur, généralement situé à distance par rapport au client, rempli de fichiers de toutes sortes. Cet ordinateur distant utilise un logiciel qui lui permet de répondre aux requêtes du type Web provenant des clients[348]. À l'instar d'Internet, le Web est considéré comme un système distribué où il n'existe aucun contrôle central :

> « *46. A distributed system with no centralized control. Running on tens of thousands of individual computers on the Internet, the Web is what is known as a distributed system. The Web was designed so that organizations with computers containing information can become part of the Web simply by attaching their computers to the Internet and running appropriate World Wide Web software. No single organization controls any membership in the Web, nor is there any single centralized point from which individual Web sites or services can be blocked from the Web. From a user's perspective, it may appear to be a single, integrated system, but in reality it has no centralized control point* » [note omise][349].

Les échanges de type Web sont effectués normalement par le biais du port de communication IP 80[350]. Le protocole utilisé pour transférer l'information entre un client et un serveur, est le HTTP *(Hyper Text Transfer Protocol)*[351] Le Web est qualifié de moyen de communication permettant « l'obtention d'information à distance »[352]. Il permet également la consultation à distance[353].

Une multitude de types de fichiers peuvent être échangés par le biais du Web, notamment des documents[354], des images[355] et des sons[356]. Le navigateur permet de visionner des pages Web

---

348 *Le guide de l'internaute 2000, supra* note 136 à la p. 166 ; *Internet*, *supra* note 214 à la p. 71.

349 *ACLU c. Reno, supra* note 196 à la p. 838.

350 *Le guide de l'internaute 2000, supra* note 136 aux pp. 156 et 167.

351 Pour des échanges plus sécurisés, il est également possible qu'un client et qu'un serveur communiquent par le biais du protocole *S-HTTP* (*Secure-HTTP*). Ce protocole utilisera la cryptographie pour établir un lien sécurisé entre le client et le serveur. Viendra sous peu le *HTTP-NG* (*HTTP-Next Generation*), qui promet des échanges plus efficaces, donc plus rapides, et plus sécurisés. Voir *Le guide de l'internaute 2000, supra* note 136 aux pp. 167-68, 555.

352 *ACLU c. Reno, supra* note 196 aux pp. 834-36.

353 *Protégez-vous sur Internet, supra* note 207 à la p. 150.

354 Comme par exemple, des fichiers de type Adobe Acrobat, portant l'extension « .pdf » et de type HTML, portant l'extension « .html » ou « .htm ». Voir *Le guide de l'internaute 2000, supra* note 136 à la p. 167.

355 Comme par exemple des fichiers multimédias vidéos RealVideo, portant les extensions « .ram », « .rm » ou « .rmm ». Il peut s'agir également de fichiers d'images ou photos, portant l'extension « .jpeg ». Voir *Le guide de l'internaute 2000, supra* note 136 aux pp. 167, 447.

356 Comme par exemple des fichiers audio pour Windows, portant l'extension « .wav » et des fichiers de type *Moving Pictures Expert Group*, portant l'extension « .mp3 ». Voir *Le guide de l'internaute 2000, supra* note 136 aux pp. 167, 447.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

en utilisant des liens hypertextes pour aller de page en page, permettant de voir et d'entendre des fichiers multimédias, de consulter le courriel et les nouvelles de groupes de discussion *Usenet*, etc[357]. La Cour suprême des États-Unis décrit la technologie dans *Reno c. ACLU*:

> « *The best known category of communication over the Internet is the World Wide Web, which allows users to search for and retrieve information stored in remote computers, as well as, in some cases, to communicate back to designated sites. In concrete terms, the Web consists of a vast number of documents stored in different computers all over the world. Some of these documents are simply files containing information. However, more elaborate documents, commonly known as Web "pages," are also prevalent. Each has its own address—"rather like a telephone number." Web pages frequently contain information and sometimes allow the viewer to communicate with the page's (or "site's") author. They generally also contain "links" to other documents created by that site's author or to other (generally) related sites. Typically, the links are either blue or underlined text—sometimes images* » [note omise][358].

Le but de la création du Web est décrit en première instance :

> « *34. Purpose. The World Wide Web (W3C) was created to serve as the platform for a global, online store of knowledge, containing information from a diversity of sources and accessible to Internet users around the world. Though information on the Web is contained in individual computers, the fact that each of these computers is connected to the Internet through W3C protocols allows all of the information to become part of a single body of knowledge. It is currently the most advanced information system developed on the Internet, and embraces within its data model most information in previous networked information systems such as FTP, gopher, wais, and Usenet* » [note omise][359].

Le Web offre donc plusieurs ressources qui pourront être utilisées par l'entremise des protocoles Web qui les supportent. Il est donc important de retenir que le Web ne constitue pas en soi un moyen de communication. C'est plutôt un canal par lequel plusieurs ressources sont utilisées, notamment par le biais d'un navigateur Web, dont nous traiterons plus tard. Bien que le Web ait une portée très large, il ne faut pas le confondre avec Internet, qui constitue plutôt l'infrastructure sous-jacente dans laquelle le Web utilisera ses diverses ressources[360]. Il convient maintenant de traiter du fonctionnement d'une session Web.

La session Web

Le Web est basé sur le mode de présentation hypertexte, c'est-à-dire que certains éléments des pages Web consultées peuvent apparaître en surbrillance, indiquant un hyperlien. Lorsqu'un utilisateur cliquera à l'aide de sa souris sur cet élément, il sera renvoyé à une autre page ou fichier, et ainsi de suite. C'est ce qu'on appelle un hyperlien[361]. Un utilisateur peut donc se

---

[357] *Le guide de l'internaute 2000, supra* note 136 à la p. 154.
[358] *Supra* note 1 à la p. 852.
[359] *ACLU c. Reno, supra* note 196 à la p. 836.
[360] *Digital Evidence, supra* note 252 à la p. 88.
[361] *Le guide de l'internaute 2000, supra* note 136 aux pp. 154-55.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

promener, ou naviguer, d'une page à l'autre ou à l'intérieur de la même page, en cliquant de temps à autre sur les hyperliens. Le langage de type HTML *(Hyper Text Markup Language*) favorise l'utilisation des hyperliens[362].

La Cour suprême américaine décrit le concept de navigation dans le Web dans *Reno c. ACLU* :

> « *Navigating the Web is relatively straightforward. A user may either type the address of a known page or enter one or more keywords into a commercial "search engine" in an effort to locate sites on a subject of interest. A particular Web page may contain the information sought by the "surfer," or, through its links, it may be an avenue to other documents located anywhere on the Internet. Users generally explore a given Web page, or move to another, by clicking a computer "mouse" on one of the page's icons or links. Access to most Web pages is freely available, but some allow access only to those who have purchased the right from a commercial provider. The Web is thus comparable, from the readers' viewpoint, to both a vast library including millions of readily available and indexed publications and a sprawling mall offering goods and services* »[363]

Le Web peut donc être utilisé de différentes manières. Elles se résument à deux façons principales. On peut y publier de l'information; on agit alors à titre de diffuseur. On peut également y rechercher des informations, soit pour simples fins de consultation, soit pour les obtenir en les téléchargeant à partir de son ordinateur; on agit alors à titre d'utilisateur à la recherche d'information ou de spectateur[364]. L'analogie du diffuseur est également reprise en première instance :

> « *40. Publishing. The World Wide Web exists fundamentally as a platform through which people and organizations can communicate through shared information. When information is made available, it is said to be "published" on the Web. Publishing on the Web simply requires that the "publisher" has a computer connected to the Internet and that the computer is running W3C server software. The computer can be as simple as a small personal computer costing less than $ 1500 dollars or as complex as a multi-million dollar mainframe computer. Many Web publishers choose instead to lease disk storage space from someone else who has the necessary computer facilities, eliminating the need for actually owning any equipment oneself* . […]
>
> 43. *Web publishers have a choice to make their Web sites open to the general pool of all Internet users, or close them, thus making the information accessible only to those with advance authorization. Many publishers choose to keep their sites open to all in order to give their information the widest potential audience. In the event that the publishers choose to maintain restrictions on access, this may be accomplished by assigning specific user names and passwords as a prerequisite to access to the site. Or, in the case of*

[362] *Ibid*. à la p. 555 ; *Protégez-vous sur Internet, supra* note 207 à la p. 150.
[363] *Supra* note 1 à la p. 852.
[364] *Protégez-vous sur Internet, supra* note 207 aux pp. 150-51.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

> *Web sites maintained for internal use of one organization, access will only be allowed from other computers within that organization's local network* » [note omise][365].

Il ressort de cet exposé que de multiples contextes de communication sont susceptibles de survenir dans le Web. Dans certains cas, l'information publiée ne sera accessible qu'à certaines personnes. Dans d'autres cas, elle sera accessible à tous. Nous y reviendrons un peu plus loin dans le cadre de la navigation Web. Par contre, le Web ne permet pas d'établir un véritable dialogue. Contrairement au courriel, aux groupes de discussion ou aux sessions de bavardage-clavier ou clavardage du service *IRC*, la communication dans le Web, effectuée par le biais de la navigation, ne fonctionne en principe que dans un seul sens: dans la plupart des cas ce sera le site Web visité qui enverra des informations à l'ordinateur de l'utilisateur[366].

L'analogie de l'utilisateur à la recherche de l'information est reprise dans l'exposé conjoint des faits dans *ACLU c. Reno* :

> « *44. Searching the Web. A variety of systems have developed that allow users of the Web to search particular information among all of the public sites that are part of the Web. Services such as Yahoo, Magellan, Altavista, Webcrawler, and Lycos are all services known as "search engines" which allow users to search for Web sites that contain certain categories of information, or to search for key words. For example, a Web user looking for the text of Supreme Court opinions would type the words "Supreme Court" into a search engine, and then be presented with a list of World Wide Web sites that contain Supreme Court information. This list would actually be a series of links to those sites. Having searched out a number of sites that might contain the desired information, the user would then follow individual links, browsing through the information on each site, until the desired material is found. For many content providers on the Web, the ability to be found by these search engines is very important* » [note omise][367].

On recherchera de l'information en utilisant une adresse *URL* (*Uniform Ressource Locator*). L'adresse recherchée sera inscrite à l'endroit approprié lors de l'utilisation d'un logiciel de navigation. On pourra également utiliser des moteurs de recherche qui facilitent le repérage par mots clés des pages ou sites Web désirés[368]. En principe, il est essentiel pour une personne

---

[365] *ACLU c. Reno, supra* note 196 à la p. 837.

[366] *Protégez-vous sur Internet, supra* note 207 aux pp. 150-51.

[367] *Supra* note 196 à la p. 837.

[368] En plus des moteurs de recherche énumérés dans *ACLU c. Reno*, on pourra notamment utiliser pour ce faire les portails ou moteurs de recherche suivants : La toile du Québec, en ligne : <http://www.toile.qc.ca> (date d'accès : 20 juin 2001), Copernic, en ligne : <http://www.copernic.com> (date d'accès : 20 juin 2001), Francité, en ligne : <http://www.francite.com> (date d'accès :20 juin 2001), *Yahoo !*, en ligne : <http://www.yahoo.ca> (date d'accès : 20 juin 2001), Nomade, en ligne : <http://www.nomade.fr> (date d'accès : 20 juin 2001), *Hot Bot*, en ligne : <http://www.hotbot.com> (date d'accès : 20 juin 2001), *Google*, en ligne : <http://google.com> (date d'accès : 20 juin 2001), *Excite*, en ligne : <http://www.excite.com> (date d'accèes : 20 juin 2001), Trouvez !, en ligne : <http://www.trouvez.com> (date d'accès :20 juin 2001). Il existe une multitude d'autres moteurs de recherche ou portails Internet. Pour une liste plus complète et des informations sur leur utilisation, *voir Search Engine Watch*, en ligne : <http://www.searchenginewatch.com> (date d'accès : 20 juin 2001). L'essence même des moteurs de recherche est de fournir aux utilisateurs une source d'information logiquement centralisée. Les moteurs de recherche abondent d'informations au sujet d'individus, de groupes, d'organisations, de services, de systèmes et de réseaux qui peuvent toutes être

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

qui publie de l'information dans le Web de pouvoir se faire trouver. Théoriquement, on pourrait, par le biais des moteurs de recherche, trouver tout ce qui est publié dans Internet. Ceci nous amène à traiter plus en détails des fonctionnalités et caractéristiques des navigateurs Web.

Les navigateurs

Les navigateurs sont les logiciels clients utilisés principalement pour effectuer les recherches dans le Web[369]. Ils peuvent également servir à d'autres fonctions, notamment à la création de pages Web simples, la consultation de groupes de nouvelles *Usenet*, l'envoi de courriel, l'utilisation de la messagerie instantanée, la gestion et tenue d'un agenda personnel, la synchronisation des informations d'un assistant numérique, la participation à des téléconférences, et l'écoute et visualisation de fichiers multimédias. Dans la présente section, nous ne nous attarderons qu'aux fonctions rattachées à la recherche et à la publication. La publication ne fera l'objet que de considérants généraux, relatifs aux problèmes liés à la protection de la vie privée. Quant aux fonctions rattachées au courriel, aux groupes de discussion et à la messagerie instantanée, elles feront l'objet de sections spécifiques plus loin dans la présente étude. Quant aux autres fonctions, nous n'en traiterons pas, compte tenu qu'elles dépasseraient le cadre de cet ouvrage.

Pour la recherche d'information, il suffit d'inscrire l'URL recherchée dans la case nommée « adresse ». L'URL se compose de trois sections : le préfixe, l'adresse Internet du serveur et le suffixe. Le préfixe[370] indique le type de ressource que l'on désire atteindre, l'adresse Internet du serveur indique soit l'adresse Internet, soit l'adresse IP du serveur Web de la personne ou du groupe de discussion que l'on veut joindre, le suffixe indique l'élément concret recherché sur le serveur distant; ce sera généralement un nom de répertoire jumelé ou non à un nom de fichier[371].

Une multitude de paramètres des navigateurs peuvent être configurés, changés et modifiés. De plus, une multitude d'informations apparaissent sur l'interface lors de l'utilisation. Nous ne nous attarderons qu'aux fonctions ou informations ayant une influence sur le caractère privée d'une communication effectuée par le biais d'un navigateur Web. C'est ce qui nous amène à traiter du témoin de transaction sécurisée, des *cookies*, de l'historique, des *log files* et de la cache.

---

utilisées pour retracer un utilisateur. Voir aussi *Intrusion Detection*, *supra* note 238 à la p. 138. De plus, lorsqu'on accède au site même, il est souvent possible d'y effectuer une recherche encore plus complète par l'entremise d'un moteur de recherche intégré.

369 Il en existe deux principaux soit le *Navigator* de la compagnie Netscape et l'Internet Explorer de la compagnie Micosoft. Les versions de ces logiciels changent constamment. Par contre, les modifications qu'on y apporte ne changent pas fondamentalement leurs principales fonctions. Il s'agit le plus souvent de modifications touchant la présentation ou l'esthétique de l'interface. Conséquemment, nous traiterons des fonctions et caractéristiques principales des versions 4.7X et plus de Netscape et 5.X et plus d'Internet Explorer. Le X indique qu'il s'agit de versions issues du logiciel de même famille. *Le guide de l'internaute 2000, supra* note 136 à la p. 155.

370 Le préfixe « *http*:// » indique qu'il s'agit d'un serveur Web, « *FTP*:// » indique qu'il s'agit d'un serveur *FTP*, « *telnet*:// » indique une session Telnet, « *mailto* : » indique l'envoi d'un courriel, « *news* : » indique qu'il s'agit d'un serveur de nouvelles d'un groupe de discussion *Usenet*, « file : » indique, par exemple, que l'on veut consulter un document se trouvant dans un fichier particulier dans notre ordinateur. *Le guide de l'internaute 2000, supra* note 136 aux pp.175-78.

371 *Le guide de l'internaute 2000, supra* note 136 à la p. 173.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

Le témoin de transaction sécurisée

Lors d'une communication, un témoin de transaction sécurisée indique à l'utilisateur si la communication est sécurisée ou non. Le témoin est représenté par un petit cadenas apparaissant dans le bas de l'écran. Si le cadenas est ouvert, la transaction n'est pas sécurisée, c'est-à-dire qu'elle n'est pas chiffrée. Si le cadenas est fermé, la transaction est sécurisée, donc chiffrée.[372]

Une communication non chiffrée indique qu'elle est plus susceptible d'être interceptée ou obtenue par un tiers. Une communication chiffrée le sera moins. Toute chose étant relative, nous avons utilisé le mot « susceptible » d'être interceptée ou obtenue[373]. Nous traiterons plus loin de la cryptographie comme technique pouvant favoriser une communication plus sécurisée. Il est par ailleurs recommandé de ne pas transmettre d'informations confidentielles si une communication n'est pas sécurisée, comme par exemple, dans le cas de la transmission d'un numéro de carte de crédit lors d'un achat en ligne sur un site transactionnel[374]. Une personne qui sait que la transaction est sécurisée pourra notamment invoquer une attente subjective de protection de la vie privée, alors que la personne qui sait que la transaction ne l'est pas, pourra difficilement le faire.

L'historique de navigation ou de déplacements à long terme et l'historique de la navigation courante ou de déplacements à court terme

Lors de la navigation, différentes pages sont consultées. Deux boutons apparaissant à l'écran facilitent cette navigation : les boutons « précédent » et « suivant ». En cliquant sur ces boutons, il sera possible d'obtenir la liste des documents, ou pages, par ordre de consultation[375]. C'est ce qu'on appelle l'historique de navigation courante ou de déplacement à court terme. Il sera donc possible d'afficher le contenu précédent et suivant des pages ou

---

372 *Ibid*. à la p. 191.

373 Il est intéressant de noter que la jurisprudence relative à l'expectative raisonnable de non-interception lors de l'utilisation d'un téléphone cellulaire, a déjà traité de la notion d'expectative relativement à la possibilité (ou probabilité, selon le cas) qu'une communication soit interceptée. En effet, l'utilisation d'un téléphone cellulaire analogique était assimilée à une diffusion. Une communication effectuée par le biais d'un téléphone cellulaire analogique, était donc considérée pouvant être interceptée par à peu près n'importe qui utilisant un balayeur d'ondes ou *scanner*. Ce qui ne conférait pas à l'utilisateur d'un téléphone cellulaire analogique, du moins en 1991, une attente raisonnable de non-interception au sens de l'article 183 du *Code criminel*. Voir *R. c. Solomon* [1992] R.J.Q. 2631, aux pp. 2642-44. Voir *contra Cheung*, *supra* note 168 aux pp. 443-46, où l'on détermine qu'il est peu probable qu'une communication précise, à un moment précis, soit interceptée par un *scanner*, compte tenu notamment de la configuration des antennes et des relais au réseau téléphonique commuté et du nombre de fréquences possibles qu'un appel peut emprunter. Le jugement analyse la technologie telle qu'elle existait en 1990. Le législateur a amendé le *Code criminel* le 1er août 1993 par le biais de la *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, c. 40, en modifiant la définition de « communication privée ». On y ajoutait le concept de communication traitée électroniquement ou autrement en vue d'empêcher sa réception en clair par une personne autre que celle à qui son auteur la destine. À notre avis cet ajout ne règle pas la question des communications cellulaires analogiques, dans la mesure où celles-ci existent encore. Il ne couvrirait que les communications effectuées par le biais d'un téléphone cellulaire numérique. Il est intéressant de noter que l'expression, « …traitée électroniquement ou autrement… », pourrait comprendre une communication chiffrée par le biais de la cryptographie. Une telle communication serait donc une « communication privée » au sens du *Code criminel*.

374 *Le guide de l'internaute 2000, Ibid*. à la p. 192.

375 *Ibid*. aux pp. 188-89, 236-37.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

documents consultés. Cet historique est automatique et s'efface à la fin de l'utilisation[376]. Dans l'intervalle, les informations s'y rapportant sont conservées dans la mémoire cache de l'ordinateur[377]. Le nombre de pages ou documents conservés varie, mais est relativement court. Il permet de revenir ou d'avancer d'environ une dizaine de pas[378]. Il y a également l'historique des dernières pages dont on a tapé spécifiquement l'adresse, ou URL désirée. Il s'agit d'un menu déroulant apparaissant sous la ligne où l'on tape l'adresse désirée. Cette fonction sert à faciliter l'accès à certains sites fréquemment visités. Puisque cette information n'apparaît que si l'utilisateur a spécifiquement tapé l'adresse[379], il sera difficile pour lui d'invoquer qu'il s'agit d'une page visitée par erreur!

L'historique de navigation ou de déplacements à long terme permet de garder une trace de tous les déplacements effectués lors d'une session de navigation. Cette fonction a pour but principal de pouvoir retrouver facilement un site ou une page visitée quelques jours auparavant[380]. Cela permet également d'identifier les pages ou documents consultés lors de navigations subséquentes sur un site déjà visité et parfois les mots clés tapés par un utilisateur lors d'une recherche[381]. C'est ce qui explique que les liens changent de couleur une fois qu'on a cliqué dessus[382]. En effet, les informations s'y rapportant sont conservées sur le disque rigide de l'ordinateur utilisé[383]. Il est possible de régler le délai d'expiration de l'historique. Cela signifie que toute trace d'un site visité au-delà de cette limite sera éliminée automatiquement[384]. Cette limite ne pourra être inférieure à un jour. Il est possible d'effacer « manuellement » l'historique en appuyant sur le bouton approprié[385]. Compte tenu que l'historique conserve au moins les données de la journée, il faudra le faire à la fin de chaque session d'utilisation, si l'on veut que ses activités journalières disparaissent de l'historique, et ce, même si l'expiration de l'historique est réglé à zéro.

Les informations conservées indiquent le nom du site visité, son adresse Internet ou URL, sa date ou heure de première consultation, sa date ou heure de dernière consultation, la date d'expiration de l'historique se rapportant aux dates et heures des diverses consultations et le nombre de consultations[386]. Dans le contexte d'une enquête criminelle, il va sans dire que toutes ces informations ont le potentiel d'être fort utiles pour les organismes d'application de la loi, ou fort compromettantes pour un usager[387].

---

376 *Ibid.* aux pp. 188,197-98, 247-48.

377 *Ibid*. à la p. 199.

378 Voir les fonctions des logiciels de navigation *Navigator* de Netscape, en ligne : <http://www.netscape.com/fr> (date d'accès : 11 juin 2001) et *Internet Explorer* de Microsoft, en ligne : <http://www.microsoft.com/france/internet/produits/ie/ie5> (date d'accès : 11 juin 2001).

379 E. Larcher, *L'Internet sécurisé*, Paris, Eyrolles, 2000, aux pp. 142-43 [ci après *L'Internet sécurisé*].

380 *Le guide de l'internaute 2000, supra* note 136 aux pp. 197, 248-50 ; *Internet le guide 2000, supra* note 255 à la p. 60.

381 *L'Internet sécurisé*, *supra* note 379 aux pp. 145-46.

382 *Internet le guide 2000, supra* note 255 à la p. 60 ; *L'Internet sécurisé*, *supra* note 379 aux pp. 144-45.

383 *Le guide de l'internaute 2000, supra* note 136 à la p. 199.

384 *Ibid*. aux pp. 198, 202, 242.

385 *Ibid*. aux pp. 197-98, 250.

386 *Ibid*. à la p. 198.

387 Il existe également des fonctions permettant d'indexer ou de classer les sites visités par un utilisateur. On crée alors des fichiers appelés signets, chemises de sites préférés ou liens personnels. Le contenu de ces fichiers peut également donner un certain historique de navigation, en ce qu'il représente généralement les sites d'intérêt visités par un utilisateur. Ces fichiers sont créés pour accéder plus facilement à des pages Web ou documents favoris. *Le guide de l'internaute 2000, supra* note 136 aux pp. 199-02, 239-40, 250-52 ; *Internet le guide 2000, supra* note 255 à la p. 59. La fonction *Smart Browsing* permet un autre type

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

L'historique de navigation ou de déplacements à long terme et l'historique de la navigation courante ou de déplacements à court terme laissent donc des traces locales, en ce sens qu'elles apparaissent dans l'ordinateur de l'utilisateur[388].

Les *cookies* ou témoins

Un *cookie* est un fichier créé dans l'ordinateur de l'utilisateur par un navigateur Web, à la demande d'un serveur Web d'un site visité. Il peut être déposé sur le système de l'utilisateur à deux occasions : lorsqu'on accède à une page Web ou lorsqu'on télécharge une image[389]. Cela permet de suivre les déplacements d'un utilisateur dans l'espace Web du serveur visité[390]. Le *cookie* a été prévu à la base pour faciliter la vie des utilisateurs du Web[391]. On y trouve des informations qui permettent au serveur Web responsable de sa création, d'enregistrer les préférences ou habitudes de visites d'un utilisateur[392]. Ces statistiques aideront notamment le serveur Web à afficher sur son site, des bannières publicitaires en fonction des habitudes de visite et des préférences d'un utilisateur et de conserver en mémoire les items déposés dans les paniers de magasinage virtuel[393]. Un utilisateur aura le choix d'accepter ou de refuser les *cookies*. Il faudra que son navigateur soit configuré en conséquence[394]. L'utilisateur raisonnable ou ordinaire doit donc effectuer un choix à cet égard.

Le *cookie* contient généralement la date et l'heure de la dernière visite d'un utilisateur sur un site et des informations personnelles ou non qu'il aurait pu inscrire volontairement en

---

d'historique. En effet, il est possible de configurer le logiciel de navigation afin qu'il reconnaisse les premiers caractères tapés par un utilisateur lors de l'inscription de l'adresse dans la case de recherche appropriée. Cette fonction fait en sorte que le logiciel reconnaît les premiers caractères et inscrit automatiquement le reste de l'adresse sans que l'utilisateur n'ait à l'écrire au complet. Cette fonction a donc pour but de faciliter la tâche de l'utilisateur en lui évitant d'avoir à écrire l'adresse au complet. Pour que le logiciel reconnaisse ainsi les premiers caractères, il faut que les adresses tapées soient conservées dans la mémoire de l'ordinateur. C'est ce qui constitue en quelque sorte un historique d'utilisation. Un utilisateur peut activer ou désactiver cette fonction. *Le guide de l'internaute 2000, supra* note 136 à la p. 204.

388 *L'Internet sécurisé*, *supra* note 379 aux pp. 141-42.

389 *Protégez-vous sur Internet, supra* note 207 à la p. 156.

390 *Internet le guide 2000, supra* note 255 à la p. 61.

391 *Protégez-vous sur Internet, supra* note 207 à la p. 156. Ceci est dû principalement au fait que le protocole *HTTP* est un protocole sans état, c'est-à-dire qu'il ne permet pas aux serveurs Web de garder en mémoire un certain nombre d'informations relatives à une succession de requêtes envoyées par un même utilisateur au cours d'une même période. *L'Internet sécurisé*, *supra* note 379 à la p. 161.

392 Normalement, chaque site ne peut accéder qu'aux *cookies* qu'il a crées. Cependant, beaucoup de sites Web passent des accords avec des sociétés dont le seul but est de dresser le profil des utilisateurs. Les *cookies* sont conséquemment presque tous émis par les mêmes sites, qui pourront à loisir consulter la majorité des cookies présents dans le système de l'utilisateur. Ceci permet théoriquement de pouvoir traquer un utilisateur sur les différents sites visités. Voir *Protégez-vous sur Internet, supra* note 207 à la p. 158; *L'Internet sécurisé*, *supra* note 379 à la p. 169.

393 *Le guide de l'internaute 2000, supra* note 136 aux pp. 207, 284, 553 ; *Intrusion Detection*, *supra* note 238 à la p. 140 ; *Protégez-vous sur Internet, supra* note 207 à la p. 156. Voir aussi la description officielle des *cookies* dans la *RFC* 2109, en ligne : <http://www.normos.org/ietf/*RFC*/*RFC*2109.txt> (date d'accès : 5 septembre 2001).

394 *Le guide de l'internaute 2000, supra* note 136 aux pp. 207, 242, 287-88 ; *L'Internet sécurisé*, *supra* note 379 aux pp. 170-75. Il existe également des logiciels qui facilitent la gestion et la destruction des *cookies*. Voir notamment *Cookie Monster*, en ligne : <http://www.geocities.com/paris/1778/monster.html> (date d'accès : 5 septembre 2001) et *Cookie Crusher*, en ligne : <http://www.thelimitsoft.com/cookie.html> (date d'accès : 5 septembre 2001). Un utilisateur peut donc agir pour que ces fichiers ne soient pas constitués contre son gré lors de sa navigation, évitant du coup qu'ils ne se retrouvent dans la mémoire de son ordinateur.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

complétant un formulaire dans ce même site. Le *cookie* pourra conséquemment révéler à ce serveur des informations personnelles au sujet de l'utilisateur à chacune de ses visites, dont son identité personnelle si elle a été révélée dans un formulaire[395]. Il permet également de retracer, à l'aide de l'information colligée, les usagers et de localiser leur ordinateur, notamment en identifiant leur pays d'origine[396].

Le *cookie* agit donc en quelque sorte comme un espion envoyé furtivement, dont le but est la collecte d'informations qu'on pourrait qualifier *prima facie* de confidentielles. L'utilisation des *cookies* s'est généralisée car ils constituent, à l'heure actuelle, une technique de renseignement mercatique d'une exceptionnelle efficacité[397]. La transmission de *cookies*, entre clients et serveurs, permet également d'ajouter une certaine persistance de l'information dans le cadre des transactions Web[398].

Il découle de ces descriptions techniques que les *cookies* pourraient être utilisés par des agents de l'État pour faciliter certaines enquêtes. Il peut s'agir notamment du cas où les organismes d'enquêtes ont eux-mêmes déposés les *cookies* dans la mémoire de l'ordinateur d'un individu, du cas où les agents de l'État recueillent des *cookies* dans la mémoire de celui-ci, ou du cas où les agents de l'État recueillent des informations relatives aux *cookies*, se trouvant chez des tiers qui les ont déposés dans la mémoire de l'ordinateur d'un individu. De par la nature des interventions, les deux derniers cas sont les plus susceptibles de soulever des immixtions étatiques dans la sphère de vie privée d'un individu. Le premier cas est moins certain, car le dépôt du *cookie* serait effectué automatiquement suite à une visite sur un site Web. Il découle en quelque sorte de la navigation et peut être la conséquence d'une configuration inadéquate du navigateur[399]. Finalement, il faudra aussi se demander si les *cookies* ainsi déposés révéleront effectivement des informations ayant un caractère personnel et privé au sens de l'arrêt *Dyment*. Il faudra, à notre avis, le déterminer dans chaque cas d'espèce.

La mémoire cache

La mémoire cache ou simplement « la cache », est un fichier créé par le navigateur Web, dans lequel on emmagasine une foule d'informations sur la navigation d'un utilisateur. Pour ce faire, un navigateur conserve dans le cache une copie transitoire de la page ou document Web visité. Le but de cette opération est de faciliter la tâche d'un utilisateur pour retrouver un site déjà visité. On y retrouvera des images et des sources HTML de pages Web visitées récemment. Il s'agit en fait d'un fichier conservant l'identité et une copie des pages Web consultées[400]. L'historique de navigation ou de déplacements à long terme, utilise la cache pour stocker l'information nécessaire à son fonctionnement. Un utilisateur pourra déterminer

---

[395] *Le guide de l'internaute 2000, supra* note 136 à la p. 286 ; *L'Internet sécurisé*, *supra* note 379 aux pp. 168-69.

[396] *Droit du Cyberespace*, *supra* note 8 à la p. 11-44 ; *Internet le guide 2000, supra* note 255 à la p. 61.

[397] *La criminalité sur l'Internet, supra* note 339 à la p. 69.

[398] *L'Internet sécurisé*, *supra* note 379 à la p. 162.

[399] Une enquête effectuée par le journaliste Pierre Tourangeau en mars 2001, démontre que dix des cent vingt-cinq sites Web du gouvernement canadien déposent systématiquement des cookies dans la mémoire des visiteurs de leur sites. Quatre le feraient sans avis préalable, dont la commission des droits de la personne ! Voir Tourangeau, Pierre, « Les gouvernements ont les internautes à l'œil » (2001), Radio-Canada.ca-Zone nouvelles, en ligne : <http://src.ca/url.asp?/nouvelles/index/nouvelles/200103/02/004-cookies.asp> (date d'accès : 2 mars 2001). L'existence ou non d'un avis, pourra avoir une influence sur le niveau d'expectative raisonnable de vie privée d'un visiteur.

[400] *Le guide de l'internaute 2000, supra* note 136 à la p. 207 ; *Internet Law*, *supra* note 332 aux pp. 138-39.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

combien de pages ou documents pourront être contenus dans la cache en en fixant la capacité de stockage[401].

Il sera également possible d'utiliser des logiciels spécialisés qui font le « ménage » des traces laissées dans la mémoire cache à la fin de chaque utilisation[402].

Les fichiers *log* ou de journalisation

Le fait d'utiliser des ressources dans le Web, génère des enregistrements ailleurs que sur l'ordinateur de l'utilisateur. Il s'agit de la notion de traces distantes[403]. En effet, chaque serveur Web accédé dispose d'un ou plusieurs fichiers qui enregistrent de nombreuses informations relatives aux ordinateurs, aux logiciels de navigation et même aux individus accédant à n'importe quel document proposé par le serveur. Chaque visite chez un serveur sera donc en quelque sorte enregistrée dans des fichiers appelés fichiers *logs* ou *log files*. Des informations concernant l'utilisateur y sont laissées à chaque branchement : la date et l'heure de visite du site et de consultation des pages, le type et la version du navigateur Web utilisé, le type d'ordinateur ou d'architecture matérielle, le type et la version du système d'exploitation utilisé, le nom de la machine du client ou par défaut son adresse IP, les noms de groupe et d'utilisateurs optionnels, lorsque l'accès à une partie du site requiert une authentification, le contenu de la ligne de commande (méthode, fichier accédé ou consulté, version du protocole HTTP), la taille des données éventuellement émises, la page demandée ou pour laquelle il y a eu tentative de demande, le type de logiciel d'exploitation utilisé et l'identité de la page visitée auparavant, donc la provenance de l'utilisateur et le contenu de la recherche effectuée pour arriver au serveur[404].

L'administrateur de site Web ayant accès en principe à toutes ces informations, il devient possible de connaître les moindres faits et gestes des utilisateurs. Il est même possible, comme nous l'avons vu précédemment, d'inférer la localisation géographique d'un utilisateur, grâce à la manière dont sont écrits les noms de domaine[405]. Un utilisateur qui ne prend pas les mesures nécessaires pour contrer ces traces distantes qui sont constituées lors de l'utilisation normale du Web, risque fort de n'avoir aucune expectative raisonnable de vie privée eu égard à toutes les informations énumérées ci-haut.

Il existe plusieurs manières d'empêcher ce type de traces, dont la mise en place de *firewall* ou passerelle coupe-feu et l'utilisation de *proxy server*[406]. Nous n'entrerons pas dans le détail de

---

401 *Le guide de l'internaute 2000, supra* note 136 aux pp. 241-42.

402 Voir notamment le logiciel *Norton Clean Sweep* de la firme *Symantec*, en ligne : <http://www.symantec.com/sabu/qdeck/ncs/features.html> (date d'accès : 10 septembre 2001), qui permet d'effacer les programmes, fichiers, et autres informations indésirables qui proviennent de l'utilisation d'Internet, dont les cookies, les pages Web, les *URL*, etc. (consulté le 13 septembre 2001).

403 *L'Internet sécurisé*, *supra* note 379 à la p. 150.

404 *Le guide de l'internaute 2000, supra* note 136 à la p. 285 ; *L'Internet sécurisé*, *supra* note 379 aux pp. 150-54, 158.

405 *L'Internet sécurisé*, *supra* note 379 à la p. 152.

406 Le « *proxy server* » ou « serveur mandataire », désigne un logiciel de sécurité servant d'intermédiaire entre le navigateur d'un internaute utilisant un réseau local protégé par un coupe-feu, et le serveur Web qu'il veut consulter, permettant ainsi à des données de sortir du réseau local et d'y entrer, sans mettre en danger la sécurité du réseau. Les serveurs mandataires, d'abord créés pour des raisons de sécurité, ont évolué pour devenir également des serveurs caches. Le « *firewall* » ou « coupe-feu », est un dispositif informatique qui permet le passage sélectif des flux d'information entre un réseau interne et un réseau public, ainsi que la neutralisation des tentatives de pénétration en provenance du réseau public. Office de la langue française,

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

ce type de techniques, car cela dépasserait largement le cadre de notre étude. Il suffit de retenir qu'il s'agit principalement de la mise en place de composantes matérielles et/ou logicielles permettant notamment la protection de l'identité des utilisateurs accédant à Internet à partir d'un réseau ou par l'entremise d'un fsI. En plus d'être compliquées pour un utilisateur ordinaire, ces techniques procurent un anonymat relatif; certaines informations restent toujours disponibles pour fins d'enregistrement, dont le type de navigateur utilisé[407].

Pour l'utilisateur ordinaire, les techniques favorisant l'anonymat sont les plus simples à utiliser et les plus sûres[408]. Nous en discuterons plus loin dans la section traitant des technologies particulières ayant une influence sur le caractère privé des communications effectuées dans les divers contextes apportés par Internet et les nouvelles TI.

Constats des limites à l'expectative raisonnable de vie privée lors de la recherche et de la publication d'information effectuées par le biais d'un navigateur Web et de l'établissement d'une communication sécurisée

Le constat le plus évident en matière d'expectative raisonnable de vie privée est sûrement celui découlant de la publication volontaire d'information disponible par le biais d'un navigateur Web. Pour les fins de la présente étude, cette publication s'effectuera par le biais d'une page ou site Web.

En effet, une personne qui publie une page Web afin qu'elle soit accessible par le biais d'un navigateur, peut difficilement invoquer une quelconque expectative raisonnable de vie privée à l'égard de son contenu. La nature même de la publication dans le Web est de rendre l'information accessible. Une personne voulant rester anonyme n'y publiera certainement pas une page Web ! En effet, les multiples moteurs de recherche répertorient pratiquement toute l'information publiée par le biais d'une page Web[409].

2001, *s.v.* « serveur mandataire » et « coupe-feu », en ligne : <http://www.olf.gouv.qc.ca/ressources/internet/fiches/2075113.htm> et <http://www.olf.gouv.qc.ca/ressources/internet/fiches/1299082.htm> (date d'accès : 12 novembre 2001)

[407] *L'Internet sécurisé*, *supra* note 379 aux pp. 155-57.

[408] *Ibid*. à la p. 157.

[409] Cette affirmation est encore plus vraie depuis que le moteur de recherche *Google*, en ligne :<http://www.google.com> (date d'accès : 12 novembre 2001), permet depuis le 9 novembre 2001, d'effectuer des recherches, non seulement de fichiers HTML et d'autres fichiers de même type généralement repérables dans le Web, mais également de fichiers qu'on ne pouvait y trouver. Il s'agit des fichiers de type *Adobe PostScript*, *Lotus 1-2-3*, *WordPro, MacWrite*, *Microsoft Excel*, *Power Point*, *Word*, *Works and Write* et des fichiers de type *RTF* (*Rich Text Format*) Il est également possible avec ce moteur de recherche de trouver des images en classant les résultats par type de couleur, fichiers ou de noms de domaine. Tous ces nouveaux types de documents, auraient augmenté de 35 millions, le nombre de fichiers disponibles pour fins de repérage. *CNET News.com*, en ligne : <http://www.news.cnet.com/news/0-1005-200-7801931.html?tag=prntfr> (date d'accès : 12 novembre 2001). De plus, suite à l'entente des pays membres du G-8 en matière d'entraide juridique informatique, il n'est pas nécessaire de requérir l'aide d'un pays membre, si l'obtention des données peut s'effectuer à partir d'une source accessible au public ou « *publicly available (open Source) data* ». Voir l'article 6 de l'Annexe 1 du communiqué. Communiqué, *Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime* (Moscou, 19-20 octobre, 1999), en ligne : Ministère des affaires étrangères et du commerce international <http://www.g8.gc.ca/1999/moscow1-f.htm> (date d'accès : 9 novembre 2001). Finalement le *Projet de Convention sur la cybercriminalité* du Conseil de l'Europe, prévoit également qu'aucune demande d'entraide n'est requise, lorsque les données sont accessibles au public. Conseil de l'Europe, A.P., 55e session, *Projet de Convention sur la cybercriminalité* (2001), art. 32, en ligne : <http://conventions.coe.int/treaty/fr/projets/FinalCybercrime.htm> (date d'accès : 19 septembre 2001). L'information publiée dans Internet qui est accessible au public ne devrait donc pas, en

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

La seule limite à ce constat est la mise en place d'une page Web accessible seulement à un nombre restreint d'utilisateurs. Cet accès est généralement réservé à des membres qui accèdent aux services offerts par le biais d'un mot de passe et d'un code d'usager. La page d'accueil du site Web sera généralement accessible à tous, ce qui ne conférera pratiquement jamais d'expectative raisonnable de vie privée. La navigation à l'intérieur du site dépendra de l'accessibilité permise par la personne offrant le service. Dans ce cas, on pourra prétendre à une certaine expectative raisonnable de vie privée quant au contenu non accessible. Le niveau d'expectative sera notamment tributaire de la facilité avec laquelle on accède au site et au nombre de membres y ayant accès. Plus l'accès est facile ou plus l'accès est accordé à un grand nombre d'utilisateurs, moins il y aura une expectative raisonnable de vie privée élevée eu égard au contenu du site[410].

Le niveau d'expectative raisonnable de vie privée d'une personne qui publie involontairement de l'information dans Internet est plus complexe. Il s'agit de celle qui recherche de l'information par le biais d'un navigateur et qui, en principe, laissera des traces malgré elle. Il en est de même pour l'expectative raisonnable de vie privée d'une personne sur qui on publie de l'information dans Internet sans égard à sa volonté. Nous traiterons de ces deux situations dans l'ordre.

Il faut savoir que l'architecture d'Internet n'a jamais été prévue pour préserver l'anonymat des personnes qui l'utilisent[411]. Il existe même de nombreux programmes Internet standards, conçus spécifiquement pour suivre et identifier les utilisateurs; la raison principale est la nécessité de pouvoir suivre les consommateurs qui achètent par le biais d'Internet. Le commerce électronique n'est donc pas étranger à toutes ces méthodes de suivi et de recherche[412].

La navigation laissera des traces inhérentes à l'utilisation d'Internet. Nous croyons que nul n'est complètement anonyme dans l'Internet. L'utilisation d'un navigateur Web ne fait pas exception :

> « […] *chaque consultation de serveur Web, chaque page visitée, chaque clic sur un lien laisse non pas une mais plusieurs traces, aussi bien sur l'ordinateur du surfeur que sur les sites qu'il visite, voire ailleurs…* »[413]

Il ne faut pas oublier que chaque ordinateur branché au réseau est identifié par une adresse IP qui lui est propre. Toute personne consultant un site Web se fait nécessairement envoyer des

---

principe, bénéficier d'aucune expectative raisonnable de vie privée. Tout ce jouera dans le sens des mots « accessible au public ».

410 Il est intéressant de noter que la Cour du Québec dans *Morin*, *supra* note 121, n'a pas considéré un babillard électronique, qui est en quelque sorte l'ancêtre des pages ou sites Web, comme étant un lieu ou l'on pouvait bénéficier d'une expectative raisonnable de vie privée, notamment en raison du fait que l'accusé avait sollicité le public en général à accéder au babillard en faisant de la publicité sur d'autres babillards électroniques. La Cour a considéré qu'il s'agissait, à toute fin pratique, d'un lieu commercial ne bénéficiant pas d'une protection en matière de vie privée. Une situation semblable pourrait également s'appliquer dans le contexte d'un site Web accessible à certains membres seulement. Le fait que le site soit accessible à certains membres ne sera pas en soi un critère déterminant dans l'appréciation de son caractère privé.

411 S. Garfinkel, *Architects of the Information Society*, Cambridge, MIT Press, 1999.

412 *Sécurité Optimale, supra* note 208 à la p. 577.

413 *L'Internet sécurisé*, *supra* note 379 à la p. 141.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

informations qui seront traitées par son ordinateur. Cet échange est inhérent au fonctionnement de l'approche client-serveur. Cette personne laisse ainsi une adresse et donc une trace de son passage sur le site qu'elle a visité[414]. Comme nous l'avons vu, les traces du passage d'une personne sur un site Web peuvent également se retrouver dans l'ordinateur de l'usager. Le niveau d'expectative raisonnable de vie privée sera conséquemment tributaire du contrôle exercé par un utilisateur sur les traces qu'il laisse soit dans son ordinateur, soit dans un ordinateur distant.

Les traces laissées dans son propre ordinateur peuvent diminuer l'expectative raisonnable de vie privée si l'utilisateur n'a pas le contrôle complet de son ordinateur. En effet, si cet ordinateur se trouve dans un lieu public, ces traces pourront facilement être consultées par un utilisateur subséquent ou par la personne responsable des lieux. L'exemple le plus évident est celui d'un utilisateur qui ne vide pas la mémoire cache ou l'historique de navigation dans le contenu de la mémoire d'un ordinateur situé dans un cybercafé ou dans une bibliothèque se trouvant dans une institution d'enseignement ou dans un lieu public, ou même et surtout, sur les lieux du travail[415]. Dans ce contexte, pourra-t-il invoquer qu'il existait une attente raisonnable de vie privée quant au contenu de la mémoire cache face à un utilisateur subséquent? Nous croyons que non. Le même problème peut également survenir dans le contexte où l'ordinateur utilisé fait partie d'un réseau interne. Un administrateur faisant l'entretien du réseau pourra tomber dans un fichier de l'utilisateur contenant des traces de visite sur des sites Web.

Quant aux traces laissées sur les ordinateurs distants, le niveau d'expectative raisonnable de vie privée à leur égard sera tributaire de la relation de confiance établie entre l'administrateur du site Web et l'utilisateur. Cette relation de confiance variera grandement selon le site visité. Il faudra donc, dans chaque cas, évaluer s'il existait ou non une relation empreinte de confidentialité entre l'utilisateur et, le plus souvent, la société qui gère le site.

Certaines autres mesures peuvent être envisagées pour éviter de laisser des traces de navigation sur un ordinateur distant. Il s'agit de la navigation anonyme. Nous y reviendrons plus en détail dans la section traitant des Technologies particulières influant sur le caractère privé des communications effectuées dans les contextes apportés par Internet et les nouvelles TI.

Il y a aussi l'expectative raisonnable de vie privée d'un individu à l'égard duquel l'information est publiée dans Internet, sans intervention directe de sa part. Nous l'avons vu, les moteurs de recherche ont pour principale fonction de rechercher. C'est donc la nature même d'Internet, avec ses quantités incommensurables d'informations, qui fait en sorte que l'on peut les obtenir et les consulter. Le Web facilite l'obtention de ces informations.

Les moteurs de recherche Internet disponibles dans le Web ne servent pas seulement à trouver des sites d'intérêt. À l'instar des annuaires téléphoniques, ils peuvent notamment servir à trouver l'adresse de courriel d'une personne[416] et les noms et numéros de téléphone des

---

[414] En effet, un journal d'accès au serveur est constitué par l'administrateur du site Web, ce qui permet de savoir qui est branché et à quel moment. *Le guide de l'internaute 2000, supra* note 136 à la p. 285.

[415] *L'Internet sécurisé*, *supra* note 379 à la p. 142.

[416] Fonction disponible sur le moteur de recherche *Alta Vista*, en ligne : <http://www.altavista.com> (date d'accès : 24 avril 2001). Il suffit d'entrer le nom d'une personne entre guillemets dans la case appropriée et de lancer la recherche sur le Web. On pourra également lancer une recherche *Usenet* à partir d'Alta Vista.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

utilisateurs d'Internet[417]. Ils peuvent également servir à obtenir les informations requises pour fins d'enregistrement et de mise en place d'un site Web, notamment les adresses de serveurs de noms de domaine, les contacts techniques, le numéro de téléphone et l'adresse[418]. C'est l'utilisation conjointe de ces ressources qui fait des moteurs de recherche un outil puissant. Ces ressources basent principalement leur recherche sur les informations découlant des adresses de courriel et IP (Internet) [419]. Il est loin d'être certain qu'un utilisateur raisonnable sait que toutes les informations, en principe publiques, sont facilement devenues concentrées et accessibles et qu'elles peuvent faire l'objet de recoupements.

Certains argumenteront que la nature même d'Internet fait en sorte que l'information y circule librement et que chaque utilisateur accepte implicitement de se faire surveiller. D'autres diront que le type de recherche qu'il permet, notamment par le biais des moteurs de recherche, n'aurait jamais été possible auparavant et que, pour ce faire, les agents de l'État auraient eu besoin de moyens et de ressources inestimables pour pouvoir y arriver. Il s'agit en fait de la concentration de l'information. En fait, Internet rend l'information publique « absolument publique », alors qu'avant, comme par exemple dans le cas d'un bottin téléphonique en papier strictement régional, elle était « relativement publique ». Les tenants de la position voulant que ce type de recherche était impossible auparavant réclament donc un certain contrôle. Dans le contexte de la présente étude, il s'agira de l'obtention d'une autorisation judiciaire quelconque, préalable à toute recherche effectuée dans le Web. Les tenants de la position voulant que l'information circule librement, s'opposent à toute forme de permission préalable pour effectuer une recherche dans le Web au sujet d'un individu.

Nous sommes d'avis qu'une forme d'autorisation judiciaire devrait être exigée avant que les organismes d'application de la loi puissent procéder de façon systématique à une recherche d'information dite « publique ». Ceci aurait pour but d'éviter que l'État procède systématiquement à une surveillance perpétuelle non contrôlée Par contre, les critères d'obtention d'une telle autorisation, pourraient être moindre que dans le cas où l'information est plus « privée ».

Finalement, l'établissement ou non d'une communication sécurisée, influera sur le niveau d'attente subjective de vie privée d'un utilisateur.

Section II - Le courriel

Nous commencerons cette section en faisant une description générale de la technologie. Ensuite, nous traiterons de la session d'utilisation du courriel, des concepts d'adresse de courriel et de pseudonyme Internet d'un utilisateur, des en-têtes et du corps du message et du rôle du fsI. Nous terminerons en traitant d'une application particulière du courriel, soit le

---

Cette recherche permettra de retrouver le nom dans les groupes de discussion ou de nouvelles *Usenet*. Voir également le moteur de recherche *Lycos*, en ligne : <http://www.lycos.com> (date d'accès : 24 avril 2001).

417 Voir l'importante base de données *World Pages*, en ligne : <http://www.worldpages.com> (date d'accès : 24 avril 2001). Voir également *Whowhere*, en ligne : <http://whowhere.lycos.com> (date d'accès : 2 novembre 2000), qui permet également de retrouver le domicile d'une personne en utilisant une carte géographique établie notamment à partir des coordonnées téléphoniques.

418 L'utilitaire ou programme *WHOIS* permet d'effectuer ce type de recherche. Les informations recueillies peuvent sembler banales, mais jointes à d'autres, elles peuvent devenir significatives, notamment pour déterminer le lieu du domicile d'un utilisateur.

419 *Sécurité Optimale, supra* note 208 à la p. 577.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

service *Listserv* et conclurons avec les constats des limites à l'expectative raisonnable de vie privée lors de l'envoi et de la réception de courriels.

Description générale de la technologie

Le courriel consiste en l'envoi de messages sous format électronique d'une personne à un ou des destinataires dans un réseau informatique[420]. La Cour suprême américaine traite brièvement de cette ressource :

> « *E-mail enables an individual to send an electronic message—generally akin to a note or letter—to another individual or to a group of addressees. The message is generally stored electronically, sometimes waiting for the recipient to check her "mailbox" and sometimes making its receipt known through some type of prompt* »[421].

On retrouve dans *ACLU c. Reno*, la description du courriel dans l'exposé conjoint des faits. On qualifie cette ressource de moyen de communication « un vers un » :

> « *23. One to one messaging. One method of communication on the Internet is via electronic mail, or "e-mail," comparable in principle to sending a first class letter. One can address and transmit a message to one or more other people. E-mail on the Internet is not routed through a central control point, and can take many and varying paths to the recipients. Unlike postal mail, simple e-mail generally is not "sealed" or secure, and can be accessed or viewed on intermediate computers between the sender and recipient (unless the message is encrypted)* »[422].

Nous verrons que le courriel offre beaucoup plus qu'une simple communication « un vers un ». Il s'agit ici de considérer cette catégorisation « un vers un », comme un exposé de principe souffrant de plusieurs exceptions. À première vue, il nous semble que la description du courriel en première instance est plus proche de la réalité technique. Nous sommes plutôt d'avis qu'un courriel envoyé en clair ressemble davantage à une carte postale qu'à une lettre. Nous y reviendrons plus loin.

La session d'utilisation du courriel

Les deux interlocuteurs n'ont pas besoin d'être présents en même temps dans le réseau pour s'en servir. Il s'agit d'un service différé ou asynchrone : un utilisateur destinataire ne recevra pas son courriel tant qu'il ne se branchera pas à sa boite postale[423]. Le courriel y restera aussi longtemps que le destinataire ne le retirera pas. Comme le courrier normal qui transite par différents bureaux de poste, le courriel chevauche différents serveurs dans Internet pour

---

[420] *Le guide de l'internaute 2000, supra* note 136 aux pp. 83-84, 92-96 ; *Internet le guide 2000, supra* note 255 à la p. 66 ; *Protégez-vous sur Internet, supra* note 207 à la p. 108.

[421] *Reno c. ACLU, supra* note 1 à la p. 851.

[422] *Supra* note 196 à la p. 834.

[423] *Le guide de l'internaute 2000, supra* note 136 à la p. 97. On dit également asynchrone par opposition à un appel téléphonique qui fonctionne en mode synchrone. Sauf le cas de l'utilisation de boîtes vocales, les deux interlocuteurs ont besoin d'être sur la ligne en même temps pour se parler. Voir *Internet*, *supra* note 214 à la p. 47.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

finalement arriver à destination. Contrairement au courrier régulier, l'adresse d'envoi ne correspond pas à la boite aux lettres du destinataire. Elle correspond plutôt de l'adresse du serveur qui remplit le rôle de bureau de poste[424].

Même si cette situation est transparente pour l'utilisateur, l'envoi et la réception de courriels font appel à deux services Internet différents. L'envoi d'un courriel se fait via un serveur SMTP. Le canal logique utilisé pour l'envoi de courriel est le port IP 25[425]. Pour reprendre l'analogie du courrier, cette démarche constitue l'équivalent de poster une lettre dans une boîte aux lettres[426]. La réception d'un courriel se fait via un serveur POP3. Cette démarche correspond à la récupération du courrier dans la boîte aux lettres louée au bureau de poste[427]. Le canal logique utilisé pour la récupération de courriels est le port IP 110[428]. Le destinataire utilise un logiciel client POP3 pour récupérer son courriel se trouvant dans le serveur postal. Pour y accéder, un client doit posséder un mot de passe et une identité. Pour reprendre l'analogie du bureau de poste, il s'agira de l'équivalent de l'ouverture à l'aide d'une clé, par le destinataire, de la boîte postale. Cet accès restreint permet d'éviter qu'un tiers accède à la boîte[429].

Entre le serveur SMTP de l'expéditeur et le serveur POP3 du destinataire, une multitude de routeurs ou relais se chargeront de transporter le courriel : ce sera la portion Internet du trajet. Le trajet exact, qui peut varier d'un envoi à l'autre même s'il est fait au même destinataire, est déterminé par le protocole de transport Internet TCP/IP[430]. C'est ici que les paquets d'informations contenant le courriel peuvent emprunter des chemins différents dans Internet. Compte tenu du fonctionnement logiciel et de la configuration matérielle utilisée pour l'envoi d'un courriel, les serveurs SMTP et POP3 se trouvent donc généralement dans des lieux autres que ceux où se trouvent les ordinateurs des expéditeurs et destinataires.

Une multitude de fonctions sont disponibles dans les différents logiciels de courriel. Nous n'énumérerons que les principales, et celles qui, selon nous, ont un impact sur le niveau d'expectative raisonnable de vie privée. De façon générale, un utilisateur de logiciel de courriel peut évidemment composer un message. Il peut répondre à un individu ou groupe, faire suivre, classer ou rediriger ses messages, y joindre des fichiers ou programmes et se constituer un carnet d'adresse. Il peut également obtenir confirmation, par le logiciel client du destinataire, qu'il a reçu et ouvert le courriel envoyé[431].

Certains logiciels de courriels contiennent également des fonctions pour accéder aux groupes de discussion *Usenet*. Nous traiterons spécifiquement des groupes de discussion *Usenet* plus loin. D'autres logiciels permettent la navigation sur le Web et l'envoi et la réception de télécopies[432]. Compte tenu qu'il s'agit là d'utilisations plutôt marginales du courriel, nous n'en traiterons pas.

---

[424] *Protégez-vous sur Internet, supra* note 207 à la p. 112.
[425] *Ibid*. à la p. 74. Voir aussi *Hacking Exposed, supra* note 272 à la p. 658.
[426] *Protégez-vous sur Internet, supra* note 207 à la p. 111.
[427] *Ibid*. à la p. 112.
[428] *Ibid*. à la p. 74. Voir aussi *Hacking Exposed, supra* note 272 à la p. 658.
[429] *Le guide de l'internaute 2000, supra* note 136 à la p. 98.
[430] *Ibid*. à la p. 97.
[431] Pour une discussion détaillée de toutes ces fonctions, voir *Le guide de l'internaute 2000, supra* note 136 aux pp.104-24.
[432] *Ibid*. aux pp. 146-51.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

Finalement, il est également possible d'accéder à sa boite de courriel par le biais d'une page Web. C'est ce qu'on appelle le *Webmail*. Il ne faut pas confondre cette situation avec l'utilisation d'un logiciel de courriel intégré à un navigateur Web. C'est à partir de la page Web du service utilisé que l'on effectuera la majorité des opérations propres au courriel[433].

L'adresse de courriel et le pseudonyme Internet d'un utilisateur

Les utilisateurs du courriel possèdent une identité. L'adresse Internet d'un utilisateur, ou son adresse de courriel, est composée d'un nom d'utilisateur qu'il possède chez son fournisseur d'accès Internet ou à l'intérieur de son organisation, suivi du nom de domaine correspondant. Le nom de l'utilisateur et celui du domaine sont séparés par le désormais célèbre sigle « @ » ou (arobas) afin de pouvoir différencier les entités[434].

Une adresse de courriel dans Internet pourrait ressembler à ceci : « pop123456@justice.gc.ca » où « pop123456 » serait le numéro de compte de l'utilisateur, « justice » serait le nom de réseau, « gc » serait le nom de domaine et « ca » serait le nom de domaine de dernier niveau.

Encore une fois, pour plus de facilité et de convivialité, il est possible de se faire attribuer un pseudonyme Internet. Il s'agit d'un nom plus court utilisé pour désigner l'adresse Internet de l'utilisateur. C'est l'administrateur de réseau de l'organisation ou le fournisseur de service Internet qui peut attribuer un ou des pseudonymes qui pourront tous pointer vers la même personne. Donc, au lieu de l'adresse mentionnée plus haut, on pourra par exemple utiliser « pierrejeanjacques@justice.gc.ca » ou « pjj@justice.gc.ca » pour pointer vers « pop123456@justice.gc.ca ».

Les en-têtes de message

Les en-têtes de message sont créés automatiquement par le logiciel de communication utilisé. Ils contiennent tous les renseignements concernant la logistique du message nécessaire à son bon cheminement dans Internet. Il y a deux types d'en-têtes : l'en-tête de message envoyé et l'en-tête de message reçu.

On retrouvera généralement dans l'en-tête de message envoyé l'adresse du destinataire et de l'expéditeur, le titre du message, les destinataires secondaires, les copies conformes et copies conformes invisibles, l'existence de fichiers joints, la personne à qui répondre, le nombre de lignes que contient le corps du message, le numéro d'identification du message, le standard MIME supporté par le logiciel utilisé pour poster le courriel, des informations relatives au contenu du message et au type d'encodage utilisés, le type d'encodage utilisé, le type de logiciel et de système d'exploitation utilisé pour envoyer le courriel, la date et l'heure d'envoi.

Quant à l'en-tête de message reçu, il contient essentiellement les références, c'est-à-dire les informations relatives au trajet du courriel à travers l'Internet. On y retrouve le chemin parcouru du message pendant son trajet dans Internet en indiquant le nombre de serveurs de courriel qui l'ont traité, la progression chronologique, les coordonnées de l'expéditeur, le titre

[433] *Ibid*. aux pp. 94-95, 98.
[434] *Ibid*. aux pp. 62-63, 92-93.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

du message, les coordonnées du destinataire, le numéro de série du message, le type d'envoi, sa longueur en nombre de caractères et le nom du logiciel utilisé pour effectuer l'envoi. Lors de la réception d'un message, toute l'information relative à l'envoi est également disponible.[435]

Le corps du message

Il s'agit essentiellement du message écrit au destinataire. C'est cette partie qui est assimilée au contenu d'une lettre ou d'une carte postale. Généralement, un message ne dépasse pas 6000 caractères. Dans le cas contraire, le serveur compresse les informations et les envoie comme fichier joint. En pratique, cela ne change rien car l'utilisateur ne s'en rend pas compte étant donné que le fichier joint fait de toute façon partie du corps du message.[436] On retrouve généralement, à la fin du message, la signature électronique[437] de l'expéditeur.

Le rôle du fournisseur de service Internet ou fsI

Le fsI, dans le contexte du courriel, joue essentiellement un rôle d'administrateur. Le fsI travaille généralement pour le compte d'une compagnie privée. Il voit à l'ouverture de comptes, à l'entretien du système, à la facturation et à la gestion du bon fonctionnement du service.

Lorsque le fsI accomplit sa fonction d'entretien du système, il est probable qu'il prenne connaissance du contenu de certains messages et de leurs fichiers joints. Lorsque cela se produit, dans la mesure où cette action n'est pas commandée par un organisme d'application de la loi, le fsI n'accomplit pas une fonction gouvernementale. Il n'est donc pas visé par l'application de la *Charte* canadienne ni n'est assimilé à Postes Canada et aux obligations qui en découlent[438].

La nature même de toute transmission par courriel fait en sorte que ce dernier passe de l'ordinateur client de l'expéditeur à l'ordinateur serveur du fsI de l'expéditeur. À partir de ce fsI, différentes recherches sont effectuées par l'ordinateur pour établir un chemin afin de s'assurer que le message de l'expéditeur se rende au fsI du destinataire.

Ce chemin peut comprendre une multitude de nœuds Internet avant que le fsI du destinataire ne soit joint. Le courriel pourra donc être compromis et ses en-têtes modifiés par n'importe quel nœud dans le système.

---

[435] *Le guide de l'internaute 2000, supra* note 136 aux pp. 99-03. Voir aussi *Protégez-vous sur Internet, supra* note 207 aux pp. 115-23.

[436] *Le guide de l'internaute 2000, supra* note 136 à la p. 103 et *Protégez-vous sur Internet, supra* note 207 aux pp. 124-29.

[437] Il ne faut pas confondre ici « signature électronique » qui n'est qu'une représentation graphique électronique de notre signature manuscrite et « signature numérique » qui indique l'utilisation de la cryptographie à clé publique et fonction de hachage servant à authentifier un document et à s'assurer de son intégrité. S. Parisien et P. Trudel, *L'identification et la certification dans le commerce électronique*, Cowansville (Qc), Yvon Blais, 1996 aux pp. 93-116 [ci après *L'identification et la certification*] ; *Droit du Cyberespace*, *supra* note 8 aux pp. 19-23 à 19-32.

[438] *Weir*, *supra* note 136 aux para. 43-49.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

Généralement, les courriels ne sont pas examinés par les fsI simplement parce qu'il en existe un nombre considérable et que seuls les messages problématiques attirent l'attention[439]. Par contre, un courriel pourra facilement être examiné, ce qu'un utilisateur normal ne pourra détecter[440].

Les listes de distribution automatisée ou *Listserv*

Comme nous l'avons vu, il est facile d'envoyer des messages à une ou plusieurs personnes à l'aide du courriel. Dans ce dernier cas, il y aura autant d'adresses qu'il y aura de destinataires. Il est également possible de faire parvenir du courrier à plusieurs personnes en n'envoyant le message qu'à une seule adresse. C'est cette opération qui renvoie à la notion de liste de distribution, dont le but le plus souvent visé est de réunir un groupe d'utilisateurs intéressés par le même sujet. Il est en effet plus rapide d'envoyer un message à une liste de plusieurs personnes que d'envoyer le message plusieurs fois à chaque personne[441].

La liste de distribution peut prendre plusieurs formes, dont trois principales. La première est constituée de la liste de contacts fréquents du carnet d'adresses, contenu dans la majorité des logiciels de courriel. Nous ne nous attarderons pas spécifiquement à cette forme qui a déjà été traitée plus haut, lors de la discussion sur le carnet d'adresses. Il suffit de retenir, pour les fins de la présente section, que c'est l'utilisateur qui contrôle son carnet d'adresses, donc la liste de distribution elle-même[442].

Une deuxième forme consiste en un service automatisé de gestion de liste et de distribution ou *Listserv*[443]. On requerra donc les services de ce système de liste de distribution déjà implanté. Les avantages d'une telle liste résident dans le fait que ces services sont entièrement automatisés et qu'ils offrent des fonctions supplémentaires, comme l'archivage et la consultation de tous les messages envoyés, la présentation de statistiques de toutes sortes et la gestion d'erreur de distribution[444]. Encore une fois nous ne traiterons pas en détail de toutes les fonctions du logiciel servant à l'utilisation de ce type de service. Nous ne nous attarderons que sur celles pouvant avoir une influence, dans un sens ou dans l'autre, sur l'expectative raisonnable de vie privée.

La Cour suprême américaine définit ce type de liste de distribution :

---

[439] Le programme d'interception *Carnivore* pourrait changer les données. En effet, ce programme permet au F.B.I. de procéder à l'interception systématique des courriels et de faire des recherches par mots clés de façon automatique. Voir United Sates, Department of Justice, *Independant Technical Review of the Carnivore System Draft Report*, *ITT Research Institute*, 2000 (auteurs : Smith, Stephen P., Perrit, Jr., Henry, *et al.*), en ligne : <http://www.usdoj.gov/jmd/publications/carnivore_draft_1.pdf> (date d'accès : 24 août 2001) et *Carnivore*, en ligne : <http://www.fbi.gov/hq/lab/carnivore/carnivore.htm> (date d'accès :24 août 2001). La technologie *Assentor* permet quant à elle d'effectuer une recherche intelligente relative au contenu des courriels, voir *Assentor*, en ligne : <http://www.assentor.com> (date d'accès : 31 octobre 2000).

[440] *Weir*, *supra* note 136 au para. 60.

[441] *Le guide de l'internaute 2000, supra* note 136 à la p. 137.

[442] *Ibid*. aux pp. 137-140.

[443] Voir *Listserv*, en ligne : <http://www.lsoft.com> (date d'accès : 5 septembre 2001).

[444] *Le guide de l'internaute 2000, supra* note 136 à la p. 141.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

> « *A mail exploder is a sort of e-mail group. Subscribers can send messages to a common e-mail address, which then forwards the message to the group's other subscribers* »[445].

Une description plus complète de la technologie est avancée en première instance. On la qualifie de moyen de communication « un vers plusieurs » :

> « *24. One-to-many messaging. The Internet also contains automatic mailing list services (such as "listservs"), [also referred to by witnesses as "mail exploders"] that allow communications about particular subjects of interest to a group of people. For example, people can subscribe to a "listserv" mailing list on a particular topic of interest to them. The subscriber can submit messages on the topic to the listserv that are forwarded (via e-mail), either automatically or through a human moderator overseeing the listserv, to anyone who has subscribed to the mailing list. A recipient of such a message can reply to the message and have the reply also distributed to everyone on the mailing list. This service provides the capability to keep abreast of developments or events in a particular subject area. Most listserv-type mailing lists automatically forward all incoming messages to all mailing list subscribers. There are thousands of such mailing list services on the Internet, collectively with hundreds of thousands of subscribers. Users of "open" listservs typically can add or remove their names from the mailing list automatically, with no direct human involvement. Listservs may also be "closed," i.e., only allowing for one's acceptance into the listserv by a human moderator* » [notes omises][446].

Pour pouvoir participer à une liste de distribution automatique, il faut s'inscrire en s'abonnant. On pourra également se désabonner du service ou joindre l'administrateur du service en cas de problème[447]. Il est aussi possible de connaître la description de la liste et de ses abonnés avec la commande *review*. Pour contrer ce type de demande, donc pour faire en sorte que le nom d'un abonné ne soit pas divulgué, un utilisateur pourra activer la commande *set conceal*. Cette commande peut bien entendu être désactivée par une autre commande lancée par l'utilisateur, soit *set noconceal*.

La troisième forme est en quelque sorte un croisement entre la première et la deuxième. Il est en effet possible de recourir aux services de firmes spécialisées offrant des sites où il sera possible de créer sa propre liste de distribution automatisée[448]. Une personne voulant créer une telle liste devra déterminer plusieurs paramètres avant de pouvoir rendre la liste accessible. Il faudra donc répondre à quelques questions concernant l'identité de la personne créant une nouvelle liste, le thème de la liste et la sécurité l'entourant. Quant à ce dernier aspect, il faudra notamment décider si n'importe qui peut se joindre anonymement à la liste ou si celle-ci ne sera réservée qu'à quelques utilisateurs[449].

---

[445] *Reno c. ACLU, supra* note 1 à la p. 851.
[446] *ACLU c. Reno, supra* note 196 à la p. 834.
[447] *Le guide de l'internaute 2000, supra* note 136 à la p. 142.
[448] Voir notamment *Egroup*, en ligne : <http://www.egroups.com> (date d'accès : 8 septembre 2001) et *Coolist*, en ligne : <http://www.coolist.com> (date d'accès : 8septembre 2001).
[449] *Le guide de l'internaute 2000, supra* note 136 aux pp. 145-146.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

Finalement, il est important de mentionner qu'il existe des moteurs de recherche et des répertoires de listes servant à trouver les listes de distribution de tous genres[450]. Il y a plus de 91 000 listes publiques présentement dans Internet regroupant plus de 74 000 000 d'utilisateurs et générant un volume quotidien d'environ 53 000 000 de messages[451]. Il s'agit donc d'une mine incommensurable de messages qui pourraient être intéressants à consulter pour les organismes d'application de la loi, compte tenu des fonctions d'archivage de messages que certaines listes de distribution offrent.

Constats des limites à l'expectative raisonnable de vie privée lors de l'envoi et la réception de courriel

Seulement quelques décisions en matière criminelle au Canada traitent spécifiquement du sujet[452]. Dans *R. c. Weir*[453], on reprochait à l'accusé d'avoir eu en sa possession de la pornographie juvénile, contrairement à l'article 163.1(4) du *Code criminel*. Un employé d'un fsI, procédant à une réparation de routine dans la boite postale de courriel de l'accusé, a découvert un message contenant des fichiers joints douteux. Ces fichiers joints contenaient ce que les responsables du fsI ont considéré comme étant de la pornographie juvénile. Conséquemment, ils ont avisé les policiers de la situation. Ceux-ci ont exigé du fsI qu'on leur envoie une copie du message et des fichiers joints. Forts de ces informations, les policiers ont pu subséquemment obtenir un mandat de perquisition permettant de fouiller le domicile de l'accusé. Du matériel illicite y a été découvert, d'où les accusations.

La Cour devait déterminer si M. Weir bénéficiait d'une expectative raisonnable de vie privée à l'égard de l'information transmise initialement par son fsI aux policiers. Le cas échéant, cette information, obtenue illégalement, n'aurait pu faire partie des motifs au soutien de la dénonciation pour l'obtention subséquente du mandat de perquisition. Ceci aurait pu avoir comme conséquence que la preuve obtenue au domicile de l'accusé n'aurait pu être utilisée contre M. Weir au procès. La Cour a déterminé que M. Weir ne bénéficiait pas d'une protection en vertu de l'article 8 de la *Charte canadienne* à l'égard de l'information transmise initialement à son insu. La Cour a d'abord déterminé que les fsI, de par leur fonction ordinaire, n'agissaient pas à titre d'agent de l'État et n'exerçaient pas une fonction assimilable à un organisme gouvernemental, tel que Postes Canada. Un fsI, dans ses fonctions ordinaires, agit donc comme une partie privée. En principe, les actions qu'il pose à l'égard de sa clientèle, en l'espèce la copie initiale des fichiers douteux, ne seraient pas susceptibles d'entraîner une application de la *Charte canadienne* :

> « *In my view, it cannot be said that the ISP was performing a governmental function. ISPs are private organizations. They are unregulated* »[454].

Ensuite la Cour a décidé que la remise subséquente des fichiers douteux aux policiers, ne constituait pas une fouille, saisie ou perquisition sans mandat effectuées par ceux-ci. Aux

---

[450] Voir notamment Francopholistes, en ligne : <http://www.cru.fr/listes> (date d'accès : 24 août 2001) et *CATALIST*, en ligne : <http://www.lsoft.com/lists/listref.html> (date d'accès : 24 août 2001).

[451] *Le guide de l'internaute 2000, supra* note 136 à la p. 144.

[452] *Weir, supra* note 136 ; *Tremblay*, *supra* note 122 ; *Gauthier*, *supra* note 135. Pour un exemple où un organisme d'application de la loi a notamment demandé l'autorisation d'intercepter des courriels et toute communication Internet, voir *R. c Blizzard*, [2001] N.B.J. No. 18, au par. 3.

[453] *Weir*, *supra* note 136.

[454] *Weir*, *supra* note 136 au para. 46.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

yeux de la Cour, les fichiers douteux ne constituaient que l'extension des informations transmises par un informateur, en l'espèce le fsI. En définitive, les fichiers ne faisaient que corroborer les dires du fsI, qui étaient par ailleurs suffisants en soi, aux fins de l'obtention subséquente du mandat visant la résidence de Weir :

> « *The characterization of the taking of the copy of the e-mail as a warrantless search is urged upon me strenuously by the defense. In my view, the facts of the case cannot be characterized in this fashion for these reasons. By the time the ISP called the police its employees had already formed a strong belief that the message on the system was child pornography and was illegal. It is as an informant, can pass that belief to the police. The copied e-mail was not necessary to give the police the reasonable and probable grounds. It was not a seizure of evidence, despite the use of the terminology by Detective Sidor. Rather it was corroboration as to the detail or texture of the informant's tip* »[455].

Contrairement à ce qui avait été décidé en première instance, la remise subséquente, aux autorités policières, des fichiers contenant les images pornographiques infantiles obtenues par le fsI, constitue, aux yeux de la Cour d'appel de l'Alberta, une « fouille » au sens de l'article 8 de la *Charte canadienne*[456]. Cette fouille, effectuée sans mandat, était donc présumée abusive. Les images contenant de la pornographie infantile auraient donc dû, en principe, être exclues de la preuve. En l'espèce, ceci aurait eu pour effet probable d'invalider le mandat de perquisition subséquent, obtenu en partie sur la foi des renseignements découlant de l'obtention des images de pornographie infantile. La Cour n'a pas invalidé le mandat de perquisition subséquent, parce que l'information, au sujet de l'existence de fichiers contenant de la pornographie infantile, avait été obtenue verbalement de la part des policiers. Donc, même si les fichiers compromettant étaient exclus, le reliquat des motifs était amplement suffisant pour justifier l'émission du mandat subséquent visant le domicile de Weir. Le résultat reste donc le même par rapport à cette question. Seule la « mécanique » pour y arriver a changé. Cette nouvelle mécanique aura par contre comme conséquence de confirmer que les fsI deviennent effectivement des agents de l'État lorsqu'ils remettent, à la demande des agents de l'État, la preuve préalablement obtenue. Les agents de l'État devront donc se prémunir d'une autorisation judiciaire avant de pouvoir accéder à cette information, sinon son obtention sera considérée comme une fouille sans mandat, donc présumée abusive, risquant d'en compromettre l'admissibilité. La Cour d'appel de l'Alberta, ne s'est par contre pas penchée sur la notion d'expectative raisonnable de vie privée rattachée au courriel. Il faut donc s'en remettre à la décision de première instance sur cette question.

La Cour en première instance a déterminé qu'un utilisateur bénéficiait d'une expectative raisonnable de vie privée, du moins quant au corps ou contenu du message :

> « *On the evidence before me, together with Ms. Berton's article and the finding in Maxwell, I am persuaded that e-mail with the ISP carries an expectation of privacy. Therefore, judicial pre-authorization (a warrant) will usually be required to search and seize it. […] In summary, I am*

[455] *Weir*, *supra* note 136 au para. 54.
[456] Voir *Weir*, 2001 ABCA 181, *supra* note 136.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

> *satisfied e-mail via the Internet ought to carry a reasonable expectation of privacy* »[457].

Cette conclusion est en partie basée sur un passage de la décision américaine rendue dans *United States c. Maxwell*[458], qui affirmait :

> « *However we find appellant definitely maintained an objective expectation of privacy in any e-mail transmissions he made so long as they were stored in the America Online computers.*
>
> *In our view, the appellant clearly had an objective expectation of privacy in those messages stored in computers in which he alone could retrieve through the use of his own assigned password. Similarly, he had an objective expectation of privacy with regard to messages he transmitted electronically to other subscribers of the service who also had individually assigned passwords. Unlike transmissions by cordless telephones, or calls to a telephone with six extensions, or telephone calls which may be answered by anyone at the other end of the line, there was virtually no risk that the appellant's computer transmissions would be received by anyone other than the intended recipients* »[459].

Par contre, la décision dans *Maxwell* a été en partie renversée et confirmée subséquemment notamment quant à la question relative à l'expectative raisonnable de vie privée rattachée à un courriel[460]. Conséquemment, une des bases du raisonnement avancé dans *Weir* se trouve modifiée. Il faut donc « relire » la décision rendue dans *Weir*, subséquemment confirmée pour d'autres motifs par la Cour d'appel de l'Alberta, avec un *caveat* à l'esprit. De plus, la décision dans *Maxwell 2* est plus conforme à la réalité technologique, ce qui est compatible avec l'approche pragmatique.

La Cour dans *Maxwell 2* a confirmé qu'il existait effectivement une expectative raisonnable de vie privée relative au courriel de l'appelant Maxwell, mais elle apporte un raisonnement différent de celui énoncé dans *Maxwell*.

La Cour a bien précisé dans *Maxwell 2* que c'était le contexte particulier de la relation empreinte de confidentialité entre le fsI *America Online* (ci-après : « AOL ») et son client Maxwell, ainsi que le type de réseau offert par AOL à ses usagers, qui contribuaient en grande partie à faire en sorte qu'un utilisateur de ce service pouvait raisonnablement s'attendre à ce que ses courriels demeurent privés :

> « *AOL differs from other systems, specifically the Internet (see American Civil Liberties Union, et al., v. Reno, 929 F.Supp. 824, 830-44 (E.D.Pa.1996)), in that e-mail messages are afforded more privacy than similar messages on the Internet, because they are privately stored for retrieval on AOL's centralized and privately-owned computer bank located*

---

457 *Weir*, *supra* note 136 aux para. 70, 77.
458 *United States c. Maxwell*, 42 M.J. 568 (A.F. Ct. Crim. App.1995), (ci-après *Maxwell*)
459 *Weir*, *supra* note 136 au para. 69.
460 *Maxwell 2, supra* note 316. Nous nous expliquons mal par ailleurs comment la décision rendue dans *Weir* le 10 février 1998 n'a pas tenu compte de la décision rendue dans *Maxwell 2*, le 21 novembre 1996 !

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

> *in Vienna, Virginia. During her testimony, Ms. Villanueva stated that AOL's policy was not to read or disclose subscribers' e-mail to anyone except authorized users, thus offering its own contractual privacy protection in addition to any federal statutory protections. It was AOL's practice to guard these "private communications" and only disclose them to third parties if given a court order. Just for comparison, the Internet has a less secure e-mail system, in which messages must pass through a series of computers in order to reach the intended recipient. Cf. ACLU v. Reno, supra. While implicit promises or contractual guarantees of privacy by commercial entities do not guarantee a constitutional expectation of privacy, we conclude that under the circumstances here appellant possessed a reasonable expectation of privacy, albeit a limited one, in the e-mail messages that he sent and/or received on AOL. Expectations of privacy, however, have limitations, and this case illustrates some of them »*[461] .

La décision *Maxwell 2* fait donc la distinction entre un courriel qui circule dans Internet de serveur en serveur, jusqu'au serveur du fsI du destinataire, et un courriel qui circule par le réseau d'AOL. Selon *Maxwell 2*, il est plus difficile de cerner le niveau d'expectative raisonnable de vie privée dans le cas d'un courriel circulant dans Internet, notamment parce qu'il existe une multitude de juridictions et relations contractuelles susceptibles d'entrer en jeu entre les différents fsI et l'expéditeur du message. *Maxwell 2* vient donc en quelque sorte limiter l'affirmation qui avait été faite dans *Maxwell*, relative à l'existence d'une expectative raisonnable de vie privée, qui ne semblait être basée que sur la relation de confiance établie entre le fsI et l'usager.

L'attente subjective pourrait, selon toute vraisemblance, être diminuée dans le contexte d'une communication où un courriel circule dans Internet. On a d'ailleurs affirmé dans *Charbonneau* que lorsque l'on envoie un courriel, l'expectative raisonnable de vie privée peut être moindre :

> « *E-mail is almost equivalent to sending a letter via the mails. When an individual sends or mails letters, messages, or other information on the computer, that Fourth Amendment expectation of privacy diminishes incrementally* »[462].

Cette question a été traitée dans *Weir* et on a décidé qu'il y avait suffisamment de preuve pour conclure que la relation entre le fsI de Weir et celui-ci permettait d'établir qu'il y avait effectivement une expectative raisonnable suffisante. À notre avis, il est recommandé d'établir pour chaque cas, la nature du lien contractuel entre le fsI et le sujet visé par l'enquête.

Outre le constat de la nature plus « privée » du réseau AO*L*, la décision *Maxwell 2* précise également une limite intéressante au niveau d'expectative raisonnable de vie privée rattachée à un courriel. En effet, plus il y a de destinataires, moins l'expectative sera élevée. Il en sera

---

[461] *Supra* note 316 à la p. 417 ; *United States c. Charbonneau,* 979 F. Supp. 1177 (S.D. Ohio 1997), à la p. 1184 [ci après *Charbonneau*].

[462] *Charbonneau*, *Ibid*.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

de même, plus le message s'éloigne du premier destinataire, c'est-à-dire si le message est redistribué à d'autres :

> « *E-mail transmissions are not unlike other forms of modern communication. We can draw parallels from these other mediums. For example, if a sender of first-class mail seals an envelope and addresses it to another person, the sender can reasonably expect the contents to remain private and free from the eyes of the police absent a search warrant founded upon reasonable cause . However, once the letter is received and opened, the destiny of the letter then lies in the control of the recipient of the letter, not the sender, absent some legal privilege.*
>
> *Similarly, the maker of a telephone call has a reasonable expectation that the police officials will not intercept and listen to the conversation; however, the conversation itself is held with the risk that one of the participants may reveal what is said to others.*
>
> *Drawing from these parallels we can say that the transmitter of an e-mail message enjoys a reasonable expectation that police officials will not intercept the transmission without probable cause and a search warrant. However, once the transmissions are received by another person, the transmitter no longer controls its destiny. In a sense, e-mail is like a letter. It is sent and lies sealed in the computer until the recipient opens his or her computer and retrieves the transmission. The sender enjoys a reasonable expectation that the transmission will not be intercepted by the police. The fact that an unauthorized "hacker" might intercept an e-mail message does not diminish the legitimate expectation of privacy anyway.*
>
> […] *Expectations of privacy in e-mail transmissions depend in large part on the type of e-mail involved and the intended recipient. Messages sent to the public at large in the "chat room" or e-mail that is "forwarded" from correspondent to correspondent lose any semblance of privacy. Once these transmissions are sent out to more and more subscribers, the subsequent expectation of privacy incrementally diminishes. This loss of an expectation of privacy, however, only goes to these specific pieces of mail for which privacy interests were lessened and ultimately abandoned* » [notes omises][463].

Les fonctions rattachées à la réponse à un courriel posent donc certains problèmes[464]. En effet, les fonctions de réponse à l'auteur d'un message, de réponse à tous les destinataires d'un message, de redirection de message et de celles permettant de faire suivre un message, favorisent une diminution de l'expectative raisonnable de vie privée de l'expéditeur initial du message. Ces fonctions favorisent en quelque sorte, la diffusion d'un courriel aux tiers : un expéditeur n'a pas de contrôle sur ce que le destinataire fera subséquemment du courriel envoyé et reçu. Conséquemment, dans la mesure où le courriel arrive à destination,

---

[463] *Supra* note 316 aux pp. 417-19.

[464] Pour une description générale de ces fonctions, voir *Le guide de l'internaute 2000, supra* note 136 aux pp.105-06.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

l'expéditeur perd un certain degré d'expectative raisonnable de vie privée à son égard, tant au niveau du contenu que des informations techniques s'y rattachant.

Il est à noter que la nétiquette relative au courriel recommande de demander préalablement une autorisation à l'expéditeur, avant de diffuser ou de faire suivre un message[465]. Une personne raisonnable utilisant Internet et un logiciel de courriel devrait être informée de la facilité avec laquelle les messages peuvent être diffusés.

La décision rendue dans *Weir* apporte finalement une distinction dans le cas d'un courriel qui a été chiffré. Dans ce cas, le niveau d'expectative raisonnable de vie privée à l'égard du contenu sera plus élevé que dans le cas du courrier de première classe :

> « *Yet the vulnerability of e-mail requires legal procedures which will minimize invasion. I am satisfied that the current Criminal Code and Charter of Rights protections are adequate when applied in the e-mail environment* »[466].

L'expectative raisonnable de vie privée sera plus élevée à l'égard du contenu en ce qu'il devient pratiquement impossible de le déchiffrer, ce qui n'est pas le cas du courrier de première classe qui n'a que l'enveloppe pour en protéger physiquement le contenu. Nous sommes d'avis qu'une personne qui chiffrera un courriel aura au moins une expectative raisonnable de vie privée subjective plus élevée.

Quant aux en-têtes, on a déterminé dans *Weir* que l'expectative raisonnable de vie privée était moindre.[467] On pourrait donc, dans ce cas, voir une norme moins élevée s'appliquer pour l'obtention d'une autorisation judiciaire, notamment des motifs raisonnables de soupçonner, comme dans le cas de l'obtention d'un mandat de localisation[468] ou d'un enregistreur de numéro[469]. Par contre, à ce jour, aucune disposition législative spécifique n'est prévue pour l'obtention des en-têtes de courriel avec une norme réduite, la norme générale des motifs raisonnables de croire devra donc au minimum être respectée dans la mesure, bien entendu, où l'on utilise l'autorisation judiciaire appropriée. La décision dans Weir suggère également une certaine minimisation des atteintes, compte tenu des vulnérabilités inhérentes de la technologie[470].

---

[465] La nétiquette est un ensemble de règles implicites, adoptées par la majorité des utilisateurs d'Internet. Ces règles ont notamment pour but de faciliter la communication et de diminuer le trafic inutile sur le réseau. Elles n'ont aucune force contraignante. Elles sont basées sur la bonne volonté des utilisateurs. *Le guide de l'internaute 2000*, *Ibid*. aux pp. 86-87, *Droit du Cyberespace*, *supra* note 8 aux pp. 3-62 à 3-64 ; *Internet*, *supra* note 214 aux pp. 67, 121 et *RFC* 1855, en ligne : <http://www.faqs.org/rfcs/rfc1855.html> (date d'accès : 5 avril 2002).

[466] *Weir*, *supra* note 136 au para. 75-76. Cette distinction est à notre avis académique, puisqu'en pratique il sera impossible de décrypter un tel message. L'obtention d'une autorisation judiciaire dans ce contexte est donc illusoire, puisqu'on ne pourra prendre connaissance du contenu du message. La similarité du niveau d'expectative raisonnable de vie privée d'un courriel et du courrier de première classe a par ailleurs été implicitement confirmée dans *Maxwell 2*, *supra* note 316, ce qui n'est pas le cas dans *Weir* où il est affirmé aux para.71-77, que le courriel bénéficierait d'une expectative raisonnable de vie privée moindre que le courrier de première classe, compte tenu de la manière dont la technologie est gérée et de la manière dont les réparations et l'entretien sont effectués.

[467] *Weir*, *Ibid*. aux paras. 72-74.

[468] Article 492.1 du *Code criminel.*

[469] Article 492.2 du *Code criminel*.

[470] *Weir*, *supra* note 136 au para. 77.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

Dans ce sens, nous soumettons que les messages électroniques envoyés par courriel ressemblent en fait plus aux cartes postales qu'aux lettres cachetées, ce qui est contraire à l'affirmation de principe de la Cour suprême américaine dans *Reno c. ACLU*[471]. En effet, les courriels sont acheminés en clair[472] par le protocole *SMTP* (*Simple Mail Transfer Protocol*). Leur transport ne se fait pas directement de l'ordinateur de l'expéditeur à l'ordinateur du destinataire. De nombreux ordinateurs du réseau font office de passerelles où il est aisé de les obtenir. Lorsque le message parvient à l'ordinateur cible, il y reste encore souvent un moment avant d'être lu. Là encore, des intrus dotés des droits d'accès nécessaires peuvent intervenir à loisir. Pour envoyer des données réellement confidentielles, il est préférable de les chiffrer.[473] C'est d'ailleurs la conclusion à laquelle arrive la Cour de District de Pennsylvanie, en comparant le courriel à une carte postale, plutôt qu'à une lettre cachetée[474].

La nature même de la technologie fait donc en sorte que l'on peut difficilement s'attendre à ce que le contenu de notre message ne puisse être obtenu par un tiers, du moins dans le contexte de l'entretien du service effectué par le fsI.[475]

Même si le courriel est considéré comme une ressource essentiellement textuelle, on peut quand même envoyer des fichiers joints contenant des sons[476], des images[477] et même des logiciels entiers[478]. Et même si la technologie fait en sorte que le fichier est considéré comme une pièce jointe au message principal, il est en fait incorporé au corps même du message. Donc, lors de l'obtention d'un courriel par un organisme d'application de la loi, il sera possible de récupérer beaucoup plus que du texte[479] ! De plus, les informations autres que celles relatives au contenu, pourront révéler en soi des informations fort utiles.

De toutes les informations contenues dans les diverses en-têtes, un utilisateur raisonnable pourra facilement connaître l'adresse IP de l'ordinateur d'un expéditeur ou de son serveur SMTP. Celle-ci se trouve généralement dans des champs nommés « *received* ». On pourra même y voir l'adresse IP d'un expéditeur, même si celui-ci envoie son courriel à partir d'un serveur Web, généralement reconnu comme plus « anonyme » qu'un serveur de courrier se trouvant chez un fsI[480]. Les champs « *received* » apparaissent généralement à l'écran même lors de la réception d'un courriel. Il faut parfois activer certains paramètres du logiciel de courriel utilisé pour les faire apparaître[481]. Des utilisateurs plus sophistiqués pourront même, à

---

471 *Supra* note 1 à la p. 851.

472 Par opposition à encryptés ou chiffrés. Nous traiterons de la cryptographie plus loin.

473 *Sécurité et protection*, *supra* note 210 aux pp. 244-45, 297. Voir aussi *Protégez-vous sur Internet, supra* note 207 à la p. 107, qui arrive à la même conclusion. Voir finalement *Weir*, *supra* note 136 au para. 59, où il a été établi par expert qu'il n'était pas recommandé de transmettre des messages de nature hautement confidentielle par courriel, notamment à cause de la nature même de la technologie qui rend les messages vulnérables lors de l'entretien du service effectué par les fsI.

474 *ACLU c. Reno, supra* note 196 à la p. 834. Voir aussi *Protégez-vous sur Internet, supra* note 207 à la p. 107, qui arrive à la même conclusion.

475 *Weir*, *supra* note 136 au para. 60.

476 Comme par exemple des fichiers de type « .wav », « .midi », etc.

477 Comme par exemple des fichiers de type « .gif », « .jpeg », etc.

478 *Internet le guide 2000, supra* note 255 à la p. 66.

479 Comme par exemple des fichiers de type « .xls », « .html », « .doc », etc. qui pourront notamment contenir de la comptabilité et correspondances personnelles.

480 *L'Internet sécurisé*, *supra* note 379 aux pp. 28-34 ; *Le guide de l'internaute 2000, supra* note 136 aux pp. 94-95.

481 *L'Internet sécurisé*, *Ibid*. à la p. 28.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

l'aide de programmes faciles à utiliser, analyser les en-têtes de messages, leur permettant ainsi d'en savoir encore plus sur les différents intervenants du processus d'envoi d'un courriel, tels les serveurs et les utilisateurs[482].

Le *Webmail* sera intéressant pour une personne ne possédant pas d'ordinateur, mais accédant au réseau à partir d'un poste public. Un voyageur peut ainsi accéder à son courriel à partir de n'importe quel ordinateur dans le monde branché à Internet. Dans ce contexte, l'expectative raisonnable de vie privée sera tributaire du lieu où se trouve l'ordinateur servant à l'établissement de la communication ou au branchement au réseau. La confidentialité inhérente des messages envoyés par le biais d'un tel service serait moindre que celle d'un logiciel de courriel traditionnel, car le contenu d'une page Web n'est généralement pas chiffré. Ce service offrirait par contre une confidentialité relative par rapport à l'identité de l'utilisateur comme traité précédemment dans le constat relatif aux en-têtes de messages[483].

En résumé, l'expectative raisonnable de vie privée sera en principe augmentée à l'égard d'un courriel :

- Plus le réseau utilisé pour le transmettre est petit;
- Plus le nombre d'intervenants dans la transmission est petit;
- Plus la relation contractuelle entre le fsI et la cible est empreinte de protection relative à la préservation du caractère privé du contenu des messages;
- Plus on utilise une méthode de protection pour préserver le caractère privé du contenu du message et même des en-têtes, telle la cryptographie;
- Plus on se rapproche du contenu du corps du message.

L'expectative raisonnable de vie privée sera en principe diminuée à l'égard d'un courriel :

- Plus le réseau utilisé pour la transmission est grand, tel Internet;
- Plus il y a de destinataires pour le message;
- Plus le message a fait l'objet d'une redistribution;
- Plus on s'éloigne du destinataire initial;
- Plus on se rapproche du contenu des en-têtes.

Quant à la liste de distribution automatisée, elle sera plus ou moins privée ou publique selon le type d'accès accordé, et le nombre de personnes y participant, etc. C'est le choix du type de liste et de ses caractéristiques qui annoncera l'expectative raisonnable de vie privée subjective de son créateur. Quant au participant, ce sera la décision d'y adhérer ou non. Bien entendu, l'ensemble des circonstances de la création et de l'utilisation de la liste seront également évaluées objectivement par la Cour. L'existence ou non de fonctions de recherche et d'archivage sera également un facteur important dans cette détermination. Finalement, un courriel envoyé ou redistribué à un agent d'infiltration ne bénéficie pas, du moins en droit américain, d'une expectative raisonnable de vie privée[484].

Section III - Le transfert de fichiers FTP

---

[482] *Protégez-vous sur Internet, supra* note 207 à la p. 141.
[483] *Le guide de l'internaute 2000, supra* note 136 aux pp. 94-95, 98.
[484] *Charbonneau, supra* note 461 à la p. 1185.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

Nous commencerons cette section par la description générale de la technologie. Nous traiterons ensuite de la session FTP et du transfert de fichiers FTP par le Web. Nous conclurons par les constats des limites à l'expectative raisonnable de vie privée lors de l'utilisation de la ressource FTP.

Description générale de la technologie

FTP est le sigle de *File Transfer Protocol*. Il s'agit d'un protocole utilisé lors de transferts de fichiers entre deux ordinateurs dans les réseaux TCP/IP tels Internet. On peut bien entendu transférer des fichiers par le biais d'une page Web ou par le courriel. Il sera par contre beaucoup plus pratique et efficace de procéder par le biais d'un transfert de fichier en protocole FTP[485]. Il s'agit d'une ressource qualifiée de moyen de communication permettant « l'obtention d'information à distance »[486].

Pour effectuer un transfert de fichier, l'utilisateur doit posséder un logiciel client FTP. Ce client interagit avec le serveur pour s'assurer que les données soient bien échangées.[487] Il s'agit d'un utilitaire conçu pour le transfert de fichiers de type FTP qui agit comme un simple gestionnaire de fichiers permettant d'échanger des fichiers avec un serveur étranger, comme s'il s'agissait d'un autre disque dur dans notre ordinateur. On sélectionne le fichier dans un répertoire d'un serveur étranger et il est rapidement transféré. Il s'agit de l'utilité fondamentale de FTP[488].

Le choix des transferts de fichiers est laissé à l'entière discrétion de l'utilisateur, dans la mesure où il possède les droits d'accès requis[489]. Les restrictions d'accès seront déterminées par le gestionnaire du serveur FTP[490].

La session FTP

FTP fonctionne pratiquement de la même façon qu'une session de communication en mode *Telnet*[491], dont nous traiterons plus loin, notamment par son approche client-serveur. Préalablement, on doit avoir en main l'adresse Internet du serveur avec lequel on veut transiger, ce qui implique que le serveur pourra être identifié par son adresse IP. Au moment de la liaison, un compte utilisateur et un mot de passe sont demandés pour valider l'identité de la personne qui veut établir un lien[492]. Le serveur déterminera les droits de l'utilisateur (client)

---

485 *Le guide de l'internaute 2000, supra* note 136 aux pp. 293-294.
486 *ACLU c. Reno, supra* note 196 aux pp. 834-835.
487 *Le guide de l'internaute 2000, supra* note 136 à la p. 554.
488 *Ibid*. à la p. 294. Voir aussi *Cyber Law*, *supra* note 200 à la p. 25.
489 *Le guide de l'internaute 2000, supra* note 136 à la p. 295.
490 *Cyber Law*, *supra* note 200 aux pp. 25-26. Pour un exemple de logiciel *FTP* voir *Ws_FTP*, en ligne : <http://www.ipswitch.com/Products/WS_*FTP*> (date d'accès : 24 avril 1999).
491 Il est encore possible d'échanger des fichiers par *FTP* en mode terminal ou Telnet, mais cette façon de procéder devient de plus en plus marginale. Voir *Le guide de l'internaute 2000, supra* note 136 aux pp. 297 et 302-303. Nous ne nous y attarderons donc pas dans la présente étude. De toute façon la compréhension des transferts de type *FTP* et du fonctionnement d'une session en mode terminal, est suffisante pour comprendre les limites à l'expectative raisonnable de vie privée lors d'une session *FTP* en mode terminal. Nous traiterons plus loin du mode terminal ou Telnet.
492 *Ibid*. à la p. 295. Il existe également le FTP anonyme. On dit anonyme, parce qu'un tel site FTP ne requiert pas de mot de passe pour y accéder. On pourra conséquemment y accéder en employant un nom d'utilisateur générique, généralement le nom « anonymous ». Il faudra alors donner notre adresse de courriel en guise de mot de passe, ce qui permet notamment à l'administrateur du site FTP d'établir des statistiques sur les

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

et les fichiers qui lui sont accessibles. Le service écoute normalement le port IP 21[493]. Une fenêtre apparaît ensuite, affichant généralement à gauche le contenu du disque rigide de l'utilisateur client, et à droite, les répertoires et le contenu du disque rigide du serveur distant[494].

La partie serveur du service est un logiciel qui peut résider sur un ordinateur de n'importe quel type[495]. Il peut notamment s'agir d'un ordinateur personnel compatible IBM ou d'un Macintosh. Il ne faut donc pas nécessairement être une institution ou une compagnie spécialisée possédant un puissant ordinateur central pour offrir un tel service : un ordinateur personnel situé dans un sous-sol, appartenant à un individu, peut très bien faire office de serveur FTP.

Plusieurs fonctions sont possibles lors de l'utilisation de FTP. Il est notamment possible de changer et de créer de nouveaux répertoires, dans la mesure où nos droits d'accès le permettent, d'accéder aux fichiers ou répertoires en cliquant dessus, de transférer des fichiers, d'afficher leur contenu, d'exécuter des programmes, de modifier ou supprimer le nom d'un fichier et, bien entendu, de terminer la session[496]. Il est également possible, grâce à d'autres programmes fonctionnant de concert avec FTP, de compresser les données transférées[497] ou de les regrouper[498]. Il sera alors possible de les transférer plus rapidement et d'économiser de l'espace disque sur les ordinateurs en « réduisant » la taille des fichiers[499].

Dans le cas des serveurs FTP anonymes, il est recommandé, pour plus d'efficacité quant à la rapidité des transferts, de se brancher à un serveur qui sera géographiquement plus près de l'utilisateur. Idéalement, il faudra trouver un site dans notre province ou pays[500].

Le transfert de fichiers FTP par le Web

Bien qu'il ne s'agit pas de son utilisation première, un navigateur Web peut également servir pour le transfert de fichiers FTP. Tous les navigateurs Web peuvent négocier ce type de transfert. Il est cependant recommandé d'utiliser un logiciel FTP spécialisé pour éviter la

---

personnes accédant à son service et de contrôler l'identité de personnes susceptibles de commettre des actions malveillantes, comme l'infiltration de virus ou le méfait de données. L'administrateur d'un site FTP peut aussi souhaiter joindre les utilisateurs en utilisant les adresses de courriel qu'ils ont données comme mot de passe, notamment dans les cas où un fichier rapatrié contient un virus. Il ne s'agit donc pas d'une session *FTP* où l'utilisateur est anonyme proprement dit. Bien au contraire, il pourrait théoriquement être identifié par son adresse de courriel ou son adresse IP. Voir *Le guide de l'internaute 2000, supra* note 136 aux pp. 303-304 ; *Internet*, *supra* note 214 à la p. 60.

493 *Le guide de l'internaute 2000, supra* note 136 aux pp. 65, 295.

494 *Ibid*. à la p. 299.

495 *Ibid*. à la p. 295.

496 *Ibid*. aux pp. 299-01.

497 Notamment par l'utilisation du logiciel *Winzip*, en ligne : <http://www.winzip.com> (date d'accès :20 juin 2001).

498 *Le guide de l'internaute 2000, supra* note 136 à la p. 312.

499 *Ibid*. aux pp. 310-312. Voir aussi *Internet*, *supra* note 214 aux pp. 61-63.

500 *Le guide de l'internaute 2000, supra* note 136 à la p. 307. Pour le Québec, voir notamment Cogiciel, en ligne : <http://www.cogiciel.com> (date d'accès : 20 juin 2001) et Mégagiciel, en ligne : <http://www.megagiciel.com> (date d'accès : 20 juin 2001). Pour les États-Unis, voir notamment *Tile.net*, en ligne : <http://tile.net/*FTP*> (date d'accès : 20 juin 2001) et *Shareware.com*, en ligne : <http://shareware.com> (date d'accès : 20 juin 2001).

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

lenteur des navigateurs Web et les problèmes de sécurité entourant l'identification de l'utilisateur, notamment quant à la transmission du mot de passe et du nom de l'usager[501].

Il s'agit simplement d'inscrire l'adresse du serveur FTP désiré à l'endroit où on inscrit les adresses de navigation; il faudra tout simplement ajouter le préfixe « FTP:// » au début de l'adresse du serveur désiré. La façon d'inscrire l'adresse variera selon qu'on accède à un serveur FTP anonyme ou non. La différence dans l'adressage réside dans l'inscription du nom d'utilisateur et d'un mot de passe dans le cas d'un serveur FTP qui n'est pas anonyme.

Constats des limites à l'expectative raisonnable de vie privée lors du transfert de fichiers FTP

De façon générale, le niveau d'expectative raisonnable de vie privée lors de l'utilisation de cette ressource sera tributaire du niveau de sécurité du protocole TCP/IP. Il faudra donc que certaines techniques, visant à protéger l'anonymat, ou que certaines mesures soient prises dans ce sens, pour limiter les chances de voir sa communication en protocole TCP/IP compromise.

Quant au FTP anonyme, toutes les opérations qui y sont effectuées par les utilisateurs sont enregistrées dans des fichiers de trace (« log files ») qui servent à établir des statistiques d'utilisation des serveurs[502]. Il n'est pas évident qu'un utilisateur ordinaire soit au courant que toutes ses opérations sont enregistrées de cette façon. Le tout pourrait dépendre de la politique de l'administrateur du site FTP visité, mais encore faut-il connaître cette politique ! Il faudra alors vérifier si celle-ci énonce clairement aux utilisateurs que leurs opérations sont susceptibles d'être enregistrées.

Un site FTP anonyme est considéré comme un service public et comme un disque rigide pour toute la planète[503]. Dans la mesure où il s'agit d'une ressource publique, il pourrait être difficile pour la personne qui l'a mis en place de prétendre à une quelconque expectative raisonnable de vie privée lors de son utilisation. Par contre, dans d'autres contextes, notamment dans le cas où l'accès est limité, il pourrait être plus probable que la personne qui a mis le service en place puisse bénéficier d'une quelconque expectative raisonnable de vie privée. Quant à l'expectative raisonnable des utilisateurs, elle sera tributaire de tous les autres facteurs techniques inhérents à l'utilisation d'Internet.

Section IV - Les groupes de discussions ou nouvelles *Usenet*

Nous commencerons cette section en faisant une description générale de la technologie. Nous traiterons ensuite de la session *Usenet*, de la structure d'un article ou message *Usenet* et de la culture rattachée à l'utilisation d'*Usenet*. Nous conclurons par le constat des limites à l'expectative raisonnable de vie privée lors de l'utilisation des groupes de nouvelles *Usenet*.

Description générale de la technologie

Usenet est un ensemble de serveurs regroupant plus de 40 000 groupes de discussion. Tous les utilisateurs d'Internet ont le droit d'envoyer des articles. Un utilisateur doit posséder un

[501] *Le guide de l'internaute 2000, supra* note 136 aux pp. 294, 310.
[502] *Internet*, *supra* note 214 à la p. 60.
[503] *Le guide de l'internaute 2000, supra* note 136 aux pp. 303, 305.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

logiciel appelé «lecteur de nouvelles pour *Usenet*» pour être en mesure de consulter ces nouvelles[504]. La plupart des navigateurs Web comportent de telles fonctions[505]. Le protocole d'échange officiel entre les serveurs *Usenet* se nomme NNTP («*Network News Transfer Protocol*») [506]. Il s'agit d'une ressource qui utilise Internet pour fonctionner.

La Cour suprême américaine traite également de cette ressource utilisée dans Internet :

> « *Newsgroups also serve groups of regular participants, but these postings may be read by others as well. There are thousands of such groups, each serving to foster an exchange of information or opinion on a particular topic running the gamut from, say, the music of Wagner to Balkan politics to AIDS prevention to the Chicago Bulls. About 100,000 new messages are posted every day.*
>
> *In most newsgroups, postings are automatically purged at regular intervals. In addition to posting a message that can be read later, two or more individuals wishing to communicate more immediately can enter a chat room to engage in real-time dialogue—in other words, by typing messages to one another that appear almost immediately on the others' computer screens. The District Court found that at any given time "tens of thousands of users are engaging in conversations on a huge range of subjects." It is "no exaggeration to conclude that the content on the Internet is as diverse as human thought. »* [notes omises].[507]

Une description plus complète de la ressource est faite en première instance. On qualifie cette ressource comme étant une « base de données de messages distribués » :

> « *Distributed message databases. Similar in function to listservs -- but quite different in how communications are transmitted -- are distributed message databases such as "USENET newsgroups." User-sponsored newsgroups are among the most popular and widespread applications of Internet services, and cover all imaginable topics of interest to users. Like listservs, newsgroups are open discussions and exchanges on particular topics. Users, however, need not subscribe to the discussion mailing list in advance, but can instead access the database at any time. Some USENET newsgroups are "moderated" but most are open access. For the moderated newsgroups, all messages to the newsgroup are forwarded to one person who can screen them for relevance to the topics under discussion. USENET newsgroups are disseminated using ad hoc, peer to peer connections between approximately 200,000 computers (called USENET "servers") around the world. For unmoderated newsgroups,*

---

504 *Ibid*. aux pp. 315, 561.

505 Pour le Navigator de Netscape, version 2 et plus et pour l'Internet Explorer de Microsoft, version 3 et plus.

506 *Le guide de l'internaute 2000, supra* note 136 à la p. 323. Les renseignements techniques sur le fonctionnement du protocole *NNTP* se trouvent à la *RFC-997*, en ligne : <http://www.normos.org/ietf/*RFC*/*RFC*977.txt> (date d'accès : 15 août 2001). Voir aussi *Internet*, *supra* note 214 à la p. 66.

507 *Reno c. ACLU, supra* note 1 aux pp. 851-852. Le nombre avancé par la Cour suprême américaine serait passé de 150 000 à 400 000 messages par jour. Voir *Le guide de l'internaute 2000, supra* note 136 à la p. 318. Pour un exemple de statistiques quotidiennes d'utilisation d'un fournisseur de service offrant les services d'un serveur *Usenet*, voir *ASA Networks*, en ligne : <http://www.asacomp.com> (date d'accès : 15 août 2001).

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

> *when an individual user with access to a USENET server posts a message to a newsgroup, the message is automatically forwarded to all adjacent USENET servers that furnish access to the newsgroup, and it is then propagated to the servers adjacent to those servers, etc. The messages are temporarily stored on each receiving server, where they are available for review and response by individual users. The messages are automatically and periodically purged from each system after a time to make room for new messages. Responses to messages, like the original messages, are automatically distributed to all other computers receiving the newsgroup or forwarded to a moderator in the case of a moderated newsgroup. The dissemination of messages to USENET servers around the world is an automated process that does not require direct human intervention or review* » [notes omises][508].

Les participants à ces groupes vont donc émettre des questions, des réponses, des opinions, des annonces, des statistiques, et même afficher des images, des sons et des fichiers multimédias. Il n'y a aucune autorité centrale qui gère *Usenet*. Les messages sont acheminés d'un serveur à l'autre[509]. Il s'agit d'un effort coopératif distribué[510].

La session *Usenet*

Usenet est un regroupement de serveurs Internet échangeant des messages. Ces ordinateurs sont appelés serveurs de nouvelles[511]. Les utilisateurs doivent se servir d'un logiciel client, le plus souvent à partir de leur navigateur Web. *Usenet* est donc basé sur une architecture client-serveur[512]. Le logiciel client s'appelle « lecteur de nouvelles ». Sohier décrit le fonctionnement d'une session *Usenet* :

> « *Les messages sont composés par les internautes et traitent d'une immense variété de sujets. Les messages traitant d'un même sujet sont classés par groupes de nouvelles. L'expéditeur doit indiquer à quel(s) groupe(s) de nouvelles son message est destiné. Sur réception, le serveur de nouvelles fera parvenir celui-ci aux autres serveurs à travers la planète pour publication. C'est de cette façon qu'un utilisateur situé à l'autre bout de la planète pourra consulter un de vos messages sur son propre serveur de nouvelles* »[513].

Il s'agit en quelque sorte d'un outil de diffusion qui vise l'échange d'information. Le premier service *Usenet* est entré en fonction en 1979 aux États-Unis où il reliait deux universités. Il a été relié à Internet, tel qu'il était à l'époque, au milieu des années 80[514]. Comme le courriel, il s'agit d'un mode de communication asynchrone[515]. On le compare à un service qui établit des

---

[508] *ACLU c. Reno, supra* note 196 aux pp. 834-35.
[509] Contrairement au courriel, qui est transféré immédiatement lors de sa réception par un agent de transfert de message, *Usenet* peut mettre plusieurs heures pour distribuer un message à tous les autres serveurs *Usenet* de la planète. Il existerait donc un certain délai de transmission des messages inhérents à *Usenet*. *Digital Evidence supra* note 252 à la p. 109.
[510] *Le guide de l'internaute 2000, supra* note 136 à la p. 319. Voir aussi *Cyber Law*, *supra* note 200 à la p. 24.
[511] *Le guide de l'internaute 2000, Ibid*. à la p. 316.
[512] *Internet*, *supra* note 214 à la p. 66.
[513] *Le guide de l'internaute 2000, Ibid*. à la p. 316.
[514] *Protégez-vous sur Internet, supra* note 207 à la p. 165.
[515] *Digital Evidence*, *supra* note 252 à la p.90.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

communications de « beaucoup-à-beaucoup », comparativement au courriel qui favorise une communication de « un-à-un »[516]. Il ne s'exerce aucun contrôle véritable sur les sujets discutés. Seul l'administrateur du serveur de nouvelles décide de l'accessibilité des groupes de nouvelles par les utilisateurs de son site[517].

Chaque utilisateur décide de sa participation. Il peut notamment décider de publier des âneries de toutes sortes, sans que personne ne puisse l'en empêcher[518].

Structure d'un article ou message *Usenet*

La *RFC* 850 définit la structure des messages ou articles *Usenet* et la RFC 977 décrit le protocole NNTP (*Network News Transfer Protocol*)[519]. Le protocole NNTP sert au transport des messages ainsi qu'à leur récupération pour consultation[520].

Tout article a une structure comportant un en-tête et un corps. L'en-tête contient un certain nombre de champs comme par exemple les champs « *date* » indiquant la date d'envoi du message, « *from*» indiquant la provenance du message[521], « *subject* » indiquant le sujet du message et « *newsgroups* » indiquant le nom du groupe de discussion auquel est envoyé le message[522].

Après l'envoi du message, les champs « *message-id* » et « *path* » y sont rajoutés. Le champ « *message-id* » permet d'identifier de façon unique chaque article ou message envoyé dans *Usenet* et Internet. Le champ « *path* » permet de tracer le chemin emprunté par un article ou message dans le réseau. On connaîtra le chemin parcouru en lisant la ligne du champ « *path* » de droite à gauche, la dernière information à gauche constituant la destination finale, et la première à droite[523]. On y trouvera l'identité du serveur d'origine, de l'ordinateur de l'émetteur du message et du serveur de réception[524].

---

[516] *Protégez-vous sur Internet, supra* note 207 à la p. 163.

[517] *Le guide de l'internaute 2000, supra* note 136 à la p. 318. Cette situation pourrait changer sous peu. En effet, par l'arrivée du système *Usenet* II, un administrateur de serveur de nouvelles pourra plus facilement éliminer un message du système si la nature de celui-ci ne cadre pas avec les règles d'utilisation du serveur. *Ibid*. à la p. 323. Voir par contre, *Internet*, *supra* note 214 à la p. 69. Il est par ailleurs présentement possible par le biais des articles ou messages de contrôle, de détruire n'importe quel article envoyé sur le réseau et même des groupes *Usenet* entiers. L'efficacité de cette fonction pour les utilisateurs dépend en pratique de chaque administrateur qui décidera dans quelle mesure ces messages de destruction seront acceptés sur son serveur *Usenet*. Il est donc théoriquement possible qu'un auteur puisse être en mesure de détruire un message qu'il a envoyé. Il faudra pour ce faire indiquer la commande appropriée dans l'en-tête, au champ « control ». *L'Internet sécurisé*, *supra* note 379 aux pp. 24-25.

[518] *Le guide de l'internaute 2000, supra* note 136 à la p. 320.

[519] Voir les *RFC* 850 et 977, en ligne :<http://www.*RFC*-editor.org> (date d'accès : 14 août 2001).

[520] *L'Internet sécurisé*, *supra* note 379 aux pp. 18-19.

[521] C'est à cet endroit qu'on trouvera l'adresse de courriel de l'expéditeur du message.

[522] *L'Internet sécurisé*, *Ibid*. aux pp. 19-20.

[523] Il est recommandé d'utiliser les informations contenues dans le champ « *path* » pour tenter d'identifier l'auteur d'un message. On pourra notamment procéder à une requête en mode Telnet, en utilisant le port de communication 119, afin de pouvoir accéder aux différents serveurs empruntés. Le but visé par cette méthode est d'utiliser le nom de l'ordinateur comme indice pour retracer plus facilement l'identité de l'auteur du message. *Digital Evidence, supra* note 252 aux pp. 107-11.

[524] *L'Internet sécurisé*, *supra* note 379 aux pp. 20-24.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

Quant au corps du message, on y trouvera évidemment le contenu et la signature de l'auteur qui pourra être stylisée. C'est dans cette partie que l'auteur laissera libre cours à son inspiration!

Culture rattachée à l'utilisation de *Usenet*

Les sujets des groupes de discussion sont variés et organisés hiérarchiquement par catégorie[525]. Les articles affichés dans ces différents groupes de discussion sont affichés quelques temps, soit pour une période déterminée par l'administrateur du serveur de chaque site. On les efface du système après un certain temps, compte tenu notamment du très grand nombre de messages qui circulent[526].

Il est conseillé de toujours consulter le document FAQ (*Frequently Asked Questions* ou foire aux questions) d'un groupe *Usenet* avant de s'y aventurer. Ce document regroupe notamment les réponses aux questions posées fréquemment; le nom de la personne responsable du groupe indique également si son contenu est archivé. Il est préférable de procéder de cette manière afin de respecter la raison d'être du groupe et d'éviter de recevoir des flammes (*flames*) qui sont des réponses furieuses et agressives[527].

On peut créer un groupe *Usenet* de deux façons, soit en le rendant accessible dans tout le réseau[528], soit en le limitant à un site local[529]. Dans les deux cas, il est préférable d'indiquer la raison d'être ou la raison sociale de ces groupes afin d'indiquer le sujet de la discussion.

Même s'il n'est pas nécessaire d'ajouter une signature électronique[530] au contenu du message, il est recommandé de le faire car elle sert à donner une meilleure information sur la personne qui publie son message. Cette signature peut prendre diverses formes et fait partie de la « culture » des groupes *Usenet*[531]. Une autre caractéristique de l'utilisation de *Usenet* est la

---

[525] On retrouvera notamment les catégories ou souches suivantes : « *comp*. » portant sur les ordinateurs, les systèmes d'information, les logiciels et le matériel informatique; « *misc*. » et « *alt*. » portant sur tout ce qui ne peut être catégorisé; « *sci*. » portant sur les sujets relevant du domaine scientifique; « *talk*. » portant sur les débats où les opinions sur tous les sujets y sont traitées. Il s'agit en quelque sorte d'une tribune téléphonique à la radio ou à la télé. Voir *Le guide de l'internaute 2000, supra* note 136 aux pp. 324-27.

[526] *Ibid*. à la p. 327.

[527] *Ibid*. aux pp. 328, 335-36 ; *Internet*, *supra* note 214 à la p. 67.

[528] Le groupe distribué dans tout Internet sera le plus souvent établi par un vote des utilisateurs. Ce vote sera organisé par l'administrateur du groupe *news.announce.newsgroup* qui en publiera les résultats. Dans le cas des catégories « alt. » et « mist. », aucun vote n'est requis et un groupe peut être créé sans aucune permission ou vote. Un groupe n'ayant pas fait l'objet d'un vote démocratique aura par contre de bonnes chances de n'être pas accessible sur tous les serveurs *Usenet*, car ce sont les administrateurs qui décident des groupes offerts sur leur site. Voir *Le guide de l'internaute 2000, supra* note 136 aux pp. 329-30 ; *Internet*, *supra* note 214 aux pp. 66-67.

[529] Le groupe distribué localement sera créé par l'administrateur de site local et ne sera accessible qu'aux utilisateurs de ce site. On annoncera quand même la raison sociale du groupe qui indique en quelque sorte le sujet des discussions qui s'y tiendront. *Le guide de l'internaute 2000, supra* note 136 à la p. 330. Certains groupes sont également modérés en ce sens qu'un « modérateur » voit au bon ordre relativement au contenu des messages, notamment quant au respect du thème du groupe et aux écarts de langage. *Internet le guide 2000, supra* note 255 à la p. 74.

[530] Encore une fois ici il s'agit d'une représentation graphique en format électronique de la signature et non l'utilisation d'une technique cryptographique pour assurer l'intégrité et la sécurité du message. *L'identification et la certification supra* note 466 aux pp. 93-116 ; *Droit du Cyberespace*, *supra* note 8 aux pp. 19-23 à 19-32.

[531] *Le guide de l'internaute 2000, supra* note 136 aux pp. 331-332. Voir également le site de *Coolsig*, en ligne :

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

possibilité de faire un suivi d'article, soit de répondre à des messages écrits par d'autres utilisateurs[532].

Compte tenu que l'on « publie » dans *Usenet*, il est recommandé d'utiliser des titres de messages précis qui en décrivent bien le contenu[533]. Il faut en effet capter l'attention des usagers, sinon le message tombe dans l'oubli[534].

Afin d'accéder à un serveur de nouvelles *Usenet*, on doit utiliser un logiciel client. Ce logiciel client sera le plus souvent inclus dans un navigateur Web[535]. Une multitude d'options et de fonctions sont disponibles dans chaque logiciel. Toutes ces options ou fonctions sont semblables. Seule la présentation graphique pour y accéder ou les utiliser varie. Il y a également une multitude de réglages à effectuer. Il s'agit de la configuration des paramètres d'utilisation des logiciels clients. Ces fonctions, options et paramètres auront des impacts sur la façon de naviguer et d'utiliser *Usenet*. Cela influencera, dans certains cas, le niveau d'expectative raisonnable de vie privée auquel on peut s'attendre dans un tel environnement. Ce qui nous amène à traiter des diverses fonctions, options ou paramètres.

Il y a d'abord les paramètres relatifs à l'identité. Ces paramètres servent à nous identifier. On suggère d'y inscrire notre nom usuel, notre adresse de courriel, une adresse de courriel de retour si celle-ci diffère de l'adresse de courriel précédente, le nom de notre organisation, et d'y indiquer le chemin d'accès pour identifier le fichier contenant notre signature électronique[536].

Il faut également désigner le forum de discussion choisi[537] et spécifier le port de communication qui est utilisé. Le plus souvent ce sera le port IP numéro 119. Ce paramètre sera donc rarement changé par l'usager lors de la configuration[538].

Il faut sélectionner le ou les groupes de nouvelles auxquels on désirera participer. Il suffit de le choisir à partir d'une liste de groupes de discussion suggérée par notre serveur de groupe *Usenet*. Le choix s'opérera à partir des sujets que suggèrent les titres, par exemple, « *alt.music.prince* » sera un groupe de discussion *Usenet* classé dans la catégorie inclassable

---

<http://www.coolsig.com> (date d'accès :13 août 2001), qui se spécialise dans les signatures électroniques.

532 *Le guide de l'internaute 2000, supra* note 136 à la p. 333.

533 *Ibid*. à la p. 337.

534 C'est d'ailleurs l'essence même de *Usenet*. Il faut que notre message soit lu, que notre opinion soit entendue et que notre nom y soit rattaché. Il s'agit en quelque sorte d'une impulsion, un désir de se faire entendre. De toute façon, un message non identifié perd en quelque sorte de son sérieux, car le contenu n'est rattaché à personne. Les personnes qui cherchent à se faire une place dans Internet commencent souvent par l'envoi de messages sur des ressources ou services s'apparentant à *Usenet*. À ce sujet, voir M Godwin, *Cyber Rights*, New-York, Times Books, 1998, aux pp. 133-135 et S. Garfinkel, *Database Nation. The Death of Privacy in The 21st Century*, Sebastopol (CA), O'Reilly & Associates, 2000, à la p. 87 [ci après *Database Nation*].

535 Voir notamment le *Netscape Navigator* version 4.7, en ligne : <http://www.netscape.com/fr>(date d'accès : 11 juin 2001) et l'*Internet Explorer* de *Microsoft* version 5, en ligne : <http://www.microsoft.com/france/internet/produits/ie/ie5> (date d'accès : 11 juin 2001). Pour la navigation dans les groupes de nouvelles *Usenet* avec Internet Explorer, on doit utiliser un logiciel qui vient avec celui-ci. Il s'agit du logiciel *Outlook Express*, en ligne : <http://www.microsoft.com/France/internet/produits/oe> (date d'accès : 11 juin 2001). *Outlook Express* vient également avec *Windows* 98 de *Microsoft*, en ligne : <http://www.microsoft.com/France/windows> (date d'accès : 11 juin 2001).

536 *Le guide de l'internaute 2000, supra* note 136 aux pp. 339 et 355.

537 *Ibid*. aux pp. 340-341 et 355-356. Il est à noter qu'il est suggéré d'utiliser un serveur géographiquement près de chez nous pour de meilleures performances.

538 *Ibid*. aux pp. 341-341.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

« *alt*. », traitant de musique « *music*. » et de l'artiste nommé Prince « *prince* ». Un utilisateur sait donc dans quel groupe ou de quel sujet il sera question lorsqu'il décide de s'abonner.

Il est également possible de rechercher par mot-clé le sujet des groupes de discussion[539]. Un utilisateur raisonnable devrait donc savoir qu'il est possible d'effectuer des recherches dans les groupes de discussions *Usenet*. D'ailleurs, lorsque qu'on ne fait que consulter les groupes de discussions *Usenet* sans y participer, on reste dans l'anonymat[540]. La situation d'une personne qui consulte les groupes de discussion *Usenet* est donc différente de celle qui y publie un message[541].

Un message *Usenet* est séparé en deux parties. Il y a l'en-tête qui révèle le titre, l'auteur, l'organisation ainsi que le ou les groupes de nouvelles dans lequel ou lesquels le message a été publié. Il y a également le corps du texte qui comprend le contenu du message, généralement du texte. Il peut également s'agir d'images ou de fichiers de type HTML[542].

Les logiciels clients mentionnés plus haut contiennent également des fonctionnalités du courriel[543]. On peut donc répondre directement au groupe suite à un message publié dans *Usenet*, répondre personnellement à l'expéditeur du message par l'entremise d'un courriel ou faire suivre le message à une autre personne par le biais du courrier électronique[544]. C'est donc à l'utilisateur de déterminer la façon appropriée de répondre à un message : en particulier, en public ou une combinaison des deux.

La nature de *Usenet* fait en sorte qu'une multitude d'informations s'y trouvent. Pour s'y retrouver, un utilisateur peut effectuer des recherches parmi les articles publiés, périmés ou même rechercher un nom de groupe de nouvelles *Usenet*. Le service *Deja.com*[545] archive et indexe pratiquement tous les articles publiés dans *Usenet* depuis un peu plus de 6 ans. Le site *Deja.com* n'archive pas par contre le contenu des groupes de discussion *Usenet* spécialisés dans la distribution d'images, de son et d'animation multimédia.

En affichant un article dans *Deja.com*, il est possible de deviner le profil de l'auteur en cliquant sur le lien « *Posting History* ». On pourra ainsi consulter tous les articles publiés par la même personne. Il est également possible avec *Deja.com* de consulter des articles par fil d'intérêt en utilisant la fonction « *view thread* » ou tout simplement en cliquant sur le nom du groupe de discussion[546].

---

539 *Ibid*. aux pp. 345-346 et 361-362.

540 Sauf quant à l'administrateur du serveur de groupe de nouvelles *Usenet* (ou *NNTP*) sur lequel on consultera les groupes. Il sera donc possible à l'administrateur de serveur *NNTP* de connaître les champs d'intérêt d'un utilisateur qui se sert de son serveur *NNTP*. Voir aussi *Protégez-vous sur Internet, supra* note 207 à la p. 180.

541 *Ibid*. à la p. 171.

542 *Le guide de l'internaute 2000, supra* note 136 à la p. 347.

543 *Ibid*. aux pp. 351 et 356.

544 *Ibid*. aux pp. 351 et 352 et 358-360.

545 Voir *Deja.com*, en ligne : <http://deja.com/usenet> (date d'accès : 2 novembre 2000). D'autres ressources indexent également le contenu des nouvelles ou messages *Usenet* récents, soit *Infoseek*, en ligne : <http://www.infoseek.com> (date d'accès : 2 novembre 2000), *Alta Vista*, en ligne : <http://www.altavista.com> (date d'accès : 24 avril 2001), *Hot Bot*, en ligne : <http://www.hotbot.com> (date d'accès : 20 juin 2001) et *TalkWay*, en ligne : <http://www.talkway.com> (date d'accès : 20 juin 2001).

546 Voir *Le guide de l'internaute 2000, supra* note 136 à la p. 366. Sur le fonctionnement de *Usenet*, voir P. Trudel *et al., supra* note 8 aux pp. 2-12 à 2-13 ; *Internet le guide 2000, supra* note 255 aux pp. 72-76 ; *Digital Evidence, supra* note 252 aux pp. 90, 107-11 ; *Cyber Law*, *supra* note 200 à la p. 24.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

Constats des limites à l'expectative raisonnable de vie privée lors de l'utilisation des groupes de nouvelles *Usenet*

Tout au long de cette section nous avons traité de la publication de messages vers un groupe de discussion *Usenet*[547]. Par sa nature, *Usenet* ne confère pas ou peu d'expectative raisonnable de vie privée, ne serait-ce que parce que les messages sont généralement envoyés à tous dans un but de publication pour fins de réponse[548]. Il s'agit en quelque sorte d'un appel à tous[549].

Cette ressource constitue principalement un outil de communication de personne à groupe ouvert[550]. On compare même *Usenet* à la plus grande place publique de tous les temps[551].

Du point de vue de l'individu, l'attente raisonnable de vie privée est diminuée par le fait qu'un utilisateur raisonnablement informé devrait savoir qu'en fournissant son nom et son adresse de courriel, il est susceptible de se faire retrouver dans Internet. De plus, le fait de choisir sciemment de participer à tel ou tel groupe et d'y laisser des messages ou opinions à la vue de tous, constitue en quelque sorte une renonciation à toute attente de vie privée, du moins quant au contenu du message et au fait qu'il se retrouve dans un groupe de discussion sous l'égide d'une thématique donnée[552], et ce, même si la thématique elle-même traite de questions rattachées à la vie privée[553]. *Usenet* n'est donc pas un forum où il est bon d'exercer son droit à la libre expression, mais plutôt un lieu qui appelle à la vigilance et à la prudence[554].

---

[547] En effet, dès qu'un message est envoyé dans un groupe de discussions *Usenet*, il est automatiquement envoyé aux quatre coins du monde; on accepte donc implicitement que tout le monde puisse le lire. On agit donc comme un diffuseur ou auteur sur *Usenet*. Cela aura pour conséquence que l'on pourra dresser un profil de tous les messages envoyés par le même auteur dans tous les groupes de discussions. Il sera conséquemment possible de relier l'adresse de courriel à un auteur, à moins d'avoir pris certaines mesures de sécurité pour contrer cette situation, notamment par l'utilisation de la commande « x-no-archive » dans l'en-tête de notre message. Cela aura pour effet que Deja.com ne l'archivera pas. Par contre cette commande ne sera pas respectée par tous les sites d'archivage. Il s'agit donc d'une protection relative. Voir *Protégez-vous sur Internet, supra* note 207 aux pp. 177-8.

[548] Certains manuels traitant de piratage informatique et de sécurité suggèrent d'utiliser *Usenet* comme plate-forme de départ pour trouver des informations sur certaines failles de sécurité qui pourraient ressortir du contenu de certains messages publiés. Voir notamment *Hacking Exposed, supra* note 272 à la p. 9 ; *Sécurité et protection*, *supra* note 210 aux pp. 49 et 72 ; Crume, Jeff, *Inside Internet Security*, Londres, Addison-Wesley, 2000, à la p. 99 [ci après *Inside Internet Security*]. De plus, un manuel destiné à l'obtention de preuves informatiques suggère de débuter par les groupes de discussion *Usenet* pour trouver une quantité impressionnante d'informations détaillées au sujet d'individus et de leurs interactions. Cette suggestion de rechercher dans les groupes de discussion *Usenet* en dit long sur le faible aspect privé du contenu des messages qu'on y trouve. *Digital Evidence, supra* note 252 à la p. 90. Voir aussi *Sécurité Optimale, supra* note 208 à la p. 576.

[549] On compare d'ailleurs cette ressource à un babillard électronique public accessible à toute personne possédant une connexion Internet. *Digital Evidence supra* note 252 à la p. 90.

[550] Sur la notion de communication de personnes à groupe ouvert, voir *Droit du Cyberespace*, *supra* note 8 aux pp. 2-11 à 2-20.

[551] *Protégez-vous sur Internet, supra* note 207 à la p. 163.

[552] Voir par exemple les groupes de discussion : *alt.society.anarchy*, *alt.anarchism.**, *alt.fan.jello-biafra* et *talk.politics.misc*, qui traitent d'anarchie. Compte tenu de la nature même de la thématique, il est raisonnable d'affirmer que les organismes d'application de la loi pourraient, de leurs bureaux, surveiller l'opinion publique émanant de ces groupes et éventuellement s'y infiltrer ou prendre toute autre action facilitant leurs enquêtes, notamment, compulser une liste de personnes pouvant être impliquées dans des activités illégales ou séditieuses. Voir *Sécurité Optimale, supra* note 208 à la p. 576.

[553] Voir à titre d'exemple les groupes de discussion : *alt.privacy*, *alt.privacy.anon-server* et *alt.privacy.clipper*.

[554] *Sécurité Optimale, supra* note 208 à la p. 577.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

Il existe par contre un certain anonymat lors de l'utilisation des groupes de discussion *Usenet*[555]. En effet, cet anonymat découle du fait qu'en publiant un message dans un groupe, il est impossible de deviner à qui il est destiné. De plus le message peut être envoyé sous n'importe quelle thématique, rendant ainsi le message insignifiant[556]. Il est d'ailleurs recommandé d'envoyer un message dans un groupe de discussion non modéré ou non supervisé, afin d'éviter que le message ne soit pas diffusé ou qu'il soit retiré pour cause de non-conformité à la thématique[557].

Nous considérons qu'il s'agit là d'un anonymat indirect en ce sens qu'il provient d'une utilisation non conforme à l'utilisation normale ou générale des groupes de discussion. Comme nous l'avons mentionné plus tôt, les groupes de discussion *Usenet* existent essentiellement pour discuter de sujets, publier des messages et y répondre. Ils n'existent pas pour envoyer des messages codés ou cachés à des destinataires précis qui ne seront pas détectés lors de la consultation de ceux-ci. Cet anonymat découle, en quelque sorte, d'un usage malveillant des groupes de discussion *Usenet*.

Du point de vue matériel et logiciel, la nature même de la ressource fait que l'on peut se faire identifier, voire même qu'il faut se faire identifier, puisque l'on doit fournir son adresse de courriel si on espère obtenir une réponse personnelle à un message[558]. Le fait qu'il existe en soi des fonctionnalités destinées aux groupes et des fonctionnalités reliées à la communication personnelle par courriel annonce clairement que la communication vers un groupe offre un caractère privé plutôt mince, voire inexistant.

Il y a également le temps de vie d'un message dans *Usenet*. De façon générale, cela dépasse rarement quinze jours. Cette période de publication favorise la permanence de l'information, ce qui en soi, porte atteinte aux attentes en matière de vie privée[559]. De plus, il y a le service

---

555 *Protégez-vous sur Internet, supra* note 207 à la p. 172.

556 Bien entendu, on peut ajouter à cette technique de dissimulation, un certain encodage pour être en mesure de déjouer les robots de surveillance et de compilation de données et les moteurs de recherche qui sondent les groupes de discussion *Usenet,* et ce, même si à la base le protocole *NNTP* n'a pas été conçu pour l'échange d'informations cryptées. On pourra utiliser la technique du rot 13 pour camoufler son message qui consiste à déplacer de 13 positions le caractère désiré, comme par exemple la lettre « a » rot 13 équivaut à la lettre « n » ou tout simplement rajouter des caractères tels les esperluettes entre chaque lettre du message, rendant le tout indétectable pour les robots. On peut également utiliser les deux techniques conjointement. Il s'agit en fin de compte de l'utilisation de techniques cryptographiques simples dont nous traiterons plus loin. Les organismes d'application de la loi ou les personnes mal intentionnées devront donc rechercher les messages « à la main », sans pouvoir utiliser de moteurs de recherche ou de robots, ce qui rend à toute fin pratique la tâche impossible. *Ibid*. aux pp. 178-9, 222 et 229.

557 R. Mansfield, *Hacker Attack ! Shield Your Computer From Internet Crime*, Alameda (CA), Sybex, 2000, aux pp. 25-27 [ci après *Hacker Attack*].

558 L'adresse de courriel utilisée dans *Usenet* devient une chaîne de caractère identifiable comme n'importe quelle autre chaîne de caractères s'y trouvant. Elle peut donc être retrouvée facilement par le moteur de recherche *Usenet* approprié. Voir *Sécurité Optimale, supra* note 208 à la p. 593. Il est conséquemment recommandé, si l'on ne veut pas être retracé ou reconnu par son adresse de courriel, d'utiliser certaines méthodes de camouflage d'adresse qui déjoueront les moteurs ou les robots de recherche. On pourra également utiliser un serveur de courriel anonyme, dont nous traiterons plus loin. Voir *Protégez-vous sur Internet, supra* note 207 aux pp. 178-80.

559 Garfinkel voit d'ailleurs *Usenet* comme une ressource favorisant la permanence des déclarations d'une personne. Il avance le concept de responsabilité absolue de nos propos et déclarations. Ce concept est basé principalement sur le fait qu'à l'époque, lorsqu'une personne faisait une déclaration publique, elle était « relativement » publique, en ce sens que seules les personnes de l'époque pouvaient facilement en avoir

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

de recherche *Deja.com*[560] qui archive et indexe même les messages et articles périmés. Un utilisateur raisonnablement informé du fonctionnement de *Usenet* ne pourra prétendre qu'il ne connaît pas cette ressource ou les autres services offerts notamment par *Alta Vista* et *Hot Bot*[561].

Seul bémol à la question de la permanence de l'information est le fait que l'outil *Deja.com* n'existait pas au début de *Usenet*[562]. Un utilisateur de *Usenet* pourrait conséquemment ne pas savoir qu'un tel service existe et qu'il favorise la permanence de l'information. Dans ce contexte, et dans la mesure où *Deja.com* est capable de reculer dans le temps, à l'époque où l'archivage et l'indexage systématique n'existait pas, il se peut qu'une personne puisse invoquer qu'elle ne pouvait raisonnablement s'attendre à ce que son message soit conservé, bien qu'il ait été envoyé à un groupe restreint de personnes. Dans ce cas, on pourrait affirmer que l'expectative raisonnable de vie privée varie selon la période à laquelle un message a été publié ou non.

Comme traité précédemment, c'est généralement notre fsI qui offre le service d'un serveur de groupe de nouvelles *Usenet*. L'expectative de vie privée à l'égard de l'identité des serveurs de nouvelles *Usenet* auxquels nous sommes abonnés, donc à l'égard des centres d'intérêt d'un utilisateur, sera tributaire de la relation de confidentialité établie entre le fsI et l'utilisateur.

Section V - Les sessions en mode terminal *Telnet*[563]

Nous commencerons cette section en faisant une description générale de la technologie. Nous traiterons ensuite de la session en mode *Telnet* et conclurons par le constat des limites à l'expectative raisonnable de vie privée lors d'une session en mode *Telnet*.

Description générale de la technologie

Telnet est une application permettant à l'utilisateur d'entrer en communication avec un ordinateur étranger dans un réseau TCP/IP[564]. On qualifie *Telnet* comme étant l'utilisation d'un ordinateur à distance et en temps réel[565]. La session *Telnet* permet à l'utilisateur d'entrer

---

connaissance, à moins bien sûr d'aller consulter des archives spécialisées 50 ans plus tard. Les archives étaient difficilement consultables et souvent inaccessibles. Avec une ressource comme *Usenet*, les propos et déclarations d'une personnes seront publics d'une façon « absolue », en ce sens qu'une personne pourra désormais y accéder et les consulter facilement, et ce, même si elles ont été faites il y a très longtemps. *Database Nation*, *supra* note 534 à la p.87. Voir également sur cette question *The Computer Privacy Handbook*, *supra* note 35 aux pp. 35-37.

560 Voir *Deja.com*, en ligne : <http://deja.com/*Usenet*> (date d'accès : 2 novembre 2000).

561 Voir *Alta Vista*, en ligne : <http://www.altavista.com> (date d'accès : 24 avril 2001) et *Hot Bot*, en ligne : <http://www.hotbot.com> (date d'accès : 20 juin 2001).

562 Comme précédemment mentionné, Deja.com est un outil spécialisé conçu spécifiquement pour effectuer des recherches sur *Usenet*. Les archives de Deja.com remontent au mois de mars 1995 et ses responsables tentent de compléter les informations afin d'étendre cette base de données jusqu'en 1979, soit l'année de sa création. Voir *Sécurité Optimale, supra* note 208 à la p. 596.

563 Les sessions Telnet « traditionnelles » sont appelées à disparaître. En effet, en raison de l'augmentation de l'utilisation des navigateurs Web et de la recherche en mode hypertexte, la plupart des banques de données sont maintenant construites pour faciliter de telles ressources et types de recherche. Voir *Le guide de l'internaute 2000, supra* note 136 aux pp. 81 et 367 ; *Internet le guide 2000, supra* note 255 aux pp. 22, 58 ; *Internet*, *supra* note 214 aux pp. 42-43, 45.

564 *Le guide de l'internaute 2000, supra* note 136 à la p. 560.

565 *ACLU c. Reno, supra* note 196 aux pp. 834-35.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

en communication avec des bases de données, des services d'information, des systèmes de gestion, etc., tous accessibles sur des ordinateurs étrangers[566].

Telnet est désormais utilisé à titre de ressource faisant partie intégrante d'un navigateur Web. Elle sera utilisée notamment lors de la consultation d'un catalogue de bibliothèques universitaires ou collégiales[567].

À l'aide d'un logiciel *Telnet*, un utilisateur se branche à partir de son poste de travail à un ordinateur étranger pour utiliser les programmes qui s'y trouvent, dans la mesure où il possède la permission de s'en servir.

Session *Telnet*

L'exposé conjoint dans *ACLU c. Reno*, décrit le contexte général d'une session *Telnet* :

> « *29. […] Another method to use information on the Internet is to access and control remote computers in "real time" using "Telnet." For example, using Telnet, a researcher at a university would be able to use the computing power of a supercomputer located at a different university. A student can use Telnet to connect to a remote library to access the library's online card catalog program* »[568].

Une session *Telnet* débute lorsque l'ordinateur « client » amorce une communication avec l'ordinateur jouant le rôle de « serveur ». Le logiciel de communication *Telnet* se charge de transformer et d'envoyer les commandes du « client » dans un langage compréhensible pour le « serveur ». Finalement, le logiciel de communication *Telnet* convertit les informations provenant du « serveur » pour qu'elles soient compréhensibles pour le « client » et lisibles pour l'utilisateur. Durant cette session, tout le traitement s'effectue sur le « serveur ». Ce n'est donc pas le « client », donc l'ordinateur de l'utilisateur, qui fait fonctionner le programme qui apparaît à son écran[569].

Avant l'implémentation des réseaux TCP/IP, on ne pouvait joindre les ordinateurs centraux que par des liens séries spécifiques. Pour ce faire, on utilisait un terminal « idiot ». On appelait ainsi ce terminal car il ne possédait pas la puissance de calcul suffisante, d'où la nécessité de le relier à un ordinateur plus puissant[570].

On reliait donc physiquement l'ordinateur « idiot » (le client) à l'ordinateur central plus puissant (le serveur) par un câble. Tout le traitement de l'information s'effectuait sur l'ordinateur central. Les terminaux, équipés de claviers, n'étaient en fait que des fenêtres qui

---

566 *Le guide de l'internaute 2000, supra* note 136 à la p. 367.
567 *Ibid*. à la p. 367.
568 *Supra* note 196 aux pp. 834-835.
569 *Le guide de l'internaute 2000, supra* note 136 à la p. 368 ; *Internet*, *supra* note 214 aux pp. 42-43.
570 *Le guide de l'internaute 2000, supra* note 136 à la p. 373 ; *Internet*, *supra* note 214 à la p. 43. La Cour suprême du Canada dans *McLaughlin, supra* note 192 s'est déjà penchée sur l'analyse d'un système informatique, ou réseau, organisé avec un ordinateur central et des terminaux. Il s'agissait en l'espèce de déterminer les éléments essentiels de l'infraction de vol de service en matière de télécommunications ou d'utilisation frauduleuse d'installations de télécommunications, contrairement à l'alinéa 287(1)b) du *Code criminel* de l'époque.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

permettaient de « voir » le traitement effectué par l'ordinateur central[571]. C'est ce qu'on appelle l'émulation de terminal.

Pour communiquer avec un « serveur » en mode *Telnet*, il suffit d'indiquer à l'endroit approprié du navigateur Web, ou du logiciel *Telnet*, l'adresse Internet du serveur[572]. Le port de communication IP par défaut lors de l'utilisation d'une session *Telnet* est le 23. Il se peut que certains serveurs n'utilisent pas le port IP 23. Il faudra conséquemment préciser le port de communication approprié à la fin de l'adresse demandée[573].

Lorsque la communication est établie avec le « serveur », celui-ci demande un nom d'utilisateur ainsi qu'un mot de passe. Si la réponse est correcte, un message de bienvenue apparaîtra et on informera quelquefois l'utilisateur de certaines statistiques le concernant, notamment la dernière date où il a accédé au serveur. Le serveur est maintenant prêt à recevoir les commandes qui varieront selon le type de services offerts par le serveur[574].

Constats des limites à l'expectative raisonnable de vie privée lors d'une session en mode *Telnet.*

Du point de vue matériel, les limites à l'expectative raisonnable de vie privée lors d'une session en mode *Telnet* découlent en grande partie des limites inhérentes en matière d'expectative raisonnable de vie privée rattachées à l'utilisation du protocole TCP/IP[575].

Par rapport aux individus impliqués dans ce type de communication, les limites découlent de la relation d'intimité établie entre l'organisme ou la personne contrôlant le serveur et l'utilisateur. La nature de la relation d'intimité entre ces deux parties dépend du type de service offert. Par exemple, une personne qui consulte les archives d'une bibliothèque nationale bénéficiera d'un niveau d'expectative raisonnable de vie privée moindre qu'une personne qui consulte à distance le serveur de son employeur pour les fins du travail.

Il y a également le fait qu'une session en mode *Telnet* se passe généralement en utilisant le port de communication numéro 23. Un ordinateur qui utilise ce port de communication a donc de grandes chances d'être en session *Telnet*. De plus, le fait que certains serveurs *Telnet* soient identifiés par leur port de communication spécifique annonce à tous que ce port IP de communication correspond effectivement à ce serveur. Dans ce contexte, le fait que l'on communique avec un tel serveur bénéficie d'une expectative raisonnable de vie privée réduite[576]. Finalement, compte tenu que la ressource semble de plus en plus vouloir

---

[571] *Le guide de l'internaute 2000, supra* note 136 à la p. 337 ; *Internet*, *supra* note 214 à la p. 44. Aujourd'hui, les micro-ordinateurs disposent de capacité de calcul suffisante mais peuvent sans difficulté se faire passer pour un terminal non intelligent pour les fins d'une communication en mode Telnet. Voir aussi *Internet*, *supra* note 214 à la p. 43).

[572] Avant l'utilisation des navigateurs Web, l'adresse était inscrite généralement de cette façon Telnet : machine.domaine.nom de domaine de dernier niveau. Avec l'utilisation des navigateurs Web, notamment Netscape 4.X et Explorer 5.X, les adresses sont maintenant demandées sous la forme suivante : //nom de domaine.nom de domaine de dernier niveau. Voir *Le guide de l'internaute 2000, supra* note 136 aux pp. 370-372 et 374-375.

[573] On indiquera alors « Telnet : //nom de domaine de dernier niveau : n » ou « n » correspond au numéro de port IP approprié autre que 23.

[574] *Le guide de l'internaute 2000, supra* note 136 aux pp. 371 à 374.

[575] Notamment quant à l'utilisation d'une connexion TCP/IP protégée ou non.

[576] Pour d'autres renseignements au sujet de l'utilisation d'une session Telnet voir notamment : Les *RFC* 854-

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

« s'intégrer » aux navigateurs Web, le niveau d'expectative raisonnable de vie privée du point de vue matériel deviendra de plus en plus tributaire des niveaux d'expectative raisonnable de vie privée que l'on retrouvent dans le Web[577].

Section VI - Le bavardage-clavier ou clavardage du service IRC[578]

Dans la présente section, nous ferons la description générale de la technologie. Ensuite, nous traiterons d'une session IRC. Nous enchaînerons avec la culture rattachée à l'utilisation du bavardage-clavier ou clavardage du service IRC pour finalement conclure par un constat des limites à l'expectative de vie privée lors de son utilisation.

Description générale de la technologie

Il s'agit d'une ressource Internet où l'on trouve des milliers de forums de discussion au sein desquels les utilisateurs s'échangent des messages en temps réel. Il s'agit d'une des ressources des plus populaires offertes dans Internet. Cela s'explique non seulement par la gratification immédiate que procure la communication en temps réel, mais également par le fait qu'une multitude de fichiers peuvent s'y échanger par le biais des versions les plus récentes des logiciels clients IRC[579].

IRC est présentement le réseau de bavardage-clavier ou clavardage le plus important et peut être utilisé par n'importe qui possédant une connexion Internet[580].

Un utilisateur se joint à un forum de discussion appelé canal IRC où l'on peut assister à des conversations et y participer en direct[581]. Lorsqu'on écrit une phrase à l'aide du clavier d'un ordinateur, tous les utilisateurs branchés sur le canal peuvent, presque au même moment, la lire et y répondre tout aussi rapidement[582].

On compare cette ressource à une « ligne en fête », soit une ligne sur laquelle plusieurs personnes peuvent parler simultanément. Il est approprié ici de reprendre la description d'une session de bavardage-clavier ou clavardage faite par Danny J. Sohier :

> « *On peut s'imaginer en train de déambuler dans un couloir sans fin. Une série de portes, de chaque côté dissimulent des pièces où des gens sont rassemblés pour discuter de différents sujets, et vous êtes invités à communiquer avec eux… dans certains cas. Dans chaque forum, on trouve un ou plusieurs modérateurs, un thème et des participants. Il arrive parfois qu'on y serve des victuailles virtuelles, et l'ambiance qui y règne est détendue. Toutefois, tempérez vos propos, car le*

8551 STO-8 (ajouter éventuellement l'*URL*). Quant à l'utilisation de Telnet par le biais de page Web, voir *Hytelnet*, en ligne : <http://www.lights.com/hytelnet/> (date d'accès : 20 juin 2001). Par contre, compte tenu que les sessions de communication en mode Telnet sont appelées à disparaître, le site de *Hytelnet* est également appelé à subir le même sort.

577 Voir la section traitant de l'utilisation des navigateurs Web.

578 *IRC* est l'acronyme de *Internet Relay Chat*.

579 *Hacking Exposed, supra* note 272 à la p. 647; *Digital Evidence, supra* note 252 à la p. 261.

580 Le réseau America Online possède également un important réseau de bavardage, mais il est séparé d'Internet et n'est accessible qu'à ses membres. *Digital Evidence, supra* note 252 à la p. 91.

581 On qualifie cette ressource de mode de communication en temps réel. Voir *ACLU c. Reno, supra* note 196 aux pp. 834-35.

582 *Le guide de l'internaute 2000, supra* note 136 à la p. 377.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

modérateur a le pouvoir de vous expulser momentanément, et même de vous bannir à tout jamais ! Vous ne trouvez pas votre bonheur ? Créez alors votre propre forum et invitez des copains. Vous pourrez ainsi tout vous permettre à l'intérieur de cet univers virtuel »[583].

On comprend donc par cette description imagée, qu'une session de bavardage-clavier ou clavardage implique souvent des discussions à plusieurs participants. Du moins, c'est ce que la technologie favorise à première vue[584]. L'analogie de la ligne en fête est également reprise dans la description d'IRC, énoncée dans l'exposé conjoint des faits se trouvant dans la décision *ACLU c. Reno*:

> « *27. Real time communication. In addition to transmitting messages that can be later read or accessed, individuals on the Internet can engage in an immediate dialog, in "real time", with other people on the Internet. In its simplest forms, "talk" allows one-to-one communications and "Internet Relay Chat" (or IRC) allows two or more to type messages to each other that almost immediately appear on the others' computer screens. IRC is analogous to a telephone party line, using a computer and keyboard rather than a telephone. With IRC, however, at any one time there are thousands of different party lines available, in which collectively tens of thousands of users are engaging in conversations on a huge range of subjects. Moreover, one can create a new party line to discuss a different topic at any time. Some IRC conversations are "moderated" or include "channel operators."*
>
> *28. In addition, commercial online services such as America Online, CompuServe, the Microsoft Network, and Prodigy have their own "chat" systems allowing their members to converse* » [note omise][585]

Les sessions IRC sont principalement accessibles de deux manières, en utilisant soit un logiciel spécialisé IRC, soit un service spécialisé sur un site Web[586].

---

583 *Ibid*. à la p. 377. Bien qu'on compare surtout cette ressource à une ligne en fête, certains usages malveillants y ont également cours. En effet certaines sessions de bavardage sont utilisées pour favoriser les discussions au sujet d'activités illégales et l'échange de photos et vidéos obscènes. Des pirates informatiques utilisent *IRC* pour discuter et socialiser, des pédophiles s'y rencontrent pour échanger du matériel obscène. *IRC* aurait même déjà été utilisé pour diffuser en direct une agression sexuelle commise sur des enfants. Ce serait l'aspect privé, immédiat et non permanent de certains types de communications effectuées par le biais d'*IRC* qui en ferait un conduit propice aux activités criminelles. *Digital Evidence, supra* note 252 aux pp. 91, 93. Il s'agit donc d'un milieu propice à la surveillance policière.

584 Il existe également d'autres réseaux plus petits utilisant Internet qui permettent aux utilisateurs de construire des places virtuelles en deux et même trois dimensions, leur permettant de créer des personnages tout aussi virtuels qui se rencontreront et bavarderont sur de multiples sujets. *Digital Evidence supra* note 252 à la p. 91 ; *Le guide de l'internaute 2000, supra* note 136 aux pp. 461-80. Nous ne traiterons pas en détails de ces environnements. Nous y ferons quelques références quand certaines de leurs caractéristiques correspondront avec *IRC*.

585 *ACLU c. Reno, supra* note 196 à la p. 835.

586 *Le guide de l'internaute 2000, supra* note 136 à la p. 380. Nous ne traiterons pas plus en détail du service de bavardage sur le Web. Nous référons le lecteur à la section traitant plus généralement du Web. De plus, dans certains des systèmes utilisant le Web, les commandes *IRC* ne fonctionnent pas toutes. La compréhension du fonctionnement d'une session de bavardage *IRC* entraînera donc la compréhension d'une session de bavardage à partir d'un site Web. Seules des fonctions propres à chacun des logiciels utilisés sur le Web feront en sorte que la discussion sur la session de bavardage *IRC* trouveront application. Voir *Le guide de l'internaute 2000, supra* note 136 à la p. 407.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>

Il existe plusieurs logiciels IRC[587] et causeries dans le Web[588]. Il s'agit de choisir celui qui nous convient, chacun possédant certains avantages et inconvénients. Par contre, dans l'ensemble, tous possèdent essentiellement les mêmes commandes et fonctions[589]. Il convient maintenant de traiter du fonctionnement d'une session IRC.

La session IRC

Une session IRC sera lancée lorsque l'utilisateur a fait démarrer le logiciel conçu pour cette ressource. Les ports IP 6667 à 6670 sont utilisés lors des sessions IRC[590]. Il est donc possible d'inférer qu'une session de bavardage-clavier ou clavardage est en cours si un port IP, portant un numéro de cette séquence, est utilisé sur un ordinateur donné.

Lors de la première session, le logiciel demande d'inscrire les paramètres qui seront utilisés pour chaque démarrage subséquent. Il faudra notamment sélectionner le serveur IRC auquel on voudra se brancher, inscrire son nom, son adresse de courriel et un pseudonyme IRC. Il est important de mentionner que seul le pseudonyme IRC est obligatoire. Il est d'ailleurs recommandé de ne pas fournir son adresse de courriel et de ne pas utiliser son vrai nom, notamment pour éviter de recevoir du courriel non sollicité. Malgré l'aspect grégaire de cette activité, il semble que les utilisateurs d'IRC aiment bien conserver leur anonymat[591]. C'est donc en quelque sorte l'utilisateur qui est maître du degré ou niveau d'anonymat qu'il veut bien conserver lors du réglage des paramètres du logiciel utilisé. Le niveau d'anonymat sera donc tributaire de la configuration choisie.

Un réseau IRC est composé de plusieurs serveurs[592] répartis ça et là dans Internet[593]. Ces réseaux ne sont pas externes à Internet; il s'agit plutôt de sous-ensembles, qui ne sont pas tous accessibles à l'ensemble de la communauté Internet. En effet le trafic IRC peut devenir trop lourd à supporter pour un serveur. L'administrateur du réseau se voit donc obligé de n'en permettre l'accès qu'aux utilisateurs de son site ou à ceux qui sont géographiquement plus

---

[587] Voir notamment les logiciels suivants : *mIRC*, en ligne : <http://www.mirc.com> (date d'accès : 9 juillet 2001), *IRCle*, en ligne : <http://www.microsoft.com/France/internet/produits/chat> (date d'accès : 9 juillet 2001) et *Ichat*, en ligne : <http://www.ichat.com> (date d'accès : 9 juillet 2001).

[588] Voir notamment les adresses suivantes : *Forum One*, en ligne : <http://www.forumone.com> (date d'accès 10 juillet 2001), *Ultimate ChatList*, en ligne : <http://www.chatlist.com> (date d'accès : 10 juillet 2001), *Web Chat Broadcasting Service*, en ligne : <http://www.pages.wbs.net> (date d'accès : 10 juillet 2001), *Web Talker*, en ligne : <http://www.webtalker.com> (date d'accès : 10 juillet 2001), *Ichat*, en ligne : <http://www.ichat.com> (date d'accès : 9 juillet 2001), *AbsoluteChat*, en ligne : <http://www.absolutechat.com> (date d'accès :10 juillet 2001) et *Chatalyst*, en ligne : < http://www.chatalyst.com> (date d'accès : 10 juillet 2001).

[589] *Le guide de l'internaute 2000, supra* note 136 aux pp. 380-382 et 408.

[590] *Le guide de l'internaute 2000, supra* note 136 à la p. 65 ; *Hacking Exposed, supra* note 272 à la p.660.

[591] *Le guide de l'internaute 2000, supra* note 136 aux pp. 382-383. Par exemple le réseau EFNet : www.efnet.com, contient plus de 8000 canaux *IRC* actifs. On y trouve 50 000 usagers, environ 150 administrateurs de serveur *IRC* et une cinquantaine de serveurs pour supporter toute cette infrastructure. Voir *Ibid*. à la p. 385.

[592] Les serveurs *IRC* s'échangent les messages des utilisateurs qu'ils hébergent, ce qui augmente la vitesse de lecture des messages de chacun. Le branchement à l'un des serveurs permet à l'utilisateur de se joindre aux nombreux canaux de conversation *IRC*.

[593] Voir notamment les réseaux suivants : *EFNet*, en ligne : <http://www.efnet.net> (date d'accès : 16 juin 2001), *Undernet*, en ligne : <http://www.undernet.org> (date d'accès 16 juin 2001), *DALnet*, en ligne : <http://www.dal.net> (date d'accès : 16 juin 2001) et *Chat Net*, en ligne : <http://www.chatnet.org> (date d'accès : 16 juin 2001).

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

près du serveur. Il est même recommandé de se brancher à un serveur géographiquement près du lieu où se trouve notre ordinateur pour obtenir une vitesse optimale de communication.

Il est intéressant de noter que les serveurs IRC sont identifiés par leur adresse Internet ou IP[594]. À partir de ces adresses, il est relativement facile d'identifier de quelle région provient l'utilisateur de tel ou tel serveur. Un utilisateur, lorsqu'il communique par le biais du réseau *IRC*, transmet indirectement dans la plupart des cas, sa localisation géographique, même s'il a pris soin d'utiliser un pseudonyme.

Un canal IRC (ou forum IRC) constitue un endroit virtuel où des utilisateurs échangent des commentaires en temps réel. Il existe des milliers de canaux différents traitant de presque tous les sujets possibles. Un canal sera identifié par un signe dièse « # »[595] apparaissant à l'écran du logiciel utilisé. N'importe qui peut créer un canal IRC. Certains rendront leur canal accessible à tous, d'autres le rendront accessible seulement à des personnes qu'elles connaissent[596].

Les fonctionnalités des logiciels IRC sont multiples. On pourra notamment créer un canal, rechercher un canal avec des paramètres spécifiques de recherche tels le sujet ou thème d'un canal et le nombre de participants, se brancher à un canal, accéder à un canal avec un mot de passe, quitter un canal, obtenir la liste des utilisateurs dans un canal, obtenir la liste des pseudonymes des adresses IP et de courriel et de certains détails supplémentaires sur les utilisateurs d'un canal[597]. Bien entendu, l'accès à l'information relative à l'adresse de courriel dépendra des informations qui auront été transmises par les utilisateurs lors de la session de branchement initiale. Il est d'ailleurs recommandé de ne pas donner sa véritable adresse de

---

[594] Par exemple pour le réseau *EFNet*, en ligne : <http://www.efnet.net> (date d'accès : 16 juin 2001), deux serveurs existent pour le Canada, soit « *IRC*.polymtl.ca » (port IP 6667) et « *IRC*.idirect.ca » (port IP 6667). Quant au *Undernet*, en ligne : <http://www.undernet.org> (date d'accès 16 juin 2001), trois serveurs existent pour le Canada soit : « montreal.qu.ca.undernet.org » (port IP 6660-6669) et « toronto.on.ca.undernet.org » (port IP 6660-6669) et « vancouver.bc.ca.undernet.org » (port IP 6650-6690). Finalement quant au réseau *DALnet*, en ligne : <http://www.dal.net> (date d'accès : 16 juin 2001), trois serveurs existent pour le Canada, soit : « interlog.on.ca.dal.net » (port IP 6668,7000), « opus.bc.ca.dal.net » (port IP 6660-6669, 7000) et « raptor-ab.ca.dal.net » (port IP 6660-6669, 7000). Il est facile d'inférer qu'un utilisateur branché au serveur « polymtl » provient de la région de Montréal, qu'un utilisateur branché au serveur de « vancouver.bc » provient de la région de Vancouver et qu'un utilisateur branché au serveur « raptor.ab.ca » provient de l'Alberta. De plus, si l'on sait que tel ordinateur utilise les ports IP 6660-6669, on pourra raisonnablement inférer que l'utilisateur se branche à un serveur situé à Montréal ou à Toronto.

[595] *Le guide de l'internaute 2000, supra* note 136 à la p. 389. Un exemple de canal *IRC* est #quebec.

[596] *Digital Evidence, supra* note 252 à la p. 111.

[597] *Le guide de l'internaute 2000, supra* note 136 aux pp. 390-391. Il est intéressant de noter que la commande « *whois* » permet de connaître l'adresse de courriel, l'adresse IP, le serveur utilisé, le temps écoulé de la session de communication et le canal correspondant à un pseudonyme qu'une personne utilise. Il sera bien entendu très facile d'identifier éventuellement l'interlocuteur avec son adresse IP, à moins qu'elle ne corresponde pas à l'ordinateur effectivement utilisé pour communiquer avec *IRC*, ce qui impliquerait une technique de dissimulation d'adresse IP, que seuls des utilisateurs chevronnés pourraient modifier. De plus, la commande « *whowas* », permet de retracer l'ancien pseudonyme d'un utilisateur. Finalement, la commande « *who* », permet de rechercher à l'intérieur d'un réseau *IRC*, comme par exemple *DALnet*. On pourra notamment effectuer des recherches selon le nom de fournisseur de service Internet et le nom de domaine. Dans le cas d'une recherche par nom de domaine, on obtiendra tous les utilisateurs du réseau présentement en ligne provenant du serveur du nom de domaine spécifié. La commande « *who* » permet également de trouver n'importe quelle information apparaissant dans les informations personnelles d'un utilisateur en connexion sur un réseau *IRC*. *Digital Evidence supra* note 252 aux pp. 111-13.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

courriel lors de la session de branchement initiale[598]. L'adresse IP d'un utilisateur apparaîtra dans la très grande majorité des cas.

Chaque canal IRC possède en quelque sorte son maître de cérémonie. Cette personne s'appelle opérateur (ou modérateur) de canal IRC. Un opérateur de canal sera identifié à l'écran lors d'une session IRC, par une arobas « @ » devant son pseudonyme IRC. Il n'y a pas de limite au nombre d'opérateurs au sein d'un même canal[599].

On peut devenir opérateur de deux façons : soit en créant un nouveau canal, soit lorsqu'un opérateur vous octroie ce droit sur son canal. L'opérateur peut bannir les utilisateurs, changer le thème de la discussion du canal et octroyer divers droits aux utilisateurs[600].

Chaque canal IRC possède ses propres caractéristiques déterminées par l'opérateur du canal. Elles précisent le champ d'action des utilisateurs sur le canal. Certains logiciels affichent ces caractéristiques à l'écran lors d'une session.

On peut également, par le biais d'une commande, connaître les caractéristiques d'un canal, soit : modification possible du thème d'un canal, obligation d'être branché au canal pour communiquer, accès au canal sur invitation seulement, limitation du nombre d'utilisateurs, indication qu'il s'agit d'un canal modéré, c'est-à-dire que seuls les opérateurs peuvent échanger des commentaires qui demeurent toutefois accessibles à tous, indication qu'il s'agit d'un canal privé ou secret faisant en sorte que le canal n'apparaîtra pas lorsqu'on demandera une liste des canaux, indication que telle ou telle personne est bannie du canal, indication qu'un mot de passe est nécessaire pour accéder au canal[601].

Comme mentionné plus haut, à chaque fois que l'on participe à une session IRC, il faut choisir un alias ou un pseudonyme. On peut utiliser n'importe quel pseudonyme. Les seules limites sont le nombre de caractères maximum, soit neuf, et le fait qu'un pseudonyme ne peut être utilisé par deux personnes lors d'une session. Il faut alors se choisir un autre pseudonyme. Un des seuls endroits où le pseudonyme IRC est « protégé » pour un utilisateur, même lors de son absence, est dans le réseau *DALnet*[602].

Culture rattachée à l'utilisation du service de bavardage-clavier ou clavardage IRC

Le bavardage-clavier ou clavardage IRC n'implique pas seulement des paramètres techniques. Il implique également des acteurs, soit des utilisateurs (individus ou humains) et des robots. Il importe donc de connaître comment ces acteurs agissent et de bien comprendre la culture rattachée à l'utilisation des sessions IRC.

Une partie importante des activités dans IRC tourne autour de la création, de l'administration et de la destruction d'un canal. Pour créer un canal IRC, il suffit de se rallier à un canal

---

598 *Sécurité et protection*, *supra* note 210 à la p. 477. Si on désire absolument donner notre adresse de courriel, il est suggéré de donner une adresse secondaire. En cas de problème on pourra abandonner l'adresse secondaire et en utiliser une autre.

599 *Le guide de l'internaute 2000, supra* note 136 à la p. 392.

600 *Ibid*. à la p. 392.

601 *Ibid*. aux pp. 393-94.

602 *Ibid*. aux pp. 394-95.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

inexistant dont on devient l'administrateur. On devient ainsi l'opérateur du canal qui a le pouvoir d'en déterminer les caractéristiques et le thème[603].

Le canal cesse d'exister lorsque la dernière personne le quitte. Le canal est par conséquent fermé. Il est possible de perdre son droit d'opérateur si on quitte le canal et que quelqu'un d'autre l'ouvre en notre absence[604].

Afin d'éviter cette problématique, certains utilisateurs préfèrent garder des canaux ouverts de façon permanente. Au lieu de rester constamment en ligne sur un canal, ils rédigent et laissent derrière eux des programmes qui agissent comme utilisateur IRC. Ces programmes se nomment « robot ». Généralement, ces robots agissent dans les canaux où ils se trouvent et dans certains cas, les contrôlent[605].

Un robot est programmé pour accomplir certaines tâches, notamment celles d'offrir les droits d'opérateur chaque fois qu'un de ses maîtres apparaît sur le canal, et de ne répondre qu'à certaines commandes rédigées par son créateur.

Le robot peut également offrir de l'aide aux utilisateurs du canal, présenter des messages d'accueil, bannir des utilisateurs en fonction de leurs actions ou de leurs paroles et garder la trace des utilisateurs qui sont passés sur le canal[606].

Même si la nature du bavardage-clavier ou clavardage IRC favorise les discussions en groupe, il est possible également de se « retirer » et de parler un à un en ouvrant une fenêtre de causerie exclusive entre nous et un interlocuteur. On peut également communiquer des messages sur une base personnelle et envoyer des messages confidentiels qui ne seront pas vus des autres utilisateurs[607].

Par le biais des commandes DCC (*Direct Client to Client*) il est possible d'échanger des fichiers ou d'établir une connexion directe et confidentielle avec un autre utilisateur[608]. En théorie, cette communication ne laissera pas de trace sur les serveurs IRC utilisés. Il y aura

---

603 *Ibid*. à la p. 396.
604 *Ibid.*
605 *Ibid*. à la p. 399.
606 *Ibid*. aux pp. 399-400. Pour des exemples de robots voir notamment Opbot, Le petit robot Français, en ligne : <http://www.chez.com/opbot> (date d'accès : 23 juillet 2001), *MIRC-X Boots & Add-on*, en ligne : <http://www.m*IRC*x.com> (date d'accès : 23 juillet 2001) et le site des robots de *Hiersay*, en ligne : <http://www.hiersay.net/robots.htm> (date d'accès : 23 juillet 2001).
607 *Le guide de l'internaute 2000, Ibid*. aux pp. 397-98.
608 *Ibid*. aux pp. 398-99. Une personne qui établit une connexion en mode de communication directe *DCC* (ou en mode « *fserve* », l'équivalent de *DCC*, mais pour l'échange de fichiers) ne communique plus à travers les serveurs et le réseau *IRC*. Il peut être difficile d'imaginer comment on peut communiquer directement entre ordinateurs avec un logiciel client *IRC* sans passer par un serveur *IRC*. En fait, l'information passe directement d'un fournisseur de service Internet à l'autre. Le client *IRC* envoie donc directement l'information à l'adresse IP de l'autre ordinateur plutôt que de passer par les serveurs et le réseau *IRC*. En conséquence, le réseau *IRC* ne peut garder de trace de cette communication. Par contre, lors de l'établissement de telles connexions, l'adresse IP de l'ordinateur vers lequel on communique, apparaît directement à l'écran de l'ordinateur établissant la communication. Dans tous les cas donc, l'adresse IP est révélée. Une personne malveillante ou une personne représentant les organismes d'application de la loi, pourra connaître l'adresse IP de son interlocuteur. *Digital Evidence*, *supra* note 252 aux pp. 111-14.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

par contre d'autres façons d'obtenir des informations qui pourront révéler ce type d'activité[609].

Un autre personnage important joue un rôle dans l'environnement IRC. Il s'agit de l'administrateur IRC. L'administrateur IRC gère un secteur IRC. Même si l'administrateur n'a aucun pouvoir direct sur ce qui se passe sur les canaux, il peut toutefois fermer la connexion d'un utilisateur IRC en tout temps. Seul l'administrateur d'un site IRC a le pouvoir d'effectuer cette opération[610].

Constats des limites à l'expectative raisonnable de vie privée lors de l'utilisation du service de bavardage-clavier ou clavardage IRC

Cette agence de rencontre géante comporte plusieurs limites à l'expectative raisonnable de vie privée. La nature même de la technologie favorise les intrusions dans notre vie privée. Il semble d'ailleurs que beaucoup d'utilisateurs se servent de cette ressource pour effectivement révéler des pans entiers de leur vie privée. Utiliser IRC constituerait donc en quelque sorte une renonciation implicite à préserver une grande partie des détails de sa vie intime.

Par ailleurs, bien qu'il soit possible de préserver un certain anonymat, notamment en ne révélant pas sa vraie identité et en utilisant des sessions de conversations confidentielles, la mécanique de la technologie fera toujours en sorte de révéler certains aspects de notre vie privée, ne serait-ce que l'emplacement du serveur IRC que l'on utilise. L'expectative raisonnable de vie privée à l'égard de la localisation du site utilisé est donc à notre avis très faible, voire inexistante.

Certains pourront affirmer que les paramètres techniques ou la mécanique propre à la technologie ne sauraient constituer, en soi, une renonciation à préserver quelque partie de sa vie intime. Nous pensons au contraire qu'un utilisateur du service IRC ne peut être aussi naïf dans son appréciation subjective du degré de protection de sa vie privée dans un tel environnement. En effet, la nature même des fonctions de base annoncent à l'utilisateur qu'il renonce à certains aspects de sa vie privée en les utilisant ou en participant à un canal[611]. Il faut de plus une compréhension minimale du fonctionnement des multiples fonctions offertes par les divers logiciels. Cette compréhension minimale entraîne, selon nous, une connaissance inhérente des limites de la technologie, en matière d'expectative raisonnable. L'environnement technique et logiciel d'IRC ne tend généralement pas à favoriser la protection de la vie privée d'un utilisateur.

---

[609] Notamment par l'obtention des fichiers de journalisation (*log files*) se trouvant dans les ordinateurs des personnes qui auront communiqué de cette façon. *Digital Evidence, supra* note 252 aux pp. 111-12. Par contre, la consultation de ces fichiers de journalisation implique nécessairement l'obtention de l'ordinateur lui-même ou une quelconque intrusion à distance, pour y effectuer les recherches appropriées. Cela implique donc l'obtention d'une autorisation judiciaire préalable pour ce faire.

[610] L'administrateur *IRC* est l'équivalent du « magicien du palais » lors de l'utilisation du monde virtuel *The Palace*. *Le guide de l'internaute 2000, supra* note 136 aux pp. 400 et 473. Voir *The Palace*, en ligne : <http://www.thepalace.com> (date d'accès : 29 juin 2001).

[611] Notamment par l'utilisation des fonctions permettant de connaître la version du logiciel utilisé par un utilisateur, d'afficher les pseudonymes présents sur un canal, vérifier si des gens inscrits sur votre liste d'amis se trouvent sur *IRC*, d'ouvrir une fenêtre confidentielle avec un utilisateur *IRC* (*a contrario*) et d'obtenir des informations sur les personnes correspondant à un pseudonyme. Voir *Le guide de l'internaute 2000, supra* note 136 aux pp. 404-06.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

Quant à la partie plus « humaine » rattachée à l'utilisateur, IRC favorise plutôt la discussion de groupe où il est peu probable de prétendre à quelque expectative raisonnable de vie privée, du moins objectivement. Par ailleurs, même lorsque l'on se retrouve en conversation un à un, donc nécessairement dans le contexte où une conversation plus intime se tiendra et où des détails plus croustillants de notre vie intime sont susceptibles d'être révélés, IRC fait en sorte que l'on révèle généralement quelque chose à un interlocuteur qu'on ne connaît pas ou peu.

Il convient ici de reprendre le texte de Danny J. Sohier au sujet du comportement que l'on doit avoir dans un environnement IRC :

> « *Faites cependant attention de ne pas révéler trop de renseignements à votre sujet tant que vous n'aurez pas rencontré la personne avec laquelle vous communiquez. Il est impossible de se douter de qui [sic] se cache derrière les nombreux pseudonymes IRC. Cette mise en garde ne vise pas à vous faire peur, il s'agit simplement d'un conseil de quelqu'un qui s'est déjà fait prendre au jeu* »[612].

Dans ce contexte on devra toujours avoir à l'esprit que si l'on choisit mal son interlocuteur et que l'on parle avec un agent de l'État ou une personne malveillante, on risque que notre conversation soit enregistrée, le tout sans autorisation judiciaire préalable ou sans notre consentement[613]. On doit donc toujours avoir à l'esprit qu'une conversation avec un indicateur de police dans le « monde réel » ne bénéficie pas d'une expectative raisonnable de vie privée[614]. En sera-t-il de même dans le cadre d'une session IRC ? Il a déjà été décidé que oui, dans le contexte d'un babillard électronique, où des fonctions semblables de communication en temps réel étaient disponibles[615]. Le résultat risque donc d'être le même pour une session IRC. Aux États-Unis, la décision rendue dans *United States c. Charbonneau* confirme que la

---

612 *Ibid*. à la p. 409. Il est d'ailleurs recommandé de ne jamais accepter d'offre de transferts de fichier provenant de purs inconnus, notamment pour éviter de faire envoyer des programmes contenant des virus. *Hacking Exposed, supra* note 272 aux pp. 647-48 ; *L'Internet sécurisé*, *supra* note 379 aux pp. 314-15 ; *Sécurité et protection*, *supra* note 210 aux pp. 476, 481.

613 Certains services en ligne enregistrent et sauvegardent toutes les communications qui surviennent sur leur système. De plus, certains services fournissent également des utilitaires ou programmes qui permettent d'enregistrer les conversations. Voir *Hacker Attack, supra* note 557 à la p. 91. Dans la mesure où *IRC* permet la recherche et la sauvegarde de l'information, il favorisera donc la permanence et l'accessibilité à l'information, ce qui donnera un caractère absolu aux déclarations ou propos que nous y tiendrons. Voir à ce sujet *Database Nation*, *supra* note 534 à la p. 87. Voir par contre *Digital Evidence, supra* note 252 aux pp. 111-12, où l'on affirme que les activités sur *IRC* ne sont pas archivées. De plus, il ne sera pas possible d'enregistrer ou de conserver des communications qui seront effectuées directement entre deux personnes utilisant un logiciel client *IRC*, notamment parce que les serveurs du réseaux *IRC* ne sont pas empruntés pour communiquer. On compare ce type de communication à une communication téléphonique entre deux personnes.

614 *Duarte*, *supra* note 51 à la p. 67. Pour un exemple américain d'une opération d'infiltration par un agent civil utilisant *IRC*, voir un résumé des faits de *United States of America c. Carlos Salgado Jr.*, dans: R. Power, *Tangled Web. Tales of Digital Crime From the Shadows of Cyberspace*, Indianapolis, Que. (2000), aux pp. 88-92. Pour un extrait de l'affidavit d'un agent du FBI détaillant la technique utilisée par l'agent d'infiltration, voir l'affidavit du FBI, dans : *United States of America c. Carlos Salgado Jr.*, en ligne : *ZDNET NEWS CHANNEL* <http://www5.zdnet.com/zdnn/content/zdnn/0523/zdnn0009.html> (date d'accès : 28 juillet 2001).

615 *Morin*, *supra* note 121. Les babillards électroniques offraient généralement des services de transferts de fichiers, de messagerie électronique et de conférence. Le service de bavardage *IRC* est donc très semblable aux babillards électroniques d'autrefois, du moins quant aux services de messagerie et de conférence.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

preuve recueillie par des agents du FBI lors d'une session de bavardage-clavier ou clavardage, ne bénéficie pas d'une expectative raisonnable de vie privée :

> « *All of the evidence gathered by the FBI from the chat rooms resulted from the presence of undercover agents in the rooms. Clearly, when the defendant engaged in chat room conversations, he ran the risk of speaking to an undercover agent. Furthermore, Defendant could not have a reasonable expectation of privacy in the chat rooms. Accordingly, the e-mail sent by the defendant to others in a "chat room" is not afforded any semblance of privacy* » [616].

En définitive, la technologie favorise la tenue de conversation à la vue ou la connaissance de n'importe qui sauf, bien entendu, dans le cadre d'une communication directe d'ordinateur à ordinateur, n'empruntant pas le serveur IRC[617]. Un extrait de *Maxwell 2* résume bien le concept d'expectative raisonnable de vie privée dans le contexte des sessions de bavardage-clavier ou clavardage :

« […] *the more open the method of transmission, such as the "chat room", the less privacy one can reasonably expect* »[618]

Section VII - La téléphonie et vidéoconférence Internet

Dans la présente section, nous ferons la description générale de la technologie et traiterons de la session de communication par téléphonie et vidéoconférence Internet. Nous traiterons ensuite de la culture rattachée à l'utilisation de la téléphonie et vidéoconférence Internet, pour conclure par les constats des limites à l'expectative raisonnable de vie privée lors de leur utilisation.

Description générale de la technologie

Dans le cas de la téléphonie, on utilise généralement un microphone et un haut parleur ou des écouteurs pour communiquer, de la même manière qu'avec un téléphone régulier. Il s'agit de la communication téléphonique établie à partir d'un ordinateur en passant par Internet et le réseau téléphonique traditionnel. Elle peut se faire d'ordinateur à téléphone ou d'ordinateur à ordinateur. Il y a également la téléphonie par combiné qui utilisera Internet en tout ou en partie pour faire cheminer l'appel. Elle peut donc se faire sans l'utilisation d'un ordinateur. Quant à la vidéoconférence, il s'agit d'utiliser les mêmes composantes que pour la téléphonie à partir d'un ordinateur, en plus d'une caméra vidéo qui permet aux deux interlocuteurs de se voir en même temps lors de la communication. À l'instar du téléphone, il s'agit dans les deux cas de communications synchrones[619]. La communication effectuée par le téléphone à partir d'un ordinateur, et sa version plus moderne, la vidéoconférence, sont en quelque sorte

---

[616] *Charbonneau, supra* note 461 à la p. 1185.
[617] *Hacker Attack, supra* note 557 à la p. 91. Pour d'autres renseignements au sujet de la ressource *IRC* voir notamment la *RFC* 1459, en ligne : <www.normos.org/ietf/frc/rfc1459.txt> (date d'accès : 28 juillet 2001) ; *Internet*, *supra* note 214 aux pp. 75-76, 82-83 ; *Internet le guide 2000, supra* note 255 aux pp. 77-79 ; *Cyber Law*, *supra* note 200 à la p.26.
[618] *Maxwell 2, supra* note 316 à la p. 417.
[619] *Internet*, *supra* note 214 à la p. 47.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

intégrées à l'utilisation d'Internet. La plupart des logiciels offrant la téléphonie offrent également la vidéoconférence[620].

La session de communication par téléphonie et vidéoconférence Internet

Pour une communication d'ordinateur à ordinateur, un utilisateur devra, en plus des composantes matérielles décrites ci-dessus, utiliser un logiciel de communication spécialisé pour la vidéoconférence et la téléphonie Internet. Pour pouvoir établir une communication à partir d'un ordinateur, l'initiateur d'un appel devra préalablement établir une connexion Internet avec son fsI ou autrement selon le type de branchement à Internet. La connexion étant établie, il s'agira de joindre le destinataire en composant son numéro d'adresse IP. Le destinataire de la communication devra être lui aussi posséder un ordinateur branché à Internet muni d'un logiciel de communication compatible avec celui de l'initiateur, afin de pouvoir être joint[621].

Il faut être branché sur un serveur dédié au service de téléphonie Internet pour pouvoir établir une communication. Il s'agit ici encore une fois de l'approche client-serveur. Les protocoles utilisés pour communiquer varient énormément dans ce domaine. Il suffit de retenir que chaque interlocuteur voulant établir une communication devra utiliser un logiciel qui utilise le même protocole. Dans le cas contraire, la communication ne pourra être établie[622].

Pour pouvoir effectuer un appel Internet, un utilisateur doit être enregistré dans un annuaire dynamique dans Internet qui notera son adresse IP actuelle ainsi que les coordonnées de base qui auront préalablement été configurées dans le logiciel de communication. Il sera possible de communiquer avec un interlocuteur si on connaît exactement son adresse IP. Il sera également possible de le joindre par le biais de son adresse de courriel, si celle-ci est inscrite dans l'annuaire[623].

Plusieurs fonctions existent dans les différents logiciels de téléphonie et vidéoconférence Internet. Nous ne traiterons que des principales qui, à notre avis, sont les plus susceptibles d'avoir un impact sur une quelconque expectative raisonnable de vie privée. On peut généralement visionner un tableau blanc, grâce auquel les deux interlocuteurs peuvent visionner et modifier la même image en temps réel, partager une application ou programme avec un interlocuteur en direct, comme par exemple en effectuant des corrections en collaboration lors de l'utilisation du logiciel *Word*, initier une session de bavardage-clavier ou clavardage, échanger des fichiers entre les interlocuteurs et, finalement, chiffrer la communication pour assurer à la conversation une sécurité accrue.[624]

Plusieurs paramètres peuvent également être configurés sur ces logiciels. Les plus importants pour les fins de la présente étude ont rapport à l'identité de l'utilisateur et à l'utilisation d'une communication sécurisée par le biais de la cryptographie. Quant à l'identité de l'utilisateur, le logiciel demande notamment de fournir ses nom et prénom, son adresse de courriel et sa

---

620 Voir notamment *Internet Phone*, en ligne : <http://www.eurocall.com/e/ip5/htm> (date d'accès : 23 juillet 2001), *NetMeeting*, en ligne : <http://www.microsoft.com/windows/netmeeting> (date d'accès : 23 juillet 2001) et *CU-SeeMe*, en ligne : <http://www.cuseemeworld.com> (date d'accès : 23 juillet 2001).

621 *Internet le guide 2000, supra* note 255 à la p. 82.

622 *Le guide de l'internaute 2000, supra* note 136 à la p. 415 ; *Internet le guide 2000, supra* note 255 à la p. 82.

623 *Le guide de l'internaute 2000, Ibid*. à la p. 420.

624 *Ibid*. à la p. 418.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

localisation géographique. L'utilité de ces informations concernant l'utilisateur est de faire en sorte qu'elles apparaissent à l'annuaire du serveur où il est inscrit et qu'elles soient visibles à l'écran lors d'une communication. De plus, une option permet à l'utilisateur de ne pas faire apparaître ses nom et prénom dans l'annuaire et d'enregistrer automatiquement les coordonnées de tous les interlocuteurs dans un carnet d'adresse. Quant au volet communication sécurisée, l'utilisateur aura le choix d'établir ou non une communication chiffrée, soit pour les appels faits ou reçus[625].

Certains services permettent également de joindre une personne sur son téléphone ordinaire. Le premier type de communication offert est basé sur le modèle ordinateur/ Internet/passerelle/réseau téléphonique/téléphone. La communication est établie entre un ordinateur et un téléphone par le biais de passerelle de téléphonie Internet et les réseaux téléphoniques ordinaires. Pour joindre une personne par le biais de ce service, il faut tout simplement composer le numéro de téléphone requis à partir d'un ordinateur muni d'un logiciel de communication approprié[626]. Bien entendu, le destinataire n'a pas à être branché à Internet pour que la communication puisse être établie[627].

Le deuxième type de communication offert, est basé sur le modèle téléphone/réseau téléphonique/passerelle/Internet/passerelle/réseau téléphonique/téléphone. Ce type de communication permet de passer par Internet sans avoir à utiliser d'ordinateur ! On parle donc normalement d'un combiné à l'autre. La seule différence est que le réseau utilisé pour établir la communication n'est pas uniquement le réseau téléphonique ordinaire, mais aussi, Internet. Ce système est par contre coûteux et encore peu utilisé[628]. L'appel cheminera donc par le réseau téléphonique ordinaire, jusqu'à une passerelle de téléphonie Internet. L'appel cheminera dans Internet, jusqu'à une autre passerelle de téléphonie Internet qui rétablira le lien avec le réseau téléphonique ordinaire[629]. Il s'agit en quelque sorte d'une transmission hybride. Souvent cette mécanique ou architecture du réseau est totalement inconnue par l'utilisateur.

Culture rattachée à l'utilisation de la téléphonie et vidéoconférence Internet

Ces technologies sont appelées à prendre une expansion assez grande dans les prochaines années, notamment à cause de l'utilisation de plus en plus grandissante d'Internet, de l'augmentation du nombre d'équipements de télécommunication supportant le protocole de communication Internet IP et de la presque inexistence des frais d'interurbains rattachés à leur utilisation. On prévoit même qu'en 2002, entre 10% et 15% de toutes les communications téléphoniques dans le monde seront acheminées par le biais d'Internet[630]. L'avenir serait

---

625 *Ibid*. aux pp. 420-21.

626 *Internet le guide 2000, supra* note 255 aux pp. 82-83 ; *Le guide de l'internaute 2000, supra* note 136 à la p. 416.

627 *Internet Law*, *supra* note 332 à la p. 41.

628 *Internet le guide 2000, supra* note 255 à la p. 83.

629 *Internet Law*, *supra* note 332 à la p. 42.

630 Dans la majorité des cas il n'y a pas de frais d'appel interurbain car la connexion avec un serveur en est généralement exempte. Dans la mesure où la connexion à Internet est exempte de frais d'Interurbain, la téléphonie et la vidéoconférence en seront également exemptes, sauf pour la compagnie Net2Phone qui permet de joindre l'utilisateur d'un téléphone régulier. Voir *Net2Phone*, en ligne : <http://www.net2phone.com> (date d'accès : 16 juillet 2001). *Le guide de l'internaute 2000, supra* note 136, à la p. 416 ; *Internet le guide 2000, supra* note 255 aux pp. 82-83.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

moins prometteur en ce qui concerne la vidéoconférence, compte tenu des difficultés de transmission de l'image dans Internet, et ce, même avec une connexion haute vitesse[631].

La limite principale à l'utilisation de ces technologies est la vitesse de transmission des données requises pour une communication claire et efficace. Il est préférable, pour une communication adéquate d'avoir au moins recours à un modem de 56 kbps ou à une connexion haute vitesse par câble ou ligne téléphonique.

L'attrait principal de ces technologies, outre le fait que les frais d'interurbain soient, dans la majorité des cas inexistants, est le fait de pouvoir se voir en même temps lors d'une conversation. Cet attrait est surtout relié à la nouveauté du phénomène. Un autre attrait non négligeable est le fait de pouvoir partager une application en même temps et de pouvoir s'écrire des choses sur un tableau en direct. Certains diront qu'une image vaut mille mots!

Constats des limites à l'expectative raisonnable de vie privée lors de l'utilisation de la téléphonie et vidéoconférence Internet

À sa face même, l'expectative raisonnable de vie privée eu égard à cette ressource devrait être la même que celle accordée lorsqu'une personne établit une communication par le biais du téléphone[632]. Comme il en ressort de la discussion technique précédente, il s'agit d'un mode de communication synchrone, donc en direct, qui s'apparente grandement au fonctionnement du téléphone. En définitive, ce n'est que le « tuyau » ou canal de transmission qui est différent : au lieu d'utiliser complètement le réseau téléphonique ordinaire, on utilise, du moins en partie, le réseau Internet pour communiquer. Qu'à cela ne tienne, Internet utilise parfois lui aussi le réseau téléphonique ordinaire pour fonctionner. Il faut donc, à notre avis, trouver ailleurs que dans la configuration du réseau, les rationalités qui peuvent affecter, d'une manière ou d'une autre, le niveau d'expectative raisonnable de vie privée rattaché à la téléphonie et vidéoconférence Internet.

Par ailleurs, lorsque la communication passe par Internet, elle est soumise à la technologie IP. Donc, la communication serait tributaire des limites inhérentes à l'expectative raisonnable de vie privée découlant de l'utilisation du protocole IP.

Ce sont plutôt les fonctions rattachées aux traces que peut laisser l'utilisation d'un tel service qui devront être évaluées sérieusement. En effet, l'inscription à l'annuaire fait en sorte que, généralement, le nom, l'adresse de courriel ainsi que l'adresse IP deviennent disponibles pour tous les autres membres du même service. L'expectative raisonnable de vie privée à l'égard de ces informations est conséquemment réduite. Il s'agit, en quelque sorte, d'une diffusion dans un annuaire public. Il faut se rappeler que l'utilisateur a le choix de faire apparaître ou non, son nom à l'annuaire. Il s'agit donc, du moins quant au nom, d'une diffusion volontaire de l'information qui pourra faire l'objet d'une recherche par le biais d'un moteur de recherche intégré aux fonctions de l'annuaire[633].

De plus, le carnet d'adresses et la fonction d'enregistrement automatique des coordonnées des interlocuteurs favorisent l'accumulation de traces indiquant leur identité. Dans le contexte où

---

631 *Internet le guide 2000, supra* note 255 à la p. 84.
632 *Duarte*, *supra* note 51 et les articles 183 et s. du *Code criminel*.
633 *Le guide de l'internaute 2000, supra* note 136 à la p. 424.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

l'ordinateur est accessible au public, un utilisateur subséquent pourra facilement avoir accès aux fichiers contenant cette information, confirmant du coup l'identité du ou des interlocuteurs de la personne ayant précédemment utilisé l'ordinateur.

Finalement, il ne faut pas négliger qu'une des caractéristiques inhérentes à la vidéoconférence, est que l'on montre à l'écran le visage de notre interlocuteur. Ceci peut paraître anodin en soi, mais prend toute son importance lorsque l'ordinateur d'un des interlocuteurs se trouve dans un lieu plus ou moins privé. Il sera facile pour un tiers de voir qui est à l'appareil, ce qui n'est pas le cas dans le contexte de l'utilisation du téléphone conventionnel. Comme dans le cas d'une communication téléphonique, l'utilisateur qui communique par la vidéoconférence Internet devra, à notre avis, prendre des mesures plus importantes que dans le cas d'un appel téléphonique ordinaire pour dissimuler son écran. S'il ne le fait pas il sera difficile d'invoquer une quelconque expectative raisonnable de vie privée à l'égard de l'identité de son interlocuteur[634].

Section VIII - La messagerie instantanée

Dans la présente section, nous ferons la description générale de la technologie et traiterons de la session de communication par messagerie instantanée. Nous traiterons ensuite de la culture rattachée à l'utilisation de la messagerie instantanée, pour conclure par les constats des limites à l'expectative raisonnable de vie privée lors de son utilisation.

Description générale de la technologie

La messagerie instantanée est un type de ressource Internet qui permet principalement à un utilisateur d'aviser ses amis, proches ou collègues, qu'il est branché dans le réseau[635]. Elle permet également d'entrer en communication avec l'utilisateur branché à Internet en tout temps, soit par le biais d'une session de bavardage-clavier ou clavardage, soit par l'envoi d'un simple message électronique[636].

La session de communication par messagerie instantanée

Lors de sa première session de messagerie instantanée, l'utilisateur doit s'inscrire auprès d'un réseau offrant le service. Le but principal de cette inscription est de se faire attribuer un

---

634 Articles 183 et 184 du *Code criminel* et *Duarte*, *supra* note 51 qui assimile en quelque sorte communication privée et communication bénéficiant d'une expectative raisonnable de vie privée. Voir également *a contrario* *Lubovac*, *supra* note 115.

635 Voir notamment les services de messageries instantanées *d'ICQ*, en ligne : <http://www.icq.com> (date d'accès :19 juillet 2001) , d'*AOL Instant Messanger*, en ligne : <http://www.netscape.com/fr> (date d'accès : 19 juillet 2001), de *MSN Messenger* de *Microsoft*, en ligne : <http://www.messenger.fr.msn.ca> (date d'accès : 19 juillet 2001) et de *Messenger* de *Yahoo !*, en ligne : <http://www.messenger.yahoo.com/intl/fr> (date d'accès : 19 juillet 2001).

636 *Internet le guide 2000, supra* note 255 à la p. 80 ; *Le guide de l'internaute 2000, supra* note 136 aux pp. 223-28, 481-82, 555 ; *Digital Evidence, supra* note 252 à la p. 260. D'autres méthodes peuvent également être utilisées pour communiquer avec l'utilisateur, notamment par l'envoi d'un courriel ou par l'établissement d'une communication téléphonique ou de vidéoconférence seul à seul ou en groupe. On peut aussi jouer à des jeux, acheminer des fichiers et des adresses sous forme d'*URL*. Des fonctions de navigation Internet et de gestion d'agenda sont également parfois intégrées aux logiciels de messagerie instantanée. Compte tenu qu'il ne s'agit pas là de leurs fonctions principales, nous n'en traiterons pas davantage dans cette section. Nous renvoyons le lecteur aux technologies particulières traitées précédemment pour connaître le niveau d'expectative raisonnable de vie privée rattaché à celles-ci, le cas échéant.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

numéro d'identification UIN (*Universal Identification Number*) qui servira à le différencier des autres utilisateurs. C'est par ce numéro que l'utilisateur sera désormais reconnu dans le réseau de messagerie instantanée utilisé. Chaque réseau de messagerie instantanée utilise ses propres numéros d'identification. Les utilisateurs de réseaux différents tels ICQ, *AOL Instant Messenger* de *Netscape*, *MSN Messenger* de *Microsoft* et *Messenger* de *Yahoo!*, ne peuvent donc pas, du moins à ce jour, communiquer entre eux[637]. Des ports de communication TCP différents seront utilisés par chacun des services. Par exemple *AOL Instant Messenger* utilisera le port numéro 1080, alors qu'ICQ, utilisera le port numéro 4000[638].

On demande lors de cette inscription de fournir ses nom et prénom, son adresse postale, son adresse de courriel, son âge, ses loisirs, ses centres d'intérêt et sa description physique. Afin de différencier les utilisateurs, on demande également de fournir un pseudonyme. L'utilisateur qui s'inscrit à ce service a parfois l'option de faire apparaître ou non ces informations dans la banque de données créée par le service. Il pourra également décider si les informations seront accessibles dans le Web en général ou seulement dans le réseau utilisé[639]. Cette banque de données équivaut à un répertoire géant, ou bottin, qui listera tous les abonnés du service de messagerie. Ils seront répertoriés selon les informations fournies afin qu'ils puissent en rencontrer d'autres ayant le même profil ou les mêmes centres d'intérêt.

Ces rencontres potentielles sont rendues possibles grâce à des moteurs de recherche qui permettent de trouver un autre abonné possédant les caractéristiques recherchées[640]. Il s'agit en fait d'une fonction qui se rapproche des services offerts par les lignes téléphoniques en fête ou de télé-rencontre : plus on voudra se faire retrouver, plus on fournira d'informations à notre sujet dans la banque de données lors de l'inscription.

Seul le pseudonyme est généralement requis pour l'attribution du numéro d'identité UIN. Donc, sauf quant au pseudonyme, les données inscrites sont entièrement à la discrétion de l'utilisateur. Il est par ailleurs recommandé lors d'une première utilisation de la messagerie instantanée de ne fournir que ses pseudonyme et adresse de courriel[641]. Contrairement à ce qui se passe lors de l'utilisation d'IRC, le pseudonyme peut être utilisé par plus d'un usager[642].

Lorsque l'enregistrement est complété, l'utilisateur pourra commencer à compiler une liste de contacts potentiels. Cette liste pourra être triée par catégories, un peu à la manière des signets dans les navigateurs Web. Pour activer le fonctionnement d'un logiciel de messagerie instantanée, il faut se brancher dans Internet. Un témoin, ou icône, apparaîtra dans le bas de l'écran indiquant à l'utilisateur que le logiciel est en fonction. À chaque fois qu'un branchement à Internet sera effectué, le logiciel entrera en fonction et signifiera automatiquement la présence de l'utilisateur à tous les contacts qui auront été compilés ou inscrits à la liste[643].

---

637 *Le guide de l'internaute 2000, supra* note 136 aux pp. 481-482.

638 Voir la liste des ports répertoriés sur le site de l'*Internet Assigned Numbers Authority* (*IANA*), en ligne : <http://www.iana.org/assignments/port-numbers> (date d'accès : 3 août 2001).

639 *Le guide de l'internaute 2000, supra* note 136 à la p. 225.

640 On pourra effectuer une recherche par numéro d'*UIN*, adresse de courriel, nom, prénom, pseudonyme ou champs d'intérêt. *Ibid*. aux pp. 226, 486-88.

641 *Ibid*. aux pp. 224, 484.

642 *Internet le guide 2000, supra* note 255 à la p. 80.

643 *Le guide de l'internaute 2000, supra* note 136 aux pp. 224-26 et 485-86.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

On peut débuter deux types de communication avec un utilisateur abonné. On peut envoyer un message ou bavarder en direct. On enverra généralement un message à un utilisateur qui ne sera pas branché au réseau. Ce message sera récupéré plus tard, lorsque l'utilisateur visé se branchera à Internet. Ce message est transmis en différé. On bavardera en direct avec un utilisateur, lorsqu'il sera branché à Internet. La session de bavardage s'effectuera par l'entremise du clavier de chaque utilisateur, qui verra apparaître à l'écran le contenu des messages envoyés et reçus[644].

Lorsqu'une session de bavardage-clavier ou clavardage sera établie, il sera possible de visualiser les détails fournis à la banque de données par l'interlocuteur. Ces détails peuvent également être visualisés par l'entremise du moteur de recherche propre à chaque réseau, le tout, bien entendu, sous réserve que la personne recherchée les a complétés correctement et fidèlement[645]. Dans le cas d'*AOL Messenger*, on pourra également voir si l'interlocuteur a fait l'objet d'avertissement de la part d'autres membres du réseau avec qui il a communiqué. Ces avertissements sont rendus possibles par une fonction permettant d'envoyer un avertissement à un interlocuteur grossier, inopportun ou harassant[646]. Quant à ICQ, il s'agit essentiellement d'une application non sécurisée. Il faut présumer qu'un interlocuteur pourra prendre connaissance de l'adresse *IP* de l'autre. Le site Web d'ICQ émet d'ailleurs un avertissement à cet effet[647]. Cela va à l'encontre de ce que le logiciel annonce. En effet, il est annoncé qu'il est possible d'ajuster certains paramètres, faisant en sorte que l'adresse IP est protégée et qu'elle restera inconnue d'un interlocuteur. Nous verrons qu'en pratique, cette protection est inefficace.

Culture rattachée à l'utilisation de la messagerie instantanée

Encore une fois ici, il s'agit d'un logiciel de communication servant à faciliter l'interaction sociale des utilisateurs d'Internet. Par contre, cela n'empêche pas que le logiciel soit d'une certaine utilité dans les milieux de travail[648]. Les différents paramètres qu'un utilisateur peut configurer avant d'utiliser la messagerie instantanée annoncent qu'elle est principalement utilisée pour faciliter les rencontres entre les utilisateurs : quelle serait l'utilité de donner sa description physique, son adresse de courriel, son adresse résidentielle et ses centres d'intérêt, si ce n'était pas le cas?

Une personne raisonnable qui utilise cette ressource sait donc que l'information qu'elle donne à la banque de données du réseau constitue en quelque sorte une diffusion de l'information personnelle. Cette information pourra être très détaillée dans certains cas, dans d'autres elle pourra être partielle. Une personne qui ne fournit qu'une information partielle dans un tel environnement, va en quelque sorte à l'encontre du but principal de cette ressource : trouver une personne et se faire trouver par d'autres.

---

644 *Ibid*. aux pp. 228, 488-89.
645 *Ibid*. aux pp. 227, 488-89.
646 *Ibid*. à la p. 227.
647 Pour le détail de l'avertissement, par rapport aux limites des fonctions de protection de l'adresse IP, voir *ICQ*, en ligne : <http://www.icq.com/directconnection> (date d'accès :19 juillet 2001).et *ICQ*, en ligne : <http://www.icq.com/support/security/ipprivacy.html> (date d'accès :19 juillet 2001).
648 *Internet le guide 2000, supra* note 255 à la p. 81 ; *Le guide de l'internaute 2000, supra* note 136 à la p. 483.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

Constats des limites à l'expectative raisonnable de vie privée lors de l'utilisation de la messagerie instantanée

Deux fonctions principales caractérisent la messagerie instantanée : la fonction d'avertissement de présence dans le réseau et la fonction de bavardage sous différents modes. Nous traiterons des limites en fonction de ces deux principales fonctions.

La fonction servant à avertir les tiers qu'un utilisateur est présent dans Internet est comparée à un téléavertisseur virtuel[649]. Si un utilisateur décide que sa présence sera connue des autres utilisateurs du service de messagerie instantanée choisi, il sera difficile de prétendre qu'il s'attend à ce qu'il existe une expectative raisonnable de vie privée élevée à cet égard : c'est la nature même de la technologie de faire savoir qu'on est présent! L'ampleur de l'expectative raisonnable de vie privée sera également modulée par le nombre de personnes que l'on inscrit dans sa liste de contacts. Plus il y aura de personnes avisées de notre présence dans Internet, moins on pourra s'attendre à ce qu'une expectative raisonnable de vie privée existe à cet égard.

Contrairement aux sessions de bavardage-clavier ou clavardage IRC, le bavardage effectué par le biais de la messagerie instantanée tend, en principe, à être de nature plus privée. Au lieu de se réunir dans des salles virtuelles de discussion, les utilisateurs de la messagerie instantanée doivent se chercher l'un l'autre et s'entendre mutuellement pour entamer une conversation. Même si cela limite les contacts entre les interlocuteurs, il n'en reste pas moins que cela favorise la tenue de discussions qui seront plus privées que dans d'autres réseaux de bavardage-clavier ou clavardage, notamment IRC.

Dans le cas d'ICQ, on peut raisonnablement affirmer qu'il n'existe peu ou pas d'expectative raisonnable de vie privée à l'égard de l'adresse IP d'un interlocuteur. En effet, par défaut, l'adresse IP d'un interlocuteur apparaît lors de l'établissement d'une communication. Même lorsqu'un utilisateur configure son logiciel pour masquer son adresse IP, il est relativement simple de la connaître quand même par l'utilisation de la commande « *netstat* »[650]. Cette commande très simple est disponible sous Windows 95 et 98. Elle permet, lorsqu'une communication est établie avec un interlocuteur, de connaître son adresse IP, même si la fonction de masquage de l'adresse IP a été activée[651].

Quant au contenu même de la communication en direct (synchrone), nous croyons qu'elle bénéficie de la même attente raisonnable de vie privée qu'une communication téléphonique régulière, dans la mesure bien entendu où il s'agit d'une communication un à un et qu'elle est effectuée dans des circonstances où l'on peut raisonnablement s'attendre à ce qu'elle ne soit pas à la vue et au su de tous. Pour la communication indirecte (asynchrone), l'attente de vie privée s'apparente à celle que l'on retrouve lors de l'envoi d'un courriel, notamment en raison du fait que le contenu des messages est stocké en attente chez des tiers avant la réception du message par le destinataire.

---

649 *Internet le guide 2000, supra* note 255 à la p. 80.

650 On décrit la commande « *netstat* » dans *Sécurité Optimale, supra note* 208 à la p. 760, de la façon suivante : Commande UNIX (également disponible sous Windows en MS DOS) qui affiche les connexions *TCP* courantes et leur adresse source.

651 *Digital Evidence, supra* note 252 aux pp. 95, 137.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

Nous venons de traiter des multiples contextes particuliers de communication apportés par Internet et les nouvelles TI. De tous ces contextes de communication émergent différentes expectatives raisonnables de vie privée. Par ailleurs, certaines technologies particulières sont susceptibles d'influer grandement sur le caractère privé d'une communication. Il convient donc maintenant de traiter des technologies particulières ayant une influence sur le caractère privé des communications effectuées dans les divers contextes apportés par Internet et les nouvelles TI.

Chapitre III - Les technologies particulières ayant une influence sur le caractère privé des communications effectuées dans les divers contextes apportés par Internet et les nouvelles TI

Nous venons de traiter des contextes généraux et particuliers apportés par l'utilisation de l'informatique, Internet et les nouvelles TI. Certaines technologies ont été développées expressément pour améliorer la protection des communications dans de tels contextes. Ces technologies sont la cryptographie, la stéganographie et les services anonymisateurs.

Section I - La cryptographie

Dans la présente section, nous débuterons par la description générale de la technologie. Nous traiterons ensuite de son évolution, des contextes de son utilisation et de son fonctionnement. Nous traiterons également de l'application particulière de la cryptographie dans le commerce électronique, du réseau privé virtuel ou VPN et du dilemme entre la protection de la sécurité du commerce électronique et de l'expectative raisonnable de vie privée, en opposition avec la protection de la sécurité nationale et publique. Nous conclurons en dégageant certains constats des limites à l'expectative raisonnable de vie privée lors de l'utilisation de la cryptographie.

Description générale de la technologie

Nous ne ferons pas une étude exhaustive du sujet qui pourrait, à lui seul, faire l'objet de plusieurs thèses de doctorat tant en mathématiques qu'en droit ! Nous irons donc à l'essentiel. Il suffit de retenir pour les fins de la présente étude, que la cryptographie est une technique que l'on peut utiliser pour cacher le contenu d'un message envoyé par le biais d'Internet[652].

Une multitude de définitions de la cryptographie existent. Nous en avons retenu une qui nous apparaît appropriée. Les lignes directrices de l'OCDE la définissent ainsi:

> « *La discipline incluant les principes, moyens et méthodes de transformation des données dans le but de cacher leur contenu sémantique, d'établir leur authenticité, d'empêcher que leur modification passe inaperçue, de prévenir leur répudiation et d'empêcher leur utilisation non autorisée* »[653].

La cryptographie est la science qui a pour but de protéger le caractère confidentiel d'une information donnée. Seul le destinataire de la communication est autorisé ou habilité à

[652] On peut également utiliser la cryptographie pour sécuriser les conversations téléphoniques empruntant Internet. On se servira par exemple de *PGP Phone* qui servira à chiffrer la communication modem à modem. Voir *PGP Phone*, en ligne : <http://www.pgpi.org/products/pgpfone/> (date d'accès : 12 novembre 2001).

[653] OCDE, *La politique de cryptographie : les lignes directrices et les questions actuelles*, (sans date), en ligne : <http://www.oecd.org//dsti/sti/secur/prod/gd97-204f.pdf> (date d'accès : 23 avril 1999).

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

décoder ou déchiffrer le message. Du grec "*kruptos*" et "*graphein*" qui veulent dire littéralement "secret" et "écriture", cette science du chiffrement n'est pas nouvelle. C'est plutôt la nouvelle utilisation de la cryptographie qui fait en sorte que de nouvelles techniques sont apparues. Ces techniques ont favorisé un essor technologique quantitatif et qualitatif.[654]

Évolution de la technologie et des contextes d'utilisation

Même si son utilisation remonte à l'époque de Jules César, la cryptographie a vraiment connu son essor lors de la première guerre mondiale. Il s'agissait essentiellement de protéger les communications radio qui, en raison de leur nature ubiquitaire, étaient susceptibles d'interception par l'ennemi.[655]

La deuxième guerre mondiale a vu naître le premier téléphone numérique sécurisé appelé « Sigsaly ». Les Américains en étaient les inventeurs. L'idée était toujours d'être en mesure de communiquer sans que l'ennemi puisse intercepter la communication.[656]

Les ennemis des deux grandes guerres ont par la suite été remplacés par les espions de la guerre froide. Cette période d'après guerre a vu naître aux États-Unis, en 1952, le NSA.[657] C'est la grande époque des services de renseignement et de la chasse aux communistes. Il devenait donc utile pour cet organisme de pouvoir contrôler la cryptographie, outil de protection des communications. Il était question ici de sécurité nationale.

Les années 60 à 80 ont vu naître les premiers algorithmes de chiffrement informatiques, notamment ceux utilisés dans la cryptographie à clé publique ou asymétrique. Désormais, ces algorithmes ne sont plus l'apanage des militaires et des services de renseignement. Les universitaires et les civils peuvent maintenant contrôler, et à peu de frais, la sécurité dans leurs télécommunications.

Les années 90 verront les grands joueurs du commerce électronique s'approprier la cryptographie afin de pouvoir transiger en toute sécurité dans l'Internet.[658] L'augmentation des « marchandises », de l'argent et de l'information, qui transitent par l'Internet dans le cadre du commerce électronique, fait en sorte qu'une sécurisation des communications devient essentielle.[659]

Fonctionnement

La décision rendue dans *Bernstein c. United State Dept. of Justice* nous donne un bref aperçu du fonctionnement de la cryptographie :

---

654 *Droit du Cyberespace*, *supra* note 8 aux pp. 19-14 et 19-32; *The Computer Privacy Handbook*, *supra* note 35 aux pp. 69-123; *Cyber Law*, *supra* note 200 aux pp.93-96.

655 *Privacy on the Line, supra* note 23 à la p. 49.

656 *Ibid*. à la p. 53.

657 *NSA* pour *National Security Agency*. L'équivalent du *NSA* au Canada est le CST ou centre de sécurité dans les télécommunications. En anglais *CSE* ou *Canadian Security Establishement*.

658 *Privacy on the Line, supra* note 23 aux pp.49-76.

659 Deux groupes se sont formés autour de la controverse relative à l'utilisation de la cryptographie. D'un côté on retrouve les défenseurs de la vie privée et du libre commerce, et de l'autre, les défenseurs de la sécurité nationale et de l'ordre public. *Ibid*. à la p. 6.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

« *Cryptography is the science of secret writing, a science that has roots stretching back hundreds, and perhaps thousands, of years. See generally DAVID KHAN, THE CODEBREAKERS (2d ed. 1996). For much of its history, cryptography has been the jealously guarded province of governments and militaries. In the past twenty years, however, the science has blossomed in the civilian sphere, driven on the one hand by dramatic theoretical innovations within the field, and on the other by the needs of modern communication and information technologies. As a result, cryptography has become a dynamic academic discipline within applied mathematics. It is the cryptographer's primary task to find secure methods to encrypt messages, making them unintelligible to all except the intended recipients:*

> *"Encryption basically involves running a readable message known as "plaintext" through a computer program that translates the message according to an equation or algorithm into unreadable "ciphertext." Decryption is the translation back to plaintext when the message is received by someone with an appropriate "key." Bernstein III, 974 F. Supp. at 1292.*

The applications of encryption, however, are not limited to ensuring secrecy; encryption can also be employed to ensure data integrity, authenticate users, and facilitate non repudiation (e.g., linking a specific message to a specific sender). See id »[660].

De façon très sommaire, il s'agit pour l'émetteur du message d'appliquer une fonction ou clé mathématique, pour chiffrer le message qu'il désire faire parvenir au destinataire. Le destinataire utilise lui aussi une clé mathématique pour déchiffrer le message.

Il existe deux catégories principales de cryptographie : la cryptographie à clé publique (asymétrique) et la cryptographie à clé privée (symétrique). La cryptographie à clé privée est caractérisée par l'utilisation d'une seule clé ; la même clé sert à chiffrer et à déchiffrer le message. La cryptographie à clé publique se caractérise par l'utilisation de deux clés : une clé secrète et une clé publique. L'émetteur chiffre le message avec la clé publique du destinataire et celui-ci déchiffre le message avec sa clé secrète[661]. Ces deux clés sont complémentaires l'une de l'autre. Il n'est pas possible de déduire la contrepartie privée de la clé secrète et vice versa.

Cryptographie et commerce électronique

La cryptographie est essentielle au développement du commerce électronique. C'est surtout la cryptographie à clé publique qui en favorise l'émergence. Elle protège notamment la confidentialité de certaines données sensibles telles des numéros de carte de crédit[662] ou le

---

[660] *Bernstein c. United State Dept. Of Justice,* No. 97-16686 (9th Cir. 05/06/1999), aux para. 16-18 [ci après . *Bernstein*]

[661] S. Garfinkel, et G. Spafford, *Web Security & Commerce*, Sebastopol, CA : O'Reilly & Associates, 1997, pp.187-208 [ci après *Web Security*]; Canada, Centre de sécurité dans les télécommunications, *Qu'est-ce que la cryptographie à clé publique ?*, (sans date), en ligne : <http://www.cse-cst.gc.ca/cse/francais/gov3.html> (date d'accès : 25 avril 1999).

[662] Notamment pour la carte de crédit *Master Card*, voir *Secure Electronic Transcaction Protocol* (*SET*) :

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

contenu des courriels[663]. Elle permet également, grâce à l'utilisation de différentes techniques, d'assurer l'authentification de l'identité des parties qui communiquent, l'intégrité du contenu message et la non-répudiation de la réception ou acceptation des informations contenues au message.

Il est donc possible de s'assurer qu'un message n'a pas été modifié depuis son envoi par l'émetteur, que l'émetteur ne pourra répudier l'envoi d'un message et qu'il est bien celui qu'il prétend être.[664] Il s'agit du concept de signature numérique.

La mise en place des mécanismes de paiement nécessite généralement la mise en place d'une infrastructure dans laquelle un tiers certificateur entre en jeu pour garantir l'intégrité des transactions, tant au niveau de l'identité des parties qui transigent que du contenu de leur envoi.[665]

C'est ce qu'on appelle communément une infrastructure à clé publique (ICP)[666]. Ce tiers certificateur doit, notamment, voir à l'attribution des certificats d'authenticité aux différents participants, à la gestion et l'émission des clés publiques et secrètes nécessaires pour effectuer les différentes transactions en toute sécurité. Par le biais du tiers certificateur, l'ICP assurera la génération et la distribution des paires de clés publiques/privées et elle s'occupera de la publication de la clé publique et de l'identité de chaque utilisateur sous forme de certificats dans des babillards ouverts.

Généralement, l'autorité de certification pourra procéder à la récupération des clés pour accéder au texte en clair. Cet accès est nécessaire afin d'être en mesure de pouvoir au moins assurer le service en cas de mauvais fonctionnement, de perte des clés ou d'un mot de passe par un utilisateur. Il pourrait être également nécessaire pour annuler les clés dont la sécurité est compromise[667].

Secure Electronic Transcaction Protocol (*SET*), en ligne : <http://www.setco.org> (date d'accès : 8 novembre 2001).

663 Notamment le logiciel *Pretty Good Privacy ou PGP, en ligne :* <http://www.pgpi.com> (date d'accès : 22 novembre 2000). Voir aussi le site de Postes Canada, qui offre le service PosteCS[MC], en ligne : Postes Canada <http://www.canadapost.ca/business/offerings/postecs/can/default-f.asp> (date d'accès : 8 novembre 2001).

664 Notamment avec les modes ou mécanismes de paiement électronique suivants : *Secure Electronic Transcaction Protocol* (*SET*), en ligne : <http://www.setco.org> (date d'accès : 8 novembre 2001), *Mondex*, en ligne : <http://www.mondex.com/> (date d'accès : 12 novembre 2001) et *eCash Technologies Inc.*, en ligne : <http://www.digicash.com> ou <http://www.ecashtechnologies.com> (date d'accès : 8 novembre 2001).

665 Canada, Centre de sécurité dans les télécommunications, *Qu'est-ce que la signature numérique ?*, (sans date), en ligne : <http://www.cse-cst.gc.ca/cse/francais/gov4.html> (date d'accès : 25 avril 1999).

666 Canada, Centre de sécurité dans les télécommunications, *Qu'est-ce qu'une infrastructure à clé publique ?*, (sans date), en ligne : <http://www.cse-cst.gc.ca/cse/francais/gov5.html> (date d'accès : 25 avril 1999).

667 Canada, Industrie Canada, (21 février 1998), *Glossaire : s.v.* « la récupération des clés » :

> «Récupération des clés : large éventail de techniques permettant de récupérer un texte clair à partir d'un texte chiffré quand le tiers responsable du déchiffrement ne possède pas la clé de déchiffrement (c'est-à-dire que la clé est perdue; le mot de passe chiffrant la clé a été oublié; les mandataires autorisés des tribunaux qui, autrement, n'auraient pas accès à la clé cryptographique). La récupération peut prendre les formes suivantes : 1) récupération d'une clé de chiffrement de longue durée d'une entité qui a été conservée dans un endroit secondaire (parfois appelé sauvegarde commerciale de la clé ou entiercement selon la personne qui contrôle les clés de sauvegarde); 2) encapsulage des clés; ou 3) techniques de dérivation des clés grâce auxquelles la clé confidentielle sera régénérée à l'une des extrémités de la communication par le tiers de confiance qui a fourni les

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

Le réseau privé virtuel ou VPN

Le réseau privé virtuel est une méthode permettant de connecter des réseaux en utilisant Internet comme support de données. Il est qualifié de « virtuel », parce qu'il n'est pas constitué de liaisons physiques spécialisées : toute l'information est véhiculée par Internet. Il est « privé », parce que les données empruntant Internet sont chiffrées en utilisant un protocole qui permet d'établir un « tunnel » ou canal sécurisé. C'est un réseau parce qu'il relie des ordinateurs en réseau. Au lieu que ce soit les données elles-mêmes qui soient chiffrées, c'est le tunnel ou canal par lequel elles passent, qui l'est. Le protocole de *tunelling* utilise des algorithmes de chiffrage et de ce fait, les données transitant dans Internet conservent intégrité et confidentialité[668].

Il devient donc possible d'établir un canal ou tunnel sécurisé entre n'importe quel réseau utilisant le protocole TCP/IP, tel Internet, et un réseau de type LAN qui lui est raccordé. Il est alors possible d'accéder à un LAN branché à Internet depuis n'importe quel endroit de la planète, une fonction particulièrement utile pour les travailleurs devant se déplacer[669]. Rien n'empêche également que les données qui circulent dans le canal ou tunnel sécurisé, soient elles-mêmes chiffrées, ce qui résulte en une communication hautement confidentielle, du moins du point de vue subjectif de l'utilisateur.

Privilégier la sécurité du commerce électronique et l'expectative raisonnable de vie privée ou la sécurité nationale et publique?

Principalement deux groupes se sont formés autour de la controverse relative à l'utilisation de la cryptographie. D'un côté, on retrouve les défenseurs de la vie privée et du libre commerce et de l'autre, les défenseurs de la sécurité nationale et de l'ordre public[670]. La décision dans *Bernstein c. United States Dept. of Justice* traite de cette question :

> « *It is, of course, encryption's secrecy applications that concern the government. The interception and deciphering of foreign communications has long played an important part in our nation's national security efforts. In the words of a high ranking State Department official:*
>
> > *"Policies concerning the export control of cryptographic products are based on the fact that the proliferation of such products will make it easier for foreign intelligence targets to deny the United States Government access to information vital to national security interests. Cryptographic products and software have military and intelligence applications. As demonstrated throughout history, encryption has been used to conceal foreign military*

éléments mathématiques originaux utilisés pour générer la clé.» en ligne : <http://strategis.ic.gc.ca/cgi-in/basic/ftgetdoc?table=infoallf&fname=..%2Fauthorsf%2Fsgml%2Fdoc%2Fcy00013f.html&ft_cid=108993&headline=Glossaire&id=19851&lang=f&where=((ft_text%20CONTAINS%20'cryptographie'))%20AND%20(product%20CONTAINS%20'155')%20> (date d'accès : 28 avril 1999).

668 *Les réseaux*, *supra* note 136 à la p. 106 ; *Inside Internet Security*, *supra* note 548 à la p. 162.

669 *Dictionnaire de l'informatique, supra* note 203 à la p. 948.

670 *Privacy on the Line, supra* note 23 à la p. 6.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

> *communications, on the battlefield, aboard ships and submarines, or in other military settings. Encryption is also used to conceal other foreign communications that have foreign policy and national security significance for the United States. For example, encryption can be used to conceal communications of terrorists, drug smugglers, or others intent on taking hostile action against U.S. facilities, personnel, or security interests." Lowell Decl. at 4 (reproduced in Appellant's Excerpts of Record at 97).*
>
> *As increasingly sophisticated and secure encryption methods are developed, the government's interest in halting or slowing the proliferation of such methods has grown keen. The EAR regulations at issue in this appeal evidence this interest* »[671].

C'est ici qu'entrent en jeu les problèmes reliés à l'utilisation illégitime de cette technologie. En effet, il est facile d'imaginer que des esprits malveillants peuvent se servir des différentes technologies utilisant la cryptographie à des fins illégitimes. Par exemple, les mécanismes de paiement utilisant la cryptographie peuvent faciliter le blanchiment d'argent[672].

Étant donné la force de la cryptographie utilisée ou qui pourrait l'être, il est pratiquement impossible pour les organismes d'application de la loi de déchiffrer ou d'intercepter une communication chiffrée[673]. Pour la cryptographie symétrique, la technique du triple *DES* (trois passages du *Data Encryption Standard* simple) peut atteindre une clé de 192 bits alors que pour la cryptographie asymétrique, la technique *RSA* (initiales des inventeurs *Rivet Shamir* et *Adelman*) peut atteindre 2048 bits. Plus le nombre de bits est élevé, moins il est possible de pouvoir décrypter. Compte tenu du temps et des ressources requis pour décrypter une clé à 192 bits, il devient académique de se poser la question des probabilité qu'une clé à 2048 bits soit compromise.

Compte tenu de la facilité avec laquelle ces nouvelles techniques sont utilisables et mises en place, on peut comprendre que les organismes d'application de la loi soient très préoccupés par la menace potentielle d'une utilisation abusive de celles-ci[674]. Le gouvernement canadien propose également de modifier le *Code criminel* et d'autres lois pour protéger la sécurité publique, en criminalisant la divulgation de clés, en décourageant le chiffrement à des fins criminelles, en décourageant l'utilisation de la cryptographie pour dissimuler des éléments de

---

671 *Bernstein, supra* note 660 aux para. 19-21.

672 Canada, Ministère de la Justice et Solliciteur Général, *Le blanchiment de la monnaie électronique : Analyse de Justice Canada et du Solliciteur Général du Canada*, Ottawa, 1998, en ligne : <http://www.sgc.gc.ca/home/reportsdoc/ppc/fmoney.doc> (date d'accès : 23 avril 1999). Voir également *Transnational Criminal organizations, supra* note 339; *Un monde sans loi*, *supra* note 339; L*a criminalité informatique*, *supra* note 339; *Blanchiment d'argent et crime organisé*, *supra* note 339.

673 Selon S. Garfinkel, et G. Spafford, *Web Security, supra* note 661 à la p. 197, une clé de 128 bits a peu de chance d'être compromise :

> «*On the other hand, a 128 bit key is highly resistant to a key search attack. That's because a 128-bit key allows for 2^{128} ($3,4 \times 10^{38}$) possible keys. If a computer existed that could try a billion different keys in a second, and you had a billion of these computers, it would still take 10^{13} years to try every possible 128-bit RC4 key. This time span is approximately a thousand times longer than the age of the universe, currently estimated at $1,8x10^{10}$ years*.»

674 Canada, Industrie Canada, *Résumé de la politique canadienne en matière de cryptographie*, Ottawa, 1998, (groupe de travail sur le commerce électronique), en ligne : <http://e-com.ic.gc.ca/francais/fastfacts/43d7.htm> (date d'accès : 28 avril 1999).

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

preuve et en appliquant au contexte de la cryptographie les procédures existantes d'interception, de recherche, de saisie et d'aide.[675]

Constats des limites à l'expectative raisonnable de vie privée lors de l'utilisation de la cryptographie

Aujourd'hui, il est question d'infrastructure globale de l'information, d'autoroute de l'information, et le commerce par Internet est partout. La notion à la base de ce constat est que nous déplaçons beaucoup de notre culture dans les différents canaux de communication. Si nous réussissons à le faire, nous devrons trouver des substituts digitaux pour beaucoup de nos habitudes dans le monde physique. Dans le domaine de la sécurité, beaucoup des nouvelles pratiques seront cryptographiques.

Dans certains cas, les correspondances sont évidentes. Dans le monde physique ou « réel », nous fermons les portes, nous nous déplaçons à l'écart, ou chuchotons pour plus d'intimité. Dans le monde numérique, il faut chiffrer[676].

Dans les sociétés qui ont dominé la culture humaine pour la plus grande partie de son existence, une conscience générale des modèles de contacts entre les gens constituait une caractéristique principale de la vie. Dans une société dominée par les télécommunications, les modèles de contacts sont beaucoup moins visibles à la personne ordinaire et beaucoup plus susceptibles d'être contrôlés par la police et les services de renseignements[677].

Les communications électroniques ont rendu les télécommunications trop utiles pour être évitées. Elles ont diminué, malgré les apparences, la diversité des canaux de communication par lesquels les messages écrits ont jadis transités. Elles ont également rendu l'acte d'intercepter invisible aux yeux de la cible et plus facile à effectuer[678].

Puisque aujourd'hui la plupart des conversations ne peuvent être faites que par téléphone, se placer à l'écart, pour préserver sa confidentialité, n'est désormais plus une mesure universelle de sécurité susceptible d'application. Il n'est pas réaliste de dire à quelqu'un : « Si tu n'acceptes pas la possibilité que notre communication puisse être interceptée tu as le choix de ne pas utiliser le réseau téléphonique ». Se placer à l'écart constitue l'expression d'un droit de garder notre conversation privée lors de nos contacts en face à face ; l'utilisation de la cryptographie constitue l'expression de ce droit dans le monde électronique[679].

Compte tenu des nombreuses situations où l'expectative raisonnable de vie privée peut être compromise dans Internet, certains pourraient avancer que pour être vraiment « privée », une communication, ou le canal par lequel elle transite, devrait être chiffré. Dans *Bernstein c. United States Dept. of justice*, on avance l'affirmation que le niveau d'expectative raisonnable de vie privée est en général si bas, qu'en pratique, pour pouvoir bénéficier d'une quelconque

---

675 Canada, Industrie Canada, Communiqué « Le ministre Manley présente les grandes lignes de la politique en matière de cryptographie » (1er octobre 1998), en ligne : <http://e-com.ic.gc.ca/français/releases/41d6.htm> (date d'accès : 28 avril 1999).

676 *Privacy on the Line, supra* note 23 à la p. 45.

677 *Ibid*. aux pp. 238-39.

678 *Ibid*. à la p.152.

679 *Ibid*. à la p. 240.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

expectative raisonnable de vie privée, il faudrait obligatoirement utiliser une méthode quelconque de chiffrement des données :

> « *In this increasingly electronic age, we are all required in our everyday lives to rely on modern technology to communicate with one another. This reliance on electronic communication, however, has brought with it a dramatic diminution in our ability to communicate privately. Cellular phones are subject to monitoring, email is easily intercepted, and transactions over the internet are often less than secure. Something as commonplace as furnishing our credit card number, social security number, or bank account number puts each of us at risk. Moreover, when we employ electronic methods of communication, we often leave electronic "fingerprints" behind, fingerprints that can be traced back to us. Whether we are surveilled by our government, by criminals, or by our neighbors, it is fair to say that never has our ability to shield our affairs from prying eyes been at such a low ebb. The availability and use of secure encryption may offer an opportunity to reclaim some portion of the privacy we have lost* »[680].

Nous estimons que toute communication ne doit pas nécessairement faire l'objet d'un traitement cryptographique pour être considérée comme sécurisée. Par contre, compte tenu de l'état de la technologie et de son fonctionnement, il est clair que le fait qu'une communication ait été chiffrée ou soit passée par un canal sécurisé, annonce sans équivoque que son auteur pourra facilement établir qu'il avait une expectative raisonnable de vie privée subjective très élevée.

Finalement, dans la mesure où la communication s'effectue dans le contexte d'une infrastructure à clé publique, donc dans le contexte de la présence d'un tiers certificateur, l'expectative raisonnable de vie privée sera tributaire de la relation de confiance établie entre celui-ci et l'utilisateur. Cette relation de confiance devra notamment exister tant à l'égard du contenu des messages, qu'à l'égard des informations relatives aux clés de chiffrement, pour qu'on puisse prétendre à un quelconque niveau de protection.

Section II - La stéganographie

Dans cette section, nous débuterons par la description générale de la technologie pour ensuite conclure en traitant de l'utilisation conjointe de la stéganographie et de la cryptographie.

Description générale de la technologie

La stéganographie serait «la science de la dissimulation». Son objectif est de cacher des informations importantes dans des informations banales, de telle manière que personne n'aura l'idée de les y chercher. Comme la cryptographie, la stéganographie n'est pas nouvelle. C'est plutôt sa capacité d'utilisation qui a été augmentée par l'émergence de l'informatique et des technologies de l'information. La stéganographie assistée par ordinateur a donc ouvert une nouvelle voie; il s'agit de dissimuler des textes dans des graphiques ou des fichiers son.

[680] S*upra* note 660 au para. 54.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

Cette technique profite de la structure binaire des données et se sert de l'effet bruit de fond : pour enregistrer des informations graphiques ou sonores sous forme numérique, elles sont divisées en bits, la plus petite unité d'information composée de 1 (un) et de 0 (zéro).

Un pixel ou une fraction d'un enregistrement sonore est toujours enregistré dans au moins un octet (composé de 8 (huit) bits). En modifiant ensuite l'un des ces 8 (huit) bits, l'information qu'il contient est également altérée. Toutefois, en choisissant avec soin les images ou les sons à manipuler, la modification n'est pas perceptible : elle tombe dans la catégorie du bruit de fond[681].

Utilisation complémentaire de la cryptographie

Cette technique utilisée seule serait relativement peu efficace. En effet, le fait de miser sur l'effet camouflage seulement pourrait être risqué pour quelqu'un qui désire réellement protéger les informations transmises. Il faut donc combiner cryptographie et stéganographie pour plus de sûreté ! Le message confidentiel sera d'abord chiffré par cryptographie, puis sera dissimulé dans des données anodines. La personne voulant intercepter le message devra non seulement découvrir que le fichier contient de l'information cachée, mais il devra également procéder à son décryptage, ce qui en pratique est presque impossible[682].

Il s'agit donc d'une variante non négligeable de l'utilisation de la cryptographie. Les questions relatives aux dangers de l'utilisation illégitime de cette technologie, pourraient être similaires aux dangers rattachés à la cryptographie, en ce sens qu'elle pourraient favoriser les communications secrètes et faciliter la commission d'infractions traditionnelles ou reliées aux technologies de l'information ou aux ordinateurs en général.

Section III - Techniques favorisant l'anonymat

Il existe présentement deux grandes approches pour protéger l'anonymat dans les environnements électroniques : le recours à des serveurs «anonymisateurs» Web et de courriel et l'utilisation de la cryptographie[683]. Nous en traiterons donc dans l'ordre dans la présente section. Nous conclurons ensuite en traitant des trois facettes de l'anonymat découlant de l'utilisation des diverses techniques de dissimulation dans Internet.

Les serveurs « anonymisateurs » Web et le service de courriel anonyme

Le service de courriel anonyme permet à l'utilisateur d'envoyer un courriel qui ne contient pas d'information relative à son identité. Le service de courriel anonyme se charge de retirer toute information susceptible d'identifier l'initiateur du courriel. Seul le message ne sera pas affecté[684].

---

681 *Sécurité et protection*, *supra* note 210 aux pp. 288-97.

682 *Steganos*, en ligne : <http://www.demcom.com/english/steganos> (date d'accès : 14 novembre 2000).

683 *Droit du Cyberespace*, *supra* note 8 aux pp. 11-59 à 11-60. Un exemple de ces techniques y est brièvement décrit : «Lorsqu'un usager affiche un message à un groupe de discussion (*Usenet*), le message est doté d'un en-tête. Celui-ci contient l'information nécessaire à l'acheminement du message de même qu'il contient généralement le nom de l'usager, l'auteur du message, une indication relative à l'endroit d'où origine le message ainsi que l'heure, la date et la nature de l'envoi. En théorie donc, il est possible de relier un message à son auteur à l'aide de cet en-tête. En pratique cependant, différents moyens permettent à un usager d'afficher aisément des messages anonymes où l'en-tête usuel est remplacé par un numéro.»

684 *Intrusion Detection*, *supra* note 238 à la p. 131.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

La navigation anonyme[685] dans Internet permet de se protéger des navigateurs trop indiscrets[686]. Dans le cas de la navigation Web, un serveur spécial, appelé aussi *proxy server* ou serveur mandataire, est utilisé comme intermédiaire. Les requêtes d'un utilisateur sont transmises à ce serveur qui répercute la demande à l'adresse effective, sous son identité, puis nous communique le résultat. Les serveurs Web consultés à l'adresse URL ne peuvent ainsi obtenir aucune information sur les personnes qui visitent leurs pages[687]. Ils n'obtiendront que l'information relative au serveur mandataire anonyme.

Le niveau d'expectative raisonnable de vie privée dans ce contexte sera tributaire de la relation de confiance établie entre la compagnie ou l'individu offrant le service, notamment en ce qui concerne la diffusion de l'information envoyée initialement par un utilisateur. En effet, dans bien des cas, des fichiers de journalisation seront créés par le serveur mandataire ou de courriel, rendant du coup l'information que l'on voulait cacher, disponible pour consultation ultérieure[688]. Un organisme d'application des lois muni d'une autorisation judiciaire appropriée, pourra *ex post facto* récupérer cette information au tiers offrant le service. Par contre, le fait qu'un organisme d'application de la loi puisse éventuellement récupérer l'information, n'affecte pas en soi le caractère confidentiel de la relation qui pourrait exister à l'égard de l'information détenue.

Utilisation complémentaire avec la cryptographie

Un certain type d'« anonymisation » permet, avec l'utilisation de la cryptographie à clé publique, d'assurer un quasi total anonymat. Cette technique permet également de créer de toute pièce des « personnalités pseudonymes », capables d'envoyer et de recevoir des messages sans que l'on puisse identifier l'initiateur.

Nous n'entrerons pas dans les détails de ces différentes techniques, mais il suffit de dire pour les fins de la présente étude, qu'elles sont plus sûres que la technique du serveur Web anonyme[689]. En effet, il n'est pas possible de récupérer l'information transmise, contrairement au serveur Web anonyme où sont généralement stockés les messages ou l'information concernant un utilisateur du service, correspondant à son numéro d'identité anonyme.

Les trois facettes de l'anonymat ?

Deux grandes valeurs entrent en conflit lors de l'utilisation de l'anonymat dans Internet : la liberté d'expression et le droit à la protection de la vie privée d'une part, en opposition au droit d'être protégé contre la commission de gestes illicites d'autre part[690]. C'est ce qu'on appelle généralement les deux facettes de l'anonymat.

---

685 Voir par exemple : *Anonymiser*, en ligne : <http://www.anonymiser.com> (date d'accès : 14 novembre 2000). Outre la navigation anonyme, ce site offre également le courrier électronique anonyme, l'hébergement sur un serveur anonyme et la publication de pages Web anonymes !

686 La navigation anonyme révèle généralement l'information suivante sur l'utilisateur : son nom de fournisseur de service Internet ou son affiliation organisationnelle, selon le type de branchement, sa localisation générale, son type d'ordinateur et de système d'exploitation, son type de navigateur Web et l'*URL* de la dernière page Web visitée. *Intrusion Detection*, *supra* note 238 à la p. 132.

687 *Sécurité et protection*, *supra* note 210 à la p. 394.

688 *Intrusion Detection*, *supra* note 238 à la p. 132.

689 *Ibid*. à la p. 134.

690 *Droit du Cyberespace*, *supra* note 8 à la p. 11-65.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

Bien qu'un commentaire anonyme ait peu de chance d'être sérieusement considéré, il n'en demeure pas moins que certains peuvent voir un avantage à ne pas être identifiés lorsqu'ils communiquent par le biais d'Internet[691]. À titre d'exemple, on peut raisonnablement imaginer que, dans certains pays plus ou moins démocratiques, l'anonymat puisse favoriser la liberté d'expression[692]. L'anonymat a également ses avantages dans Internet pour les utilisateurs légitimes qui décident, ou non, de donner leur vraie identité, ou qui se servent de technologies pouvant la préserver en matière de commerce électronique ou de communication[693]. La décision *ACLU c. Reno* traite de l'importance de l'anonymat dans Internet dans le cas de personnes pouvant faire l'objet de stigmates ou de discrimination :

> *« 121. Anonymity is important to Internet users who seek to access sensitive information, such as users of the Critical Path AIDS Project's Web site, the users, particularly gay youth, of Queer Resources Directory, and users of Stop Prisoner Rape (SPR). Many members of SPR's mailing list have asked to remain anonymous due to the stigma of prisoner rape »*[694].

La décision dans *Bernstein c. United States Dept. of Justice* traite également de cette problématique[695]. Par contre, il ne faut pas oublier qu'Internet favorise également les escrocs qui commettent des infractions liées à l'informatique ou non[696]. Les craintes d'être pris son nettement diminuées si on peut utiliser Internet en toute confidentialité. Il s'agit de l'utilisation illégitime, sans crainte d'être pris.

Nous soumettons qu'une troisième facette de l'anonymat doit être considérée. Il s'agit en fait du corollaire de la facette permettant l'utilisation illégitime sans crainte d'être pris. Certaines techniques d'enquête utilisées par les organismes d'application de la loi dans le « monde réel » font appel à l'anonymat ou à la tromperie. Il s'agit de l'utilisation de l'agent d'infiltration, de l'agent source ou de l'informateur anonyme. Pourquoi l'État ne pourrait-il pas utiliser ses «agents doubles ou informateurs virtuels» pour voir au maintien de l'ordre dans Internet et le « monde réel » ? Ces techniques sont légitimes dans le «monde réel», lorsqu'elles respectent certaines conditions. Quelles seraient les limites de l'utilisation de ces techniques dans Internet[697] ?

---

691 *Ibid*. aux pp. 11-59 à 11-68.

692 Fromkin, Michael A., *Anonimity and its Enmities*, 1995 J. ONLINE L. art. 4, au para.7, [ci après *Anonimity and its Enmities*] en ligne : <http://warthog.cc.wm.edu/Law/publications/jol/froomkin/.html> (date d'accès :21 avril 1999).

693 Comme par exemple par l'utilisation des modes de paiement électroniques sécurisés *Secure Electronic Transcaction Protocol* (*SET*), en ligne : <http://www.setco.org> (date d'accès : 8 novembre 2001) ou *eCash Technologies Inc.*, en ligne : <http://www.digicash.com> ou <http://www.ecashtechnologies.com> (date d'accès : 8 novembre 2001) ou par l'utilisation de *Pretty Good Privacy ou PGP, en ligne :* <http://www.pgpi.com> (date d'accès : 22 novembre 2000), pour l'envoi de courrier électronique sécurisé. Voir également Poste Canada, qui offre le service PosteCS[MC], en ligne : <http://www.canadapost.ca/business/offerings/postecs/can/default-f.asp> (date d'accès : 8 novembre 2001), qui permet la livraison protégée de documents et de courrier électronique par Internet et la communication en ligne confidentielle entre entreprises. Ce service permet également la création d'applications sur mesure et l'intégration des applications et des systèmes du commerce électroniques existants.

694 *ACLU c. Reno, supra* note 196 à la p. 849.

695 *Supra* note 660.

696 *Droit du cyberespace*, *supra* note 8 à la p. 11-59; *Anonimity and its Enmities*, *supra* note 692 aux para. 44-52.

697 La décision rendue dans *R. c. Tardif*, REJB 98-10965 (C.Q.), donne un bon exemple de l'utilisation d'une technique d'infiltration qui va quand même assez loin. Dans cette affaire, des agents de la douane américaine

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

Nous avons vu précédemment que la Cour suprême du Canada dans *Duarte* a rendu illégal, l'enregistrement subreptice d'une communication effectuée en privé dans le « monde réel ». Qu'en est-il de la même situation dans le monde virtuel? En fait, il s'agit de savoir si, dans un environnement tel Internet et ses multiples contextes particuliers, on peut raisonnablement s'attendre à ne pas être enregistré subrepticement par notre interlocuteur.

Contrairement à la situation dans *Duarte*, les personnes qui communiquent entre elles par le biais d'Internet, sont pratiquement toujours à distance l'une de l'autre et utilisent souvent un moyen de communication permettant l'enregistrement soit du contenu de la communication, soit des informations relatives au transport de celle-ci.

La décision rendue dans *Morin*, offre un bon exemple où la Cour a tout simplement rejeté la notion de surveillance participative dans le contexte de communications effectuées par le biais d'Internet et d'un babillard électronique. Il est important de reprendre en détail les faits de l'affaire, afin de bien comprendre le contexte technologique :

> « *L'accusé est l'opérateur d'un babillard électronique (B.B.S.) appelé «Underworld».*
> *Durant l'été 1994, un agent de la GRC qui était abonné à un autre babillard électronique connu sous le nom de «Skull BBS» a pris connaissance sur ce système d'annonces publicitaires, désignées comme messages publics, adressées à l'intention de tous et provenant du B.B.S. «Underworld».*

---

avaient constitué de toute pièce un site Internet offrant de la pornographie infantile. L'accusé y a commandé des vidéos qui ont été livrés à son domicile par un agent double de la Sûreté du Québec, d'où les accusations de possession de pornographie infantile contre Tardif. La Cour, se prononçant sur la demande d'arrêt des procédures de Tardif suite à un soit disant piège policier, confirme le droit des autorités policières d'infiltrer Internet pour réprimer la pornographie infantile. Elle affirme qu'il existe dans Internet des « lieux », des « zones » ou des « sites » qui permettent à des personnes d'obtenir, de s'échanger ou d'acheter du matériel de contenu pornographique interdit. C'est notamment parce que ces « zones », « lieux » ou « sites » existent, qu'il est possible de mettre sur pied un site Internet qui ne constituera pas un piège policier. La Cour se justifie ainsi :

> « [13] Avec l'arrivée des nouvelles méthodes de communication, l'État doit pouvoir aussi utiliser la technologie et si l'État réalise que l'Internet devient un endroit où des crimes sont commis, alors les policiers devraient être autorisés à créer des sites afin de décourager les personnes qui seraient désireuses de posséder du matériel de pornographie juvénile. Un problème cependant se pose si l'État est un état étranger. Dans notre cas, le fait que la Sûreté du Québec continue l'opération policière commencée par les douanes américaines fait en sorte que le problème de juridiction ne se pose plus.
> [14] On pourrait alléguer ici que les agents de l'État ont eux aussi commis une infraction en ayant en leur possession du matériel de pornographie juvénile l'ayant reçu des autorités américaines. Le tribunal, sans avoir à se pencher sur la légalité de la possession dans ces circonstances et même s'il décidait de l'illégalité de la possession, en viendrait à la conclusion que cette illégalité ne peut être fatale dans les cas d'enquêtes sur la possession de matériel de pornographie juvénile.
> [15] La pornographie juvénile implique des enfants et qui dit enfants dit protection supplémentaire. En effet, comment peut-on penser sérieusement à protéger les enfants si la société ne peut permettre aux autorités de l'État de prendre les moyens nécessaires et raisonnables d'enquêter et de décourager ceux qui seraient tentés, par le biais de l'Internet, d'obtenir du matériel de pornographie juvénile ».

Cette décision envoie un message clair aux utilisateurs. Les opérations d'infiltration, du moins dans le contexte de la répression de la pornographie infantile, semblent désormais permises par la jurisprudence au Québec.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

Ces messages publicitaires offraient en vente du matériel informatique et indiquaient dans leur texte deux numéros de téléphone auxquels les intéressés pouvaient référer pour obtenir davantage d'informations.
Un autre message publicitaire, publié sur le BBS Skull par le BBS Underworld, proposait, pour télédéchargement, des programmes informatiques récents et indiquaient trois numéros de téléphone à contacter.
C'est ainsi qu'en réponse à ces publicités, l'agent de la GRC, utilisant un ordinateur, un modem et un logiciel de communication fournis par l'État, entra, en octobre 1994, en contact avec le babillard Underworld.
Sans entrer dans le détail de toutes les communications qui surviendront entre le policier et l'opérateur du babillard Underworld, il suffit de dire que, dans le cadre d'une procédure d'accueil, le policier sera salué par un mot de bienvenue, qu'il lui sera indiqué le prix demandé pour accéder aux divers services offerts ainsi que le nombre de minutes d'utilisation y correspondant et, enfin, que l'opérateur lui indiquera son nom véritable et l'adresse à laquelle le paiement devra être envoyé.

Une fois ce paiement effectué, le policier se verra attribuer une cote d'accès supérieure qui lui permettra de profiter de tous les services offerts par le babillard Underworld.
Tout au long de ces contacts entre l'agent de la GRC et l'opérateur du babillard, le contenu des communications sera versé dans un fichier électronique afin d'être conservé par le policier. C'est d'ailleurs à partir de ce fichier que sera reproduit sur papier le contenu de ces échanges, qui sera produit sous la cote R-6.
Ultérieurement, d'autres policiers de la GRC, invoquant les informations obtenues à l'occasion de ces communications par ordinateur, obtiendront d'un juge de paix un mandat de perquisition pour saisir de Bell Canada des renseignements leur permettant d'établir un lien entre les numéros de téléphone mentionnés dans les publicités et le nom et l'adresse de leurs titulaires.
Enfin, s'appuyant sur le contenu des communications informatiques et sur le résultat de leur perquisition à Bell Canada, les policiers de la GRC obtiendront d'un deuxième juge de paix un mandat pour perquisitionner le domicile de l'accusé et y saisiront divers objets reliés à l'utilisation des ordinateurs »[698].

L'argumentation principale de Morin était que l'obtention des informations par l'agent de la GRC équivalait à une surveillance participative telle que l'avait définit le juge La Forest dans *Duarte*. L'information ayant été obtenue sans autorisation judiciaire préalable, on demandait l'exclusion des informations ainsi obtenues, ce qui aurait, en bout de ligne, invalidé la perquisition effectuée à son domicile. Quant à la méthode utilisée par l'agent de la GRC, la Cour conclut :

« *L'enregistrement ou l'introduction dans un fichier électronique du contenu des communications intervenues entre l'accusé et l'agent de la GRC constitue*

[698] *Supra*, note 121 aux pp. 1760-61.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>

assurément une méthode d'enquête et de conservation de preuve, tout comme l'était l'enregistrement des conversations privées dans l'arrêt Duarte »[699].

Restait donc à déterminer si la méthode constituait une immixtion injustifiée dans une quelconque expectative raisonnable de vie privée de Morin. Après avoir affirmé que la méthode d'analyse dans *Duarte* n'est plus celle privilégiée par la Cour suprême du Canada, la Cour conclut que l'existence d'une attente raisonnable en matière de vie privée doit être déterminée selon l'ensemble des circonstances.

La Cour applique donc les récents critères de l'époque rendus dans *Edwards*, aux faits de l'espèce et détermine qu'il n'y a pas d'atteinte à l'expectative raisonnable de Morin pour les raisons suivantes :

> « […]*1. La technique d'enquête utilisée par les policiers de la GRC n'a pas empiété sur le droit à la vie privée de l'accusé; et*
> *2. Si tel était le cas, l'accusé, compte tenu des circonstances de l'espèce, n'avait aucune attente raisonnable de respect de sa vie privée.*
> *En effet, l'examen des communications intervenues entre l'accusé et l'agent de la GRC démontre qu'aucun renseignement ou information de caractère personnel, à l'exception du nom et de l'adresse à laquelle faire parvenir le paiement, n'a été divulgué par l'accusé au policier.*
> *L'accusé n'a jamais fait connaître ses pensées, ses opinions, ses croyances, ses projets ou des détails de sa vie intime.*
> *Il n'a consenti à divulguer son nom et l'adresse où le paiement devait être acheminé que dans un contexte exclusivement commercial. L'accusé était dans la même situation que n'importe quel fournisseur de services ou de biens qui indique à son client son nom et l'adresse à laquelle le paiement devra être envoyé. Dans ce contexte de transaction d'affaires, le Tribunal est incapable de voir comment il peut y avoir empiétement ou intrusion dans la vie privée de l'accusé. Son nom et son adresse sont assurément des renseignements de caractère personnel. Mais en acceptant de les communiquer à son interlocuteur dans le contexte commercial en question, l'accusé a renoncé à revendiquer une protection de la sphère informationnelle de son droit à la vie privée.*
> *Même si on concluait que la vie privée de l'accusé était affectée par la technique d'enquête utilisée par les policiers, le Tribunal croit que l'accusé n'avait aucune attente raisonnable de respect de sa vie privée.*
> *La preuve démontre de façon concluante que l'accusé a fait publier par l'entremise d'un autre babillard électronique des messages destinés au public en général, dans lesquels il invitait les intéressés à communiquer avec lui par voie de modem à des numéros de téléphone qu'il indiquait.*
> *La preuve démontre également que l'accusé a donné son nom et une adresse dans le but de recevoir le paiement qui lui était dû.*
> *La preuve démontre au surplus que l'enregistrement par versement dans un fichier informatique du contenu des communications n'a pas été effectué de façon clandestine. Il a été amplement démontré que cette méthode de conservation de l'information est inhérente et essentielle au fonctionnement*

[699] *Ibid*. à la p. 1762.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>

> *efficace et rentable du médium utilisé et que tout opérateur de babillard électronique le sait.*
> *Enfin, il faut souligner que l'accusé n'a pas prouvé, personnellement ou autrement, l'existence d'une attente subjective de respect de sa vie privée, qui est un des facteurs à prendre en considération dans l'appréciation de l'ensemble des circonstances.*
> *En somme, l'accusé a lancé des invitations générales de communiquer avec lui, et ce, à plusieurs reprises. Il est impossible de conclure qu'une personne raisonnable, dans la situation de l'accusé, pouvait s'attendre au respect de sa vie privée en de telles circonstances. Une personne raisonnable saurait que, lorsque de telles invitations sont lancées au public en général, elle ne peut pas s'attendre à ce qu'il n'y ait pas d'étrangers, y compris des policiers, qui communiquent avec elle* » [notes omises][700].

Nous soumettons que si cette décision avait été rendue avant que les critères élaborés dans *Edwards* ne trouvent application, la conclusion aurait vraisemblablement été autre. En effet, comme nous l'avons exposé plus haut dans la présente étude, l'arrêt *Duarte* ne semble plus d'application, du moins quant au mécanisme de détermination de ce qui constitue une situation dans laquelle l'utilisation d'une technique d'enquête se transforme en immixtion injustifiée dans une quelconque expectative raisonnable de vie privée. Il s'agit d'un très bon exemple d'application des critères élaborés dans *Edwards* En fait, ce qui est intéressant dans *Morin*, c'est qu'il s'agit d'une décision relative à des faits spécifiques à un environnement, qui correspond encore aujourd'hui à bien des contextes de communication dans Internet. La décision dans *Morin* est lourde de conséquences pour les utilisateurs d'Internet. Elle vient confirmer que l'anonymat n'est pas seulement l'apanage des utilisateurs, mais qu'il peut aussi constituer une arme redoutable entre les mains des agents de l'État pour la répression de la criminalité dans, ou, utilisant Internet[701]. Les propos relatifs aux conversations avec un indicateur, avancés par le juge La Forest dans *Duarte*, prennent tout leur sens :

> « *Pour conclure, la Charte n'est pas destinée à nous protéger si nous choisissons mal nos amis. S'il s'avère que notre "ami" est un indicateur et que nous sommes reconnus coupables sur la foi de son témoignage, c'est peut-être malheureux pour nous. Mais la Charte a pour objet de garantir le droit à la protection contre les fouilles, les perquisitions ou les saisies abusives. Une conversation avec un indicateur n'est pas une fouille, une perquisition ou une saisie au sens de la Charte* »[702].

Dans Internet il faut, à notre avis, choisir encore mieux ses amis que dans la vie de tous les jours ou le « monde réel ». C'est la nature même de la technologie qui le commande.

Nous venons de traiter des contextes techniques généraux et particuliers de communication apportés par l'utilisation de l'informatique, d'Internet et les nouvelles TI en plus des

---

[700] *Ibid*. aux pp. 1763-64.

[701] Outre *Morin*, *supra* note 212, voir *R. c. Pecchiarich,* [1995] O.J. No. 1004 (Cour de l'Ont. Div. Prov.) ; *Hambrick*, *supra* note 237 ; *R. c. Kerster*, [2001] B.C.J. No. 274 (C.S. C.-B.), où des policiers se font passer pour des utilisateurs, trompant ainsi leurs cibles quant à leur véritable identité. Pour des exemples américains d'opérations d'infiltration par des agents de l'État voir *Charbonneau, supra* note 461 ; *United States c. White*, No. 00-2318 (10th Cir. 03/27/2001).

[702] *Duarte*, *supra* note 51 à la p. 57.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

technologies particulières ayant une influence sur le caractère privé des communications effectuées dans de tels contextes. Il convient donc maintenant de faire la synthèse de tous les nouveaux facteurs apportés par ces nouveaux contextes. Cette synthèse nous permettra de mieux les cerner, ce qui, éventuellement, pourra faciliter la détermination du niveau d'expectative raisonnable de vie privée s'y rattachant.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>

Partie III - Les nouveaux facteurs émanant des contextes apportés par Internet et les nouvelles TI influant sur le niveau d'expectative raisonnable de vie privée

Dans cette partie, nous présenterons les facteurs émanant des contextes de communication apportés par Internet et les nouvelles TI influant sur le niveau d'expectative raisonnable de vie privée. Nous élaborerons ensuite le **Tableau I** qui fera la synthèse des facteurs qui tendent à favoriser l'existence d'une expectative raisonnable de vie privée et ceux qui tendent à la nier.
Nous avons tout au long de l'étude, fait référence à une multitude de contextes généraux et particuliers découlant de l'utilisation d'Internet et des nouvelles TI. De ces contextes, émanent de nouvelles rationalités. De ces rationalités, émanent une multitude de nouveaux facteurs pouvant influer dans un sens ou dans l'autre sur le niveau d'expectative raisonnable de vie privée. Afin de mieux s'y retrouver, nous les avons divisés en deux grandes catégories : les facteurs qui tendent à favoriser l'existence d'une expectative raisonnable de vie privée lors de l'utilisation d'Internet et des nouvelles TI, et ceux qui tendent à la nier. Ces catégories et facteurs font l'objet d'un tableau contenu à la section suivante (voir le **Tableau I**).

Bien entendu, ces catégories peuvent être modulées dans un sens ou dans l'autre. L'idée est de pouvoir prendre conscience des nouveaux facteurs afin de pouvoir, le cas échéant, anticiper le mieux possible, quel sera leur effet lorsqu'un tribunal aura à déterminer de ce qui peut constituer ou non une situation où une expectative raisonnable de vie privée sera reconnue. Il faut également toujours garder à l'esprit que, même lorsqu'il sera déterminé qu'une expectative raisonnable de vie privée existe dans une situation donnée, celle-ci peut également varier quant à son intensité. Les facteurs énumérés dans le **Tableau I** peuvent donc jouer à divers niveau du raisonnement juridique.

Le **Tableau I** n'est pas une panacée. Il est appelé à être modifié à bien des égards, notamment en raison des changements technologiques et jurisprudentiels. Il a par contre l'avantage de donner un portrait général, une vue d'ensemble, des éléments principaux émanant des nouvelles TI et Internet, dont on devra généralement tenir compte dans la détermination de l'existence ou non d'une expectative raisonnable de vie privée. Il ne faut pas oublier que ce tableau ne tient pas compte des facteurs ou critères « ordinaires », élaborés par la Cour suprême du Canada dans son interprétation contextuelle de l'article 8 de la *Charte canadienne*[703]. Il est donc incomplet à certains égards, donc à utiliser avec prudence.
Tableau I. Identification des facteurs émanant des contextes apportés par Internet et les nouvelles TI[704]

Facteurs qui accroissent expectative raisonnable de vie privée	**Facteurs qui diminue l'expectative raisonnable de vie privée**
Le contexte de l'évolution des technologies de en matière de communication	
- La diminution des communications en présence l'un de l'autre	- L'augmentation des communications à distance
- Moins on exerce de contrôle sur l'information transmise ou sur le mode de communication utilisé	- Plus on exerce de contrôle sur le caractère privé de l'information transmise ou sur le mode de communication utilisé

[703] Comme par exemple l'application de la *Charte canadienne* dans un contexte réglementaire ou criminel proprement dit.
[704] Les divers facteurs ont été placés en opposition les un par rapport aux autres. Par contre, lorsqu'il nous semblait impossible de placer un facteur en opposition à un autre, nous avons laissé la case vide.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

Facteurs qui accroissent expectative raisonnable de vie privée	Facteurs qui diminue l'expectative raisonnable de vie privée
- La connaissance de l'identité de notre ou nos interlocuteurs	- La communication avec des personnes inconnues
- Le fait que les télécommunications faisaient partie intégrante des communications de personne à personne, permettant ainsi de se placer à l'écart pour bénéficier d'une certaine confidentialité	- Le fait que les télécommunications fassent de plus en plus partie de la réalité quotidienne en matière de communication de personne à personne, empêchant ainsi de se placer à l'écart pour bénéficier d'une certaine confidentialité
- L'utilisation d'un ordinateur en prenant des mesures pour préserver une certaine confidentialité dans nos communications quotidiennes	- L'utilisation d'un ordinateur ou d'une nouvelle TI à la vue et au su de tous
Le contexte de l'utilisation de l'informatique d'Internet et des nouvelles TI	
	- La capacité grandissante de stockage en mémoire des ordinateurs
	- L'absence d'oubli ou de pardon qui caractérise les ordinateurs
	- La capacité des ordinateurs d'effectuer des recherches exhaustives dans leur mémoire
	- La capacité des ordinateurs de transférer les données contenues en mémoire
	- La mise en réseau des ordinateurs et l'émergence de l'utilisation des nouvelles TI
Le contexte légal tel que décrit par la Cour suprême américaine	
	- L'utilisateur se place dans autant de contextes particuliers qu'il en existe dans Internet, lorsqu'il communique par le biais de celui-ci
- L'expectative raisonnable de vie rattachée à un contexte donné	- L'expectative raisonnable de vie privée d'un utilisateur sera tributaire de l'expectative raisonnable de vie privée rattachée au contexte dans lequel il s'est placé
- L'utilisation d'un mot de passe et/ou d'un code d'accès pour accéder à un ordinateur	- L'absence d'utilisation de mot de passe et/ou code d'accès pour accéder à un ordinateur
- L'utilisation d'un mot de passe et/ou d'un code d'accès pour se brancher à un réseau	- L'absence d'un mot de passe et/ou d'un code d'accès pour se brancher à un réseau
Le contexte technique	
- L'utilisation de périphériques rapprochés de l'ordinateur et accessibles à un nombre restreint de personne, comme par exemple, dans un bureau à accès restreint par un code	- L'utilisation de périphériques éloignés de l'ordinateur et utilisés par un grand nombre d'utilisateurs dans ces lieux ou locaux ouverts

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>

Facteurs qui accroissent expectative raisonnable de vie privée	Facteurs qui diminue l'expectative raisonnable de vie privée
où une serrure	
- L'utilisation d'un microprocesseur qui ne révélera pas de numéro d'identification	- L'identification du microprocesseur par un numéro d'identification
- L'utilisation de clavier dans un contexte non susceptible de surveillance ou de *monitoring*	- L'utilisation de la surveillance du clavier ou du *keyboard monitoring*
- L'utilisation d'une cage de Faraday ou d'un écran plat à cristaux	- L'utilisation d'un écran émettant des ondes susceptibles d'interception
	- La mise en réseau d'ordinateurs
	- L'architecture de base d'Internet
- L'utilisation de composantes matérielles propres, une infrastructure propre, pour la création d'un réseau de type LAN, MAN, ou WAN	- L'utilisation d'Internet comme base pour la création d'un réseau de type LAN, MAN, ou WAN
- Un nombre limité d'utilisateurs et d'ordinateurs placés en réseau : plus le nombre est bas, plus le réseau est susceptible de générer une expectative raisonnable de vie privée lors de son utilisation	- Un nombre élevé d'utilisateurs et d'ordinateurs placés en réseau : plus le nombre est élevé, moins le réseau est susceptible de générer une expectative raisonnable de vie privée lors de son utilisation
- L'absence d'administrateur de réseau. Il s'agira en pratique de réseaux minuscules ne nécessitant pas ou peu d'entretien	- L'existence de l'administrateur de réseau et de ses employés qui doivent nécessairement procéder à l'entretien, la préservation et à la surveillance du réseau
- L'existence d'une politique en matière de protection des données détenues par l'administrateur de réseau	- L'absence de politique en matière de protection des données détenues par l'administrateur de réseau
- La mise en place et l'utilisation d'un intranet	- La mise en place et l'utilisation d'un extranet
	- Le fonctionnement du protocole TCP/IP et des autres protocoles qu'il supporte
	- L'existence du protocole ICMP gérant les messages d'erreur
	- Le concept d'adresse IP
- L'utilisation d'une adresse IP dynamique	- L'utilisation d'une adresse IP statique
	- Le concept d'adresse Internet d'un appareil ou nom logique
- L'utilisation d'un canal pour transporter de l'information ou établir une communication	- L'utilisation des paquets IP ou Datagramme pour transporter l'information
	- Le concept de numéro de port IP
	- Le fonctionnement des ports de communication TCP/IP
	- L'identification par le domaine et le serveur de nom de domaine

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

Facteurs qui accroissent expectative raisonnable de vie privée	Facteurs qui diminue l'expectative raisonnable de vie privée
- Le contexte technique (suite)	
	- L'approche client-serveur
- La communication synchrone	- La communication asynchrone
Le contexte du branchement	
- Le branchement direct à Internet sans intermédiaire	- L'existence d'un tiers par qui l'information va passer pour se rendre dans Internet
- Le branchement à Internet, en tout ou en partie, à partir d'un lien téléphonique entre l'utilisateur et un fsI, établissant ainsi une communication susceptible d'être reconnue et protégée par la partie VI du *Code criminel*	- Le branchement à Internet à partir d'une technologie non spécifiquement protégée en matière de vie privée par la partie VI du *Code criminel* ou autrement, notamment la connexion bidirectionnelle par satellite
- Le branchement à Internet à partir du domicile de l'utilisateur, impliquant généralement une expectative raisonnable de vie privée élevée	- Le branchement à Internet à partir d'un endroit autre que le domicile de l'utilisateur, tels les lieux du travail, un cybercafé, une école ou de tout autre endroit public
- Le branchement à partir d'un lieu de travail dont l'employeur représente l'État	- Le branchement à partir d'un lieu de travail dont l'employeur constitue une partie privée ou ne représente pas l'État
- Le branchement effectué par le biais d'une technologie ne bénéficiant pas d'une protection statutaire	- Le branchement effectué par le biais d'une technologie bénéficiant déjà d'une expectative raisonnable de vie privée
	- Une politique d'utilisation pour fins de travail seulement
- L'existence d'un lien par modem téléphonique entre l'utilisateur et le fsI	- L'existence d'un lien par modem câble entre l'utilisateur et le fsI
Le contexte territorial partout distribué ou juridictionnel	
	- L'ubiquité inhérente rattachée à l'utilisation d'Internet
	- L'aspect international d'Internet favorisant l'émergence d'une criminalité soulevant des questions relatives à la sécurité nationale
	- L'augmentation de la criminalité informatique transfrontalière favorisant les interventions Étatiques étrangères
Le contexte de l'utilisation du Web	
- L'existence d'une politique en matière de protection des données détenues par un tiers chez qui un utilisateur laissera de l'information lors de son passage	- L'absence de politique en matière de protection des données détenues par un tiers chez qui un utilisateur laissera de l'information lors de son passage

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>

Facteurs qui accroissent expectative raisonnable de vie privée	Facteurs qui diminue l'expectative raisonnable de vie privée
- La navigation sécurisée par l'utilisation d'un serveur mandataire, d'un anonymisateur ou d'un coupe-feu	- La navigation non sécurisée
Le contexte de l'utilisation du Web (suite)	
- L'existence de plusieurs intermédiaires favorisant l'anonymat, entre le client utilisateur et le serveur visité	- La navigation sécurisée par seulement un intermédiaire
- La publication d'une page Web dont l'accès au contenu est restreint à un certain nombre d'usagers	- La publication d'une page Web dont l'accès au contenu est ouvert et accessible à tous
- Le refus des cookies et leur nettoyage des fichiers les contenant	- L'acceptation des cookies
	- L'existence de moteurs de recherche de plus en plus exhaustifs
- La désactivation des divers historiques et le nettoyage de la mémoire cache de l'ordinateur	- Le contenu des divers historiques dans la mémoire cache de l'ordinateur
- Le choix de configuration du logiciel favorisant l'anonymat	- Le choix de configuration du logiciel ne tendant pas à favoriser l'anonymat
Le contexte de l'utilisation du courriel	
- L'utilisation d'un mot de passe et/ou d'un code d'accès pour accéder à une boite de réception de courriel	
- L'existence d'une politique en matière de protection des données détenues par le fsI	- L'absence de politique en matière de protection des données détenues par le fsI
	- Les divers fichiers de journalisation ou *log files* constitués chez les tiers
	- Les limites inhérentes des protocoles SMTP et POP3 révélant l'information au sujet de l'identité des machines qui communiquent
	La technologie favorisant la redistribution du courriel
- L'envoi à un nombre restreint de personne ou communication un vers un	- L'envoi à un nombre de personnes élevé ou communication un vers tous
	- L'utilisation de listserv ou d'une liste de distribution ouverte
	- L'existence d'un archivage des courriels envoyés par le biais de listserv en plus de l'existence de fonctions de recherche
- La protection inhérente du contenu des messages	- Absence de protection inhérente des en-têtes de messages
- Plus on se rapproche du contenu d'un message ou des données s'y rapportant	- Plus on se rapproche des données techniques relatives à l'envoi d'un message
Le contexte de l'utilisation du transfert FTP	

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>

Facteurs qui accroissent expectative raisonnable de vie privée	Facteurs qui diminue l'expectative raisonnable de vie privée
	- Le besoin de proximité des serveurs FTP pour plus de performance
- L'utilisation d'un site FTP privé ou à accès restreint	- L'utilisation d'un site FTP public ou permettant les connexions anonymes
Le contexte de l'utilisation des groupes de discussions ou de nouvelles *Usenet*	
	- L'envoi de message dans un but de publication et d'obtention d'une réponse
- L'impossibilité de savoir exactement à qui le message s'adresse	- La communication à groupe ouvert, même si le sujet discuté paraît de nature privée
	- La publication de coordonnées personnelles tel l'adresse de courriel
	- Le choix de la thématique par un utilisateur, même
	- L'existence d'un modérateur
	- Les en-têtes de groupes *Usenet* qui indiquent la provenance du message
- L'absence d'un système d'archivage avant mars 1995	- La présence d'un système d'archivage des messages *Usenet* depuis mars 1995
- La possibilité d'utiliser une technique cryptographique simple, permettant de déjouer les moteurs de recherche	- La présence d'un système de recherche ou moteur de recherche
Le contexte de la session en mode *Telnet*	
- La session effectuée sur un serveur de nature privée	- La session effectuée sur un serveur de nature publique -
	- L'utilisation du port de communication numéro 23 qui annonce une communication de type *Telnet*
Le contexte du bavardage-clavier ou clavardage du service IRC	
	- La nature même du service qui favorise l'échange de confidences et d'informations personnelles entre plusieurs personnes
	- L'identification de l'emplacement géographique du serveur utilisé, entraînant du coup une inférence de proximité de l'utilisateur de la ressource
	- La possibilité de connaître la version du logiciel utilisé par un autre utilisateur
	- La possibilité de confirmer la présence de nos amis dans IRC
- L'ouverture d'une fenêtre confidentielle	- L'ouverture d'une fenêtre confidentielle (*a contrario*),
	- La possibilité d'obtenir de l'information sur

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>

Facteurs qui accroissent expectative raisonnable de vie privée	Facteurs qui diminue l'expectative raisonnable de vie privée
	les personnes correspondant à un pseudonyme
- La possibilité d'établir une communication un à un sans recourir au réseau IRC	- Les discussions souvent intimes avec un interlocuteur à distance que l'on connaît peu ou pas
Le contexte de l'utilisation de la téléphonie et de la vidéoconférence Internet	
	- La publication du nom, de l'adresse et de l'adresse IP correspondante dans un annuaire qui constitue un équivalent d'un immense carnet d'adresse public ou bottin téléphonique
	- La fonction d'enregistrement automatique des coordonnées de notre interlocuteur
Le contexte de l'utilisation de la téléphonie et de la vidéoconférence Internet (suite)	
	- La présence de notre interlocuteur à l'écran
- La communication synchrone	
- L'ignorance qu'Internet sera utilisé lors de la communication	- La connaissance qu'Internet sera utilisé lors de la communication
- L'utilisation d'un combiné téléphonique utilisant en partie Internet pour établir la communication vers une autre personne utilisant un combiné téléphonique	- Les limites inhérentes au protocole IP lors de l'utilisation d'Internet pour procéder à la transmission de la communication
- Le mode de communication un vers un	
Le contexte de la messagerie instantanée	
	- La fonction d'avertissement de présence dans le réseau aux autres utilisateurs
- L'avertissement donné à un nombre restreint d'utilisateurs	- L'avertissement donné à un nombre élevé d'utilisateurs
- La nécessité qu'ont es utilisateurs de se chercher entre eux, contrairement à l'adhésion à des groupes de discussion	- La discussion à distance avec d'autres utilisateurs
	- L'apparition de l'adresse IP de notre interlocuteur lors d'une communication
- La fonction permettant de cacher l'adresse IP à notre interlocuteur	- La possibilité d'utiliser la fonction *netstat*, permettant de connaître quand même l'adresse IP
- La possibilité d'utiliser la communication synchrone	- La possibilité d'utiliser la communication asynchrone
Le contexte de l'utilisation de la cryptographie, de la stéganographie et des techniques favorisant l'anonymat	
- La transmission chiffrée et/ou cachée par la cryptographie et/ou stéganographie	- La transmission de données en clair dans un réseau qui, à sa face même, ne semble pas favoriser les communications privées

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>

Facteurs qui accroissent expectative raisonnable de vie privée	Facteurs qui diminue l'expectative raisonnable de vie privée
- La transmission de données par un canal chiffré	- La transmission de données par le biais d'un canal non sécurisé
- La cryptographie forte	- La cryptographie faible
- L'absence de tiers certificateur	- La présence de tiers certificateur, susceptible de révéler l'information relative à l'émission de certains types de clés
- Le tiers certificateur reconnu comme une personne ou un organisme de confiance	- Le tiers certificateur reconnu comme une personne ou un organisme de confiance
- L'absence d'infrastructure à clé publique	- L'utilisation d'une infrastructure à clé publique
- L'utilisation d'un serveur anonymisateur pour communiquer dans Internet	- L'utilisation d'un fsI ordinaire pour communiquer dans Internet
- L'interdiction d'enregistrer subrepticement, par le biais de la surveillance participative, les communications effectuées dans Internet (approche selon une norme plus générale, du juge La Forest dans *Duarte* et *Wong*)	- La permission d'enregistrer subrepticement, par le biais de la surveillance participative, les communications effectuées dans Internet (approche selon l'ensemble des circonstances, favorisée dans *Edwards*, *Morin* et *Belnavis*)

Les facteurs que nous venons d'énumérer constituent, à notre avis, un échantillon significatif de critères dont ont devra désormais tenir compte lors de la détermination de l'expectative raisonnable de vie privée dans le contexte d'Internet et des nouvelles TI. Il convient maintenant de conclure la présente étude.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

CONCLUSION

Le but de la présente étude était de déterminer les principaux contextes de communication dans Internet, afin d'être en mesure de déterminer dans chaque cas, le niveau d'expectative raisonnable de vie privée susceptible d'application.

Nous estimons avoir démontré qu'Internet, par ses multiples contextes généraux et particuliers, ne constitue pas en soi un contexte factuel donné, mais plutôt un ensemble de contextes, susceptibles d'influer sur le niveau d'expectative raisonnable de vie privée.

Avec le temps, la position de la Cour suprême du Canada a évolué sur la manière d'évaluer l'existence d'une expectative raisonnable de vie privée. De l'approche de principe, fondée sur une norme plus générale, la Cour est passée à l'approche pragmatique ou au cas par cas. La première approche semble plus sensible à des considérations générales ou philosophiques en matière de protection du droit à la vie privée. Les concepts de sphères d'intimité et d'intelligence collective sont, à notre avis, plus susceptibles d'être retenus par cette approche. La deuxième approche semble plus sensible aux contextes factuels précis. Elle sera donc tributaire de la nature de la technologie et de son évolution.

Même lorsqu'une expectative raisonnable de vie privée est reconnue dans un contexte donné, celle-ci est susceptible de modulation. Elle sera soit « complète » ou « réduite ». Il faudra donc se demander dans chaque cas, dans quelle mesure on bénéficiera d'une expectative raisonnable de vie privée. Finalement, l'immixtion dans l'expectative raisonnable de vie privée devra avoir été effectuée de façon raisonnable. L'ampleur de l'immixtion sera souvent tributaire de la nature de la technologie utilisée. La reconnaissance de l'expectative raisonnable de vie privée n'est donc pas l'étape ultime.

Le droit relatif à l'expectative raisonnable de vie privée a évolué depuis 1982; les contextes factuels apportés par Internet et les nouvelles TI évoluent rapidement depuis 1995 et, même lorsque l'expectative raisonnable de vie privée est reconnue, celle-ci est susceptible d'application « restreinte » ou « complète ».

Malgré certaines certitudes qui ressortent de la présente étude, notamment quant à l'identification des facteurs susceptibles de moduler le niveau d'expectative raisonnable de vie privée, il n'en demeure pas moins que, placées dans le contexte décrit au présent paragraphe, celles-ci sont à accepter avec les *caveat* qui s'imposent. L'expectative raisonnable de vie privée dans Internet est donc, en quelque sorte, condamnée à varier sans cesse.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

BIBLIOGRAPHIE

– Législation, réglementation et projet de loi (canadiens)

Charte canadienne des droits et libertés, partie I de la *Loi Constitutionnelle de 1982*, constituant l'annexe B de la *Loi de 1982 sur le Canada* (R.-U.), 1982, c.11, en ligne : Ministère de la justice <http://lois.justice.gc.ca/fr/charte/index.html> (date d'accès : 30 août 2001).

Code civil du Québec, L.Q. 1991, c. 64, en ligne : Les publications du Québec <http://publicationsduquebec.gouv.qc.ca/fr/cgi/frameset.cgi?url=/documents/lr/CCQ/CCQ_1.html> (date d'accès : 30 août 2001).

Code criminel, L.R.C. 1985, c. C-46, en ligne : Ministère de la justice <http://lois.justice.gc.ca/fr/C-46/index.html> (date d'accès : 30 août 2001).

Loi d'interprétation, L.R.C. 1985, c. I-21, en ligne: Ministère de la justice <http://lois.justice.gc.ca/fr/I-21/texte.html> (date d'accès : 30 août 2001).

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, c. 40.

Loi sur la protection des renseignements personnels dans le secteur privé, L.R.Q. c. P-39.1, en ligne : Les publications du Québec <http://publicationsduquebec.gouv.qc.ca/fr/cgi/frameset.cgi?url=/documents/lr/P_39_1/P39_1.html> (date d'accès 30 août 2001).

Loi sur la protection des renseignements personnels et les documents électroniques, L.R.C. 1985, c. P-8.6, en ligne : Ministère de la justice <http://lois.justice.gc.ca/fr/P-8.6/74408.html> (date d'accès : 30 août 2001).

Loi sur la radiocommunication L.R.C. 1985, c. R-2, en ligne : Ministère de la justice <http://lois.justice.gc.ca/fr/R-2/texte.html> (date d'accès : 30 août 2001).

Loi sur la société canadienne des postes, L.R.C. (1985), c. C-10, en ligne : Ministère de la justice <http://lois.justice.gc.ca/fr/C-10/81511.html> (date d'accès : 30 avril 2001).

Loi sur le droit d'auteur L.R.C. 1985, c. C-42, en ligne : Ministère de la justice <http://lois.justice.gc.ca/fr/C-42/texte.html> (date d'accès : 30 août 2001).

Loi sur l'entraide juridique en matière criminelle L.R.C. 1985 (4e Supp.), c. M-13.6, en ligne : Ministère de la justice <http://lois.justice.gc.ca/fr/M-13.6/31941.html> (date d'accès : 30 août 2001).

Loi sur les douanes, L.C. 1986 (2e Supp.), c. 1, en ligne : Ministère de la justice <http://lois.justice.gc.ca/fr/C-52.6/29004.html> (date d'accès : 30 avril 2001).

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

Loi sur le Service canadien du renseignement de sécurité L.R.C. 1985, c. C-23, en ligne : Ministère de la justice <http://lois.justice.gc.ca/fr/c-23/texte.html> (date d'accès : 30 août 2001).

Loi sur le service correctionnel et la mise en liberté sous condition, L.C. 1992, c. 20, en ligne : Ministère de la justice <http://lois.justice.gc.ca/fr/C-44.6/88250.html> (date d'accès : 30 avril 2001).

Loi sur les infractions en matière de sécurité, L.R.C. 1985, c. S-7, en ligne : Ministère de la justice <http://lois.justice.gc.ca/fr/S-7/47206.html> (date d'accès : 30 août 2001).

P.L. C-36, *Loi antiterroriste*, 1ère sess., 37e, 2001, en ligne : Parlement du Canada <http://www.parl.gc.ca/common/Bills_House_Government.asp?Language=F&Parl=37&Ses=1#C-36> (date d'accès : 12 novembre 2001).

Règlement sur le système carcéral et la mise en liberté sous condition, D.O.R.S./92-620, en ligne : Ministère de la justice <http://lois.justice.gc.ca/fr/C-44.6/DORS-92-620/texte.html> (date d'accès : 20 avril 2001).

Traité d'entraide juridique en matière pénale entre le gouvernement du Canada et le gouvernement des États-Unis d'Amérique, 18 mars 1985, R.T. Can. 1990/19 (entrée en vigueur : 24 janvier 1990), en ligne : Lexum < http://www2.lexum.umontreal.ca/ca_us/fr/CTS.1990.19.fr.cfm> (date d'accès : 13 septembre 2001).

– **Conventions (internationales)**

Convention des Nations Unies contre le trafic illicite des stupéfiants et des substances psychotropes, 20 décembre 1988, R.T.N.U. (entrée en vigueur : 11 novembre 1990), en ligne : Traités multilatéraux déposés auprès du secrétaire général des Nations Unies <http://untreaty.un.org/FRENCH/bible/frenchinternetbible/partI/chapterVI/treaty22.asp> (date d'accès : 13 septembre 2001).

Convention sur la cybercriminalité, 23 novembre 2001, S.T.E. 185 (ouvert pour signature : 23 novembre 2001), en ligne : Conseil de l'Europe <http://conventions.coe.int/Treaty/fr/Treaties/Html/185.htm> (date d'accès : 24 novembre 2001).

– **Législation et projet de loi (américains)**

Bill of Rights (1791), en ligne : FindLaw <http://guide.lp.findlaw.com/casecode/constitution/> (date d'accès : 13 *septembre* 2001).

Communication Decency Act, constitue le Titre V du *Telecommunications Act of 1996* (Pub. L. 104-104, 110 Stat.56).

USA Patriot Act of 2001, Bill H.R. 3162, 107th Cong. (2001), en ligne : *FindLaw* <http://news.findLaw.com/cnn/docs/terrorism/hr3162.pdf> (date d'accès : 12 novembre 2001).

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

– **Jurisprudence (canadiennes)**

Atwal c. Canada, [1988] 1 C.F. 107.

Baron c. Canada, [1993] 1 R.C.S. 416, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1993/vol1/html/1993rcs1_0416.html> (date d'accès : 30 août 2001).

Canadian Civil Liberty Assn. c. Canada (Attorney General) (1998), 126 C.C.C. (3d) 257, permission d'en appeler à la Cour suprême du Canada refusée 131 C.C.C. (3d) vi.

C*omité paritaire c. Potash*, [1994] 2 R.C.S. 406, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1994/vol2/html/1994rcs2_0406.html> (date d'accès : 30 août 2001).

Gagnon c. Deslauriers (1997), 141 F.T.R. 163 (Fed T.D.).

Godbout c. Ville de Longueuil, [1997] 3 R.C.S. 844, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1997/vol3/html/1997rcs3_0844.html> (date d'accès : 30 août 2001).

Hunter c. Southam, [1984] 2 R.C.S. 145, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scs/fr/publies/1984/vol2/html/1984rcs2_0145.html> (date d'accès : 30 août 2001).

Jamieson c. United States of America et al.,(1992) 73 C.C.C. (3d) 460.

M. (A.) c. Ryan, [1997] 1 R.C.S. 157, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1997/vol1/html/1997rcs1_0157.html> (date d'accès : 30 août 2001).

Michaud c. Québec (Procureur Général), [1996] 3 R.C.S. 3, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1996/vol3/html/1996rcs3_0003.html> (date d'accès : 30 août 2001).

Mills c. La Reine, [1986] 1 R.C.S. 863, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1986/vol1/html/1986rcs1_0863.html> (date d'accès : 30 août 2001).

R. c. Araujo, [2000] 2 R.C.S. 992, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/2000/vol2/html/2000rcs2_0992.html> (date d'accès : 30 août 2001).

R. c. Bartle, [1994] 3 R.C.S. 173, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1994/vol3/html/1994rcs3_0173.html> (date d'accès : 30 août 2001).

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

R. c. Beare, [1988] 2 R.C.S. 386, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scs/fr/publies/1988/vol2/html/1988rcs2_0386.html> (date d'accès : 30 août 2001).

R. c. Belnavis, [1997] 3 R.C.S. 341, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1997/vol3/html/1997rcs3_0341.html> (date d'accès : 30 août 2001).

R. c Blizzard, [2001] N.B.J. no. 18.

R. c. Boersma, [1994] 2 R.C.S. 488, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1994/vol2/html/1994rcs2_0488.html> (date d'accès : 30 août 2001).

R. c. Borden, [1994] 3 R.C.S. 145, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1994/vol3/html/1994rcs3_0145.html> (date d'accès : 30 août 2001).

R c. Bourque, (1995) 103 C.C.C. (3d) 559 (C.A.Qc.).

R. c. Carothers, [1978] 6 W.W.R. 571 (Co Ct. C.-B.).

R. c. Cheung and Tam (1995), 100 C.C.C. (3d) 441 (C.S. C.-B.).

R. c. CIP Inc., [1992] 1 R.C.S. 843, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1992/vol1/html/1992rcs1_0843.html> (date d'accès : 30 août 2001).

R. c. Clarkson, [1986] 1 R.C.S. 383, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scs/fr/publies/1986/vol1/html/1986rcs1_0383.html> (date d'accès : 30 août 2001).

R. c. Colarusso, [1994] 1 R.C.S. 20, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1994/vol1/html/1994rcs1_0020.html> (Date d'accès : 30 août 2001).

R. c. Collins, [1987] 1 R.C.S. 265, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scs/fr/publies/1987/vol1/html/1987rcs1_0265.html> (date d'accès : 30 août 2001).

R. c. Cook, [1998] 2 R.C.S. 597, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1998/vol2/html/1998rcs2_0597.html> (date d'accès : 30 août 2001).

R. c. Dersch, [1993] 3 R.C.S. 768, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1993/vol3/html/1993rcs3_0768.html> (date d'accès : 30 août 2001).

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

R. c. Duarte, [1990] 1 R.C.S. 30, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1990/vol1/html/1990rcs1_0030.html> (date d'accès : 30 août 2001).

R. c. Dyment, [1988] 2 R.C.S. 417, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1988/vol2/html/1988rcs2_0417.html> (date d'accès : 30 août 2001).

R. c Edwards, [1996] 1 R.C.S.128, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1996/vol1/html/1996rcs1_0128.html> (date d'accès : 30 août 2001).

R. c. Elzein, [1993] R.J.Q. 2563 (C.A.Qc.); (1993) 82 C.C.C. (3d) 455 (version traduite en anglais); requête en autorisation de pourvoi rejetée [1993] 4 R.C.S. v.

R. c. Erickson, [1993] 2 R.C.S. 649, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1993/vol2/html/1993rcs2_0649.html> (date d'accès : 30 août 2001).

R. c. Evans, [1996] 1 R.C.S. 8, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1996/vol1/html/1996rcs1_0008.html> (date d'accès : 30 août 2001).

R. c. Feagan, (1993) 80 C.C.C. (3d) 356.

R.. c. Feeney,[1997] 2 R.C.S. 117, en ligne : Lexum (Cour suprême du Canada) < http://www.lexum.umontreal.ca/csc-scc/fr/pub/1997/vol2/html/1997rcs2_0013.html> (date d'accès : 30 août 2001).

R. c. Gauthier, REJB 99-14108.

R. c. Genest, [1989] 1 R.C.S. 59, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1989/vol1/html/1989rcs1_0059.html> (date d'accès : 30 août 2001).

R. v. Goldman, [1980] 1 R.C.S. 976.

R. c. Goodleaf, [1997] A.Q. No 2665 (C.A.Qc.).

R. c. Grant, [1993] 3 R.C.S. 223, 242, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1993/vol3/html/1993rcs3_0223.html> (date d'accès : 30 août 2001).

R. c. Greffe, [1990] 1 R.C.S. 755, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1990/vol1/html/1990rcs1_0755.html> (date d'accès : 30 août 2001).

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>

Juriscom.net
droit des technologies de l'information

R. c. Hufsky, [1988] 1 R.C.S. 621, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1988/vol1/html/1988rcs1_0621.html> (date d'accès : 30 août 2001).

R. c. Hutchings (1996), 111 C.C.C. (3d) 215 (C.A.C-.B.).

R. c. Joyal (1996), 43 C.R. (4th) 317 (C.A.Qc.).

R. c. Kokesch, [1990] 3 R.C.S. 3, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1990/vol3/html/1990rcs3_0003.html> (date d'accès : 30 août 2001).

R. c. Krist (1995), 100 C.C.C. (3d) 58 (C.A.C.-B.).

R. c. Ladouceur, [1990] 1 R.C.S. 1257, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1990/vol1/html/1990rcs1_1257.html> (date d'accès : 30 août 2001).

R. c. Lauda, [1998]2 R.C.S. 683, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1998/vol2/html/1998rcs2_0683.html> (date d'accès : 30 août 2001).

R. v. Laurin (1997), 113 C.C.C. (3d) 519 (Ont. C.A.).

R v. Lebeau and Lofthouse, (Non rapporté) C.A. Ont. (nos. 337/86, 403/86) 22 janvier 1988.

R. c. Lillico (1994), 92 C.C.C. (3d) 90, 95 (C.O.D.G.).

R. c. Lubovac (1989), 52 C.C.C. (3d) 551 (C.A. Alta.); requête en autorisation de pourvoi rejetée 53 C.C.C. (3d) vii.

R c. Macooh, [1993] 2 R.C.S. 802, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1993/vol2/html/1993rcs2_0802.html> (date d'accès : 30 août 2001).

R. c. McLaughlin, [1980] 2 R.C.S. 331.

R. c. McKinlay Transport Ltd., [1990] 1 R.C.S. 627, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1990/vol1/html/1990rcs1_0627.html> (date d'accès : 30 août 2001).

R v. Mc Queen (1975), 25 C.C.C. (2d) 262 (C.A. Alta.).

R. c. Mellenthin, [1992] 3 R.C.S. 615, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1992/vol3/html/1992rcs3_0615.html> (date d'accès : 30 août 2001).

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

R. c. Mills, [1999] 3 R.C.S. 668, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1999/vol3/html/1999rcs3_0668.html> (date d'accès : 30 août 2001).

R. c M. (M.R.), [1998] 3 R.C.S. 393, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1998/vol3/html/1998rcs3_0393.html> (date d'accès : 30 août 2001).

R. c. Monney, [1999] 1 R.C.S. 652, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1999/vol1/html/1999rcs1_0652.html> (date d'accès : 30 août 2001).

R. c. Morales 16 C.R. (4th) 88.

R. c. Morgentaler (No2), [1988] 1 R.C.S. 30, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1988/vol1/html/1988rcs1_0030.html> (date d'accès : 30 août 2001).

R. c. Morin, [1996] R.J.Q. 1758 (C.Q.).

R. c. Neill (1993), 54 W.A.C. 118 (C.A.C.-B.).

R. c. Nikolovski, [1996] 3 R.C.S. 1197, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1996/vol3/html/1996rcs3_1197.html> (date d'accès : 30 août 2001).

R. v. O'Connor, [1995] 4 R.C.S. 411, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1995/vol4/html/1995rcs4_0411.html> (date d'accès : 30 août 2001).

R. c. Paolitto,(1994) 91 C.C.C. (3d) 75.

R. c. Plant, [1993] 3 R.C.S. 281, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1993/vol3/html/1993rcs3_0281.html> (date d'accès : 30 août 2001).

R. c. Pohoretsky, [1987] 1 R.C.S. 945, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1987/vol1/html/1987rcs1_0945.html> (date d'accès : 30 août 2001).

R. c. Richer (1993), 82 C.C.C. (3d) 385.

R. c. Robillard, [1996] R.J.Q. 2886 (C.A.Qc.).

R. c. Rodney (1984), 12 C.C.C. (3d) 195.

R. c. Shergill (1997), 23 O.T.C. 290 (Div. Gen.).

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>

Juriscom.net droit des technologies de l'information

R. c. Silveira, [1995] 2 R.C.S. 297, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1995/vol2/html/1995rcs2_0297.html> (date d'accès : 30 août 2001).

R. c. Simmons, [1988] 2 R.C.S. 495, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1988/vol2/html/1988rcs2_0495.html> (date d'accès : 30 août 2001).

R. c. Singh (1998), 127 C.C.C. (3d) 429.

R. c. Solomon [1992] R.J.Q. 2631 (C.M. Mtl.).

R. c. Solomon [1996] R.J.Q. 1789 (C.A.Q.), confirmé par la Cour suprême à: [1997] 3 R.C.S. 696.

R. c. Stillman, [1997] 1 R.C.S. 607, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1997/vol1/html/1997rcs1_0607.html> (date d'accès : 30 août 2001).

R. c. Stewart, [1988] 1 R.C.S. 963, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1988/vol1/html/1988rcs1_0963.html> (date d'accès : 30 août 2001).

R. c. Tardif, REJB 98-10965 (C.Q.).

R. c. Thompson, [1990] 2 R.C.S. 1111, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1990/vol2/html/1990rcs2_1111.html> (date d'accès : 30 août 2001). (date d'accès : 30 août 2001).

R. c. Tremblay (29 mars 2001), Trois-Rivières 410-01-019056-001, (C.Q.), pourvoi de plein droit à la C.A. (29 juin 2001).

R. c. Weir [1998] A.J. No 155, conf. en partie par 2001 ABCA 181, en ligne : CanLII (Cour d'appel de l'Alberta) <http://www.canlii.org/ab/cas/abca/2001/2001abca181.html> (date d'accès : 30 août 2001).

R. c. Wijesinha, [1995] 3 R.C.S. 422, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1995/vol3/html/1995rcs3_0422.html> (date d'accès : 30 août 2001).

R. c. Wise, [1992] 1 R.C.S. 527, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1992/vol1/html/1992rcs1_0527.html> (date d'accès : 30 août 2001).

R. c. Wong, [1990] 3 R.C.S. 36, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1990/vol3/html/1990rcs3_0036.html> (date d'accès : 30 août 2001).

Re Copeland and Adamson et al. [1972] 3 O.R. 248 (Ont. H.C.).

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>

Re Postes Canada. et Canada (P.G.) (1995), 95 C.C.C. (3d) 568.

Rodriguez c. Colombie-Britannique (Procureur Général), [1993] 3 R.C.S. 519, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1993/vol3/html/1993rcs3_0519.html> (date d'accès : 30 août 2001).

Schreiber c. Canada (Procureur général), [1998] 1 R.C.S. 841, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1998/vol1/html/1998rcs1_0841.html> (date d'accès : 30 août 2001).

Société Radio-Canada c. Lessard, [1991] 3 R.C.S. 421, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1991/vol3/html/1991rcs3_0421.html> (date d'accès : 30 août 2001).

Thomson Newspapers Ltd. c. Canada (Directeur des enquêtes et recherches, Commission sur les pratiques restrictives en matière de commerce), [1990] 1 R.C.S. 425, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1990/vol1/html/1990rcs1_0425.html> (date d'accès : 30 août 2001).

Weatherall c. Procureur Général du Canada, [1993] 2 R.C.S. 872, en ligne : Lexum (Cour suprême du Canada) <http://www.lexum.umontreal.ca/csc-scc/fr/pub/1993/vol2/html/1993rcs2_0872.html> (date d'accès : 30 août 2001).

– **Jurisprudence (américaine)**

ACLU c. Reno, 929 F.Supp. 824 (E.D.Pa. 1996).

Bernstein c. United State Dept. Of Justice, No. 97-16686 (9th Cir. 05/06/1999).

Bohach c. City of Reno, 932 F. Supp 1232 (D. Nev. 1996).

Davis c. Gracey, 111 F.3d 1472 (Cir., 1997).

Ex Parte Jackson, 96 US 727 (1878).

Katz c. United States, 389 U.S. 347 (1967).

McKammey c. Roach, 55 F.3d 1236 (6th Cir. 1993).

Olmstead c. United States, 277 U.S. 438 (1928).

Reno c. ACLU, 521 U.S. 844 (1997), aussi disponible à : http://www.aclu.org/court/renovaclu.html (consulté le 31 juillet 1998).

Restuccia c. Burk Technology Inc., 5 Mass. L. Reptr. No 31,712 (1996).

Shoars c. Epson America, No S.W.C. 112749 (Cal. Super C.T. 1990).

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

Smyth c. Pillsbury Company, 914 F. Supp. 97 (E.D.Pa. 1996).

Steve Jackson Games, Inc. c. United States Secret Services 36 F.3d 457 (5th Cir. 1994).

United States c. Chan, 830 F. Supp. 531 (N.D.Cal. 1993).

United States c. Charbonneau, 979 F. Supp. 1177 (S.D. Ohio 1997).

United States c. Hambrick No. 99-4793 (4th Cir. 08/03/2000).

United States c. Maxwell, 42 M.J. 568 (Air Force Crim. App.1995).

United States c. Maxwell, 45 M.J. 406 (Air Force Crim. App.1996).

United States.c. Moriarty, 962 F. Supp. 217, (D.Mass. 1997).

United States c Miller, 425 U.S. 435 (1976).

United States c. Reyes, 922 F. Supp. 818 (S.D.N.Y. 1996).

United States c. Simons, No. 99-4238 (4th Cir. 02/28/2000).

United States c. White, No. 00-2318 (10th Cir. 03/27/2001).

Wesley College c. Pitts, 974 F. Supp. 375, 384-390 (D. Del. 1997).

– **Doctrine (monographies canadiennes)**

Béliveau, P. et Vauclair, M., *Principes de preuve et de procédure pénales,* 5e éd., Montréal, Thémis, 1998.

Benyekhlef, K., *La protection de la vie privée dans les échanges internationaux d'information*, Montréal, Thémis, 1992.

Côté, R. et Laperrière, R., dir., *Vie privée sous surveillance :la protection des renseignements privés en droit québécois et comparé*, Cowansville (Qc.), Yvon Blais,1994.

Davis, R. W.K. et Hutchison, S. C., Computer Crime in Canada, Toronto, Carswell, 1997.

Ewaschuk, E. G., *Criminal Pleadings and Practice in Canada*, 2d ed., Aurora, (Ont.), Canada Law Books, 1997.

Fontana, J. A., *The Law of Search and Seizure in Canada Fourth Edition*, Toronto,Butterworths, 1997.

Gahtan, A. M., *Electronic Evidence*, Scarborough (Ont.), Carswell, 1999.

Gathan, A. M., Kratz, Martin P.J.et Mann, J. Fraser, *Internet Law*, Scarborough (Ont.), Carswell, 1998.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>

Hubbard, R. W. *et al*., *Wiretapping and Other Electronic Surveillance Law and Procedure*, feuilles mobiles, Aurora (Ont.), Canada Law Book, 2001.

Johnston, D., Handa, S., et Morgan, C., *Cyber Law*, Toronto, Stoddart, 1997.

McIsaac, B., Shields, R. et Klein, K., *The Law of privacy in Canada*, Scarborough (Ont), Carswell, 2000.

Michaud, M., *Le droit au respect de la vie privée dans le contexte médiatique : de Warren Brandeis à l'Inforoute*, Cowansville (Qc.), Yvon Blais, 1996.

Nadeau, A.-R., *Vie privé et droits fondamentaux*, Cowansville (Qc.), Yvon Blais, 2000.

Parisien, S. et Trudel, P., *L'identification et la certification dans le commerce électronique*, Cowansville (Qc.), Yvon Blais, 1996.

Sookman, B., *Computer, Internet and Electronic Commerce Law*, Scarborough (Ont.), Carswell, 2000.

Takach, G. S., *Computer Law*, Toronto, Irwin Law, 1998.

Trudel, P. *et al*., *Droit du cyberespace*, Montréal, Thémis, Centre de recherche en droit public, Faculté de droit, 1997.

– **Doctrine (monographies américaines et françaises)**

Adam, N. R. et *al*., *Electronic Commerce : Technical, Business, and Legal Issues*, Upper Saddle River (NJ), Prentice Hall PTR, 1999.

Agre, P. E. et Rotenberg, M., dir., *Technology and Privacy* : *The New Landscape*, Cambridge, MIT Press, 1998, 125.

De Maillard, J., *Un monde sans loi*, Paris, Stock, 1998.

Godwin, M., *Cyber Rights*, New-York, Times Books, 1998.

Grabosky, P. N. et Smith, R. G., *Crime in the Digital Age*, New Brunswick (NJ), Transaction Publishers, 1998.

Hérail, J.-L. et Ramael, P., *Blanchiment d'argent et crime organisé*, Paris, Presses Universitaires de France, 1996.

Lawson, J., *The Complete Internet Handbook for Lawyers*, Chicago, American Bar Association, 1999.

Richards, J. R., *Transnational Criminal organizations, Cybercrime, and Money Laundering*, New-York, CRC Press, 1999.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>

Juriscom.net
droit des technologies de l'information

Rosé, P., *La criminalité informatique,* Paris, Presses Universitaires de France, coll. « Que sais-je? », 1995.

– **Doctrine (articles canadiens)**

Basque, G., « Introduction à l'Internet » dans Poulin, Daniel, *et al*. dir.*, Les autoroutes électroniques, usages, droits et promesses*, Actes du colloque, Cowansville (Qc.), Yvon Blais, 1995, 9.

Benyekhlef, K., « Les dimensions constitutionnelles du droit à la vie privée » dans Trudel, Pierre, dir., *Droit du public à l'information et vie privée : deux droits irréconciliable?*, Montréal, Thémis, 1992, 17.

Boisvert, A.-M., « Communicatique et responsabilité pénale : criminalité informatique et « vol » d'information », dans Beauchard, Jean *et al.*, *Le droit de la communicatique, Actes du colloque conjoint des Facultés de droit de l'Université de Poitiers et de l'Université de Montréal*, Montréal, Thémis, 1990, 93.

Campbell, G. S., *Emerging Issues of the internet and the Canadian Criminal Law*, 3 (1998) Can. Crim. L.R. 101.

Chasse, K., « Surreptious video and computer surveillance : Warrantless SVS and SCS », (1987) 4 C.C.L.R. 95.

Chasse, K., « Surreptious video and computer surveillance : Warrantless SVS and SCS (part two) », (1987) 4 C.C.L.R. 129.

Cournoyer, G. et Paradis, Y., « La Charte canadienne : la procédure », dans Claude Leblond, dir., *Collection de droit 2000-2001 Droit Pénal (procédure et preuve)*, vol. 10, Cowansville (Qc.), Yvon Blais, 2001, à la p. 191.

Cournoyer, G. et Paradis, Y., « La Charte canadienne : les droits protégés, principes de base », dans Claude Leblond, dir., *Collection de droit 2000-2001 Droit Pénal (procédure et preuve)*, vol. 10, Cowansville (Qc.), Yvon Blais, 2001, à la p. 205.

Laperrière, R., « The 'Quebec Model' of Data Protection : A Compromise Between *Laissez-faire* and Public Control in a Technological Era » dans Colin J. Bennett et Rebecca Grant, dir., V*isions of Privacy. Policy Choices for the Digital Age*, Toronto, University of Toronto Press, 1999, 182.

Larochelle, J., « Le droit à a vie privée et la Charte canadienne des droits et libertés » dans *Développements récents en droit criminel (1990)*, Cowansville (Qc.), Yvon Blais, 1990, 117.

Scott, D.J.E., « Interception of a Hacker's Computer Communication » (1993) 25 Ottawa L. Rev. 525.

Trudel, P. et Gérin-Lajoie, R., « La protection des droits et des valeurs dans la gestion des réseaux ouverts » dans Poulin, Daniel, *et al*. dir.*, Les autoroutes électroniques, usages, droits et promesses*, Actes du colloque, Cowansville (Qc.), Yvon Blais, 1995, 279.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

Veilleux, D., « Le droit à la vie privée-sa portée face à la surveillance de l'employeur » (2000) 60 R. du B. 1.

– **Doctrine (articles américains)**

Adler, M., « *Cyberspace, General Searches and Digital Contraband : The Fourth Amendment and the Net-Wide Search* » (1996) 105 Yale L.J.1093.

Connor B., M., « Home Is Where Your Modem Is : An Appropriate Application of Search and Seizure Law to Electronic Mail » 34 (1996) Am. Crim. L. Rev. 163.

Denning, D. E., « Digital Communication Must Not Weaken Law Enforcement » dans M. David Ermann, *et al*. dir., *Computer, Ethics and Society*, New York, Oxford University Press, 1997, 247.

Denning, D. E. et Baugh, Jr., W. E., « Hiding Crimes in Cyberspace », (1999) 2 *Information, Communication and Society*, 251, en ligne : Dorothy Denning's Home Page <http://www.cs.georgetown.edu/~denning/crypto/hiding1.doc> (date d'accès : 10 juillet 2001).

Dierks, M. P., « Computer Network Abuse », (1993) 6 Harv. J.L. & Tech. 307.

Downes, L., « Electronic Communication and the Plain View Exception : "Bad Physics" » (1994) 7 Harv. J.L. & Tech 239.

Fromkin, M. A., *Anonimity and its Enmities*, 1995 J. ONLINE L. art. 4, en ligne : <http://warthog.cc.wm.edu/law/publications/jol/froomkin/.html> (date d'accès :21 avril 1999).

Gerhart, P. F., « Emplyee Privacy Rights in the United States » 17 (1995) Comp. Lab. L.J. 175.

Goodman, M. D., « Why the Police Don't Care About Computer Crime? » 10 (1997) Harv. J.L. & Tech 466.

Jackson, D. W., « Protection of Privacy In The Search And Seizure Of E-Mail : Is the United States Doomed to an Orwellian Future? » 17 (1999) TEMP. ENVTL. L.& TECH. J. 97.

Lessig, L., « Reading the Constitution in Cyberspace » 45 (1996) Emory L.J. 869.

Natt Grantt, II, Larry O., « An Affront to Human Dignity : Electronic Mail Monitoring in the Workplace » 8 (1995) Harv. J.L. & Tech 345.

Note, « Keeping Secrets in Cyberspace : Establishing Fourth Amendment Protection for Internet Communication, 110 (1997) Harv. L. Rev. 1591.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

Phillips, D. J., « Cryptography, Secrets, and the Structuring of Trust » dans Philip E. Agre et Marc Rotenberg dir., *Technology and Privacy* : *The New Landscape*, Cambridge, MIT Press, 1998, 243.

Rotenberg, M., « Wiretap Laws Must Not Weaken Digital Communications » dans M. David Ermann, *et al*. dir., *Computer, Ethics and Society*, New York, Oxford University Press, 1997, 263.

Rule, J. B., « High-Tech Workplace Surveillance : What's Really New? » dans David Lyon et Elia Zureik, dir., *Computers, Surveillance & Privacy*, Minneapolis, University of Minnesota Press, 1996, 66.

Sergent, R. S. « A Fourth Amendment Model for Computer Networks and Data Privacy » 81 (1995) Va. L. Rev. 1181.

Slobogin, C. et Schumacher, J., *Reasonable Expectation of Privacy and Autonomy in Fourth Amendment Cases : An Empirical Look at Understandings Recognized and Permitted by Society* (1993) Duke L.J. 727.

Sundstrom, S. A. « You've Got Mail! (And the Government Knows It) : Applying the Fourth Amendment to Workplace E-mail Monitoring » 72 (1998) N.Y.U. L. Rev. 2064.

Tribe, L. H., « The Constitution in Cyberspace » dans Ermann, M. David, *et al*. dir., *Computer, Ethics and Society*, New York, Oxford University Press, 1997, 208.

Warren, S. D. et Brandeis, L. D., « The Right toPrivacy » (1890) Harv. L.R. 193.

Winick, R., «Searches and Seizure of Computers and Computer Data» (1994) 8 Harv. J.L. & Tech 75.

Winters, S., « The New Privacy Interest : Electronic Mail in the Workplace » (1993) 8 High Tech L.J. 197.

White, J. J. « E-mail@Work.Com : Employer Monitoring of Employee E-mail » 48 (1997) Ala. L. R. 1079.

– **Rapports et documents gouvernementaux (canadiens)**

Canada, Centre de sécurité dans les télécommunications, *Qu'est-ce que la cryptographie à clé publique ?*, (sans date), en ligne : <http://www.cse-cst.gc.ca/cse/francais/gov3.html> (date d'accès : 25 avril 1999).

Canada, Centre de sécurité dans les télécommunications, *Qu'est-ce que la signature numérique ?*, (sans date), en ligne : <http://www.cse-cst.gc.ca/cse/francais/gov4.html> (date d'accès : 25 avril 1999).

Canada, Centre de sécurité dans les télécommunications, *Qu'est-ce qu'une infrastructure à clé publique ?*, (sans date), en ligne : <http://www.cse-cst.gc.ca/cse/francais/gov5.html> (date d'accès : 25 avril 1999).

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

Canada, Comité permanent de la justice et des questions juridiques, *Les infractions relatives aux ordinateurs,* (Compte rendu officiel), Ottawa, Approvisionnements et services Canada, 1983 (Présidente : Céline Hervieux-Payette).

Canada, Comité permanent de la justice et des questions juridiques, *Les infractions relatives aux ordinateurs,* (Rapport final), Ottawa, Approvisionnements et services Canada, 1983 (Présidente : Céline Hervieux-Payette).

Canada, Industrie Canada, (21 février 1998), *Glossaire : s.v.* « la récupération des clés », en ligne : <http://strategis.ic.gc.ca/cgi-bin/basic/ftgetdoc?table=infoallf&fname=..%2Fauthorsf%2Fsgml%2Fdoc%2Fcy00013f.html&ft_cid=108993&headline=Glossaire&id=19851&lang=f&where=((ft_text%20CONTAINS%20'cryptographie'))%20AND%20(product%20CONTAINS%20'155')%20> (date d'accès : 28 avril 1999).

Canada, Industrie Canada, *Résumé de la politique canadienne en matière de cryptographie*, Ottawa, 1998, (groupe de travail sur le commerce électronique), en ligne : <http://e-com.ic.gc.ca/francais/fastfacts/43d7.htm> (date d'accès : 28 avril 1999).

Canada, Ministère de la justice, *Vie privée sans frontières : les flux transfrontières de renseignements personnels en provenance du Canada*, Ottawa, Approvisionnements et Services Canada, 1990 (Étude réalisée par le Groupe de Recherche en Informatique et Droit).
Canada, Ministère de la Justice et Solliciteur Général, *Le blanchiment de la monnaie électronique : Analyse de Justice Canada et du Solliciteur Général du Canada*, Ottawa, 1998, en ligne : <http://www.sgc.gc.ca/home/reportsdoc/ppc/fmoney.doc> (date d'accès : 23 avril 1999).

Canada, Rapport du groupe d'étude établi conjointement par le ministère des Communications et le ministère de la Justice. *L'ordinateur et la vie privée.* Ottawa : Information Canada, 1972.

Canada, Service canadien du renseignement de sécurité, *Rapport public de 1997*, Ottawa, Approvisionnements et Services, 1998.

Canada, Service canadien du renseignement de sécurité, *Rapport public de 1999*, Ottawa, Approvisionnements et Services, 2000.

Canada, Solliciteur Général, *Maintenir le cap : La sécurité nationale dans les années 1990*, Ottawa, Approvisionnements et services, 1991 (Réponse du gouvernement au Rapport du Comité spécial de la Chambre des communes sur l'examen de la Loi sur le Service canadien du renseignement de sécurité et de la Loi sur les infraction en matière de sécurité).

Canada, Statistique Canada, *Enjeux auxquels sont confrontés les fournisseurs canadiens de services Internet : survol tiré d'une enquête des FSI*, Ottawa, Indicateurs des services, 63F0002XPB no 28, décembre 1999 (Auteurs : Norah Hillary et Gord Baldwin).

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>

Canada, Statistique Canada, *Être branché ou ne pas l'être : croissance de l'utilisation des services de communication par ordinateur*, Ottawa, Indicateurs des services, 63F0002XPB no 27, novembre 1999 (Auteurs : Paul Dickinson et Jonathan Ellison).

Québec, Conseil du Trésor, *Implantation de services de courriel dans les écoles*, par Abran, France et Trudel Pierre, Québec, Conseil du trésor, 2000 (Document de réflexion).

– **Rapports et documents gouvernementaux et non gouvernementaux (internationaux)**

Conseil de l'Europe, état des signatures et ratifications, en ligne : Convention sur la cybercriminalité <http://conventions.coe.int/Treaty/FR/searching.asp?NT=185&DF=> (date d'accès : 24 novembre 2001).

OCDE, Groupe d'action financière sur les blanchiments de capitaux (GAFI), *Rapport du GAFI XII sur les typologies du blanchiment des capitaux* (2000-2001), Document de travail, février 2001.

OCDE, *La politique de cryptographie : les lignes directrices et les questions actuelles*, (sans date), en ligne : <http://www.oecd.org//dsti/sti/secur/prod/gd97-204f.pdf> (date d'accès : 23 avril 1999).

– **Rapports et documents gouvernementaux et non gouvernementaux (américains)**

American Bar Association, Task Force on Computer Crime Section of Criminal Justice, *Report on Computer Crime,* Washington D.C., 1984 (Président : Joseph B. Thompkins, Jr.).

U.S. Congress, Office of Technology Assessment, *Electronic Surveillance in a Digital Age*, OTA-BP-ITC-149, Washington DC, U.S. Government Printing Office, 1995, en ligne : <http://www.wws.princeton.edu/cgi-bin/byteserv.prl/~ota/disk1/1995/9513/9513.PDF> (date d'accès : 10 août 2001).

United Sates, Department of Justice, *Independant Technical Review of the Carnivore System Draft Report*, ITT Research Institute, 2000 (auteurs : Smith, Stephen P., Perrit, Jr., Henry, *et al.*), en ligne : <http://www.usdoj.gov/jmd/publications/carnivore_draft_1.pdf> (date d'accès : 24 août 2001).

– **Monographies (canadiennes)**

Bélanger, A. et Roy, J.-H., *Internet le guide 2000*, 5e éd., Montréal, Québec Science, 2000.

Bennett, C. J. et Grant, R., *Visions of Privacy. Policy Choices for the Digital Age*, Toronto, University of Toronto Press, 1999.

Poussart, B., *Les communications électroniques* , St-Hyacinthe (Qc.), Collection infomètre, Isabelle Quintin, 2000.

Sohier, D. J., *Le guide de l'internaute,* Montréal, Les éditions logiques, 2000.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>

Juriscom.net droit des technologies de l'information

– **Monographies (américaines et françaises)**

Amoroso, E., *Intrusion Detection*, Sparta (NJ), Intrusion.Net Books, 1999.

(Anonyme), *Sécurité Optimale,* 2e éd., Paris, Campus Press France, 1999.

Bacard, A., *The Computer Privacy Handbook*, Berkeley (CA), Peachpit Press 1995.

Casey, Ehogan, *Digital Evidence and Computer Crime*, San Diego (CA), Academic Press, 2000.

Cillufo, F. J., *et al.*, *Cybercrime... Cyberterrorism... Cyberwarfare... Averting an Electronic Waterloo,* Washington, CSIS Press (The Center for Strategic and International Studies), 1998.

Crume, J., *Inside Internet Security*, Londres, Addison-Wesley, 2000.

Denning, D. E., *Information Warfare and Security*, Reading (Mass.), Addison-Wesley, 1999.

Diffie, W.. et Landau, S., *Privacy on the Line. The Politics of Wiretapping and Encryption*, MIT Press, Cambridge, 1998.

Dufour, A., *Internet*, Paris, Presses Universitaires de France, coll. « Que sais-je? », 1998.

Dufresne, D. et Latrive, F., *Pirates et flics du Net*, Seuil, Paris, 2000.

Electronic Frontier Fondation, *Cracking DES. Secrets of Encryption Research, Wiretap Politics & Chip Design*, Sebastopol (CA), O'Reilly & Associates, 1998.

Ermann, M. D. *et al.*, *Computer, Ethics and Society*, New York, Oxford University Press, 1997.

Fabrot, B., *Protégez-vous sur Internet : Anonymat et sécurité*, Paris, Marabout Informatique, 1999.

Garfinkel, S., et Spafford, G., *Web Security & Commerce*, Sebastopol (CA), O'Reilly & Associates, 1997.

Garfinkel, S., *Database Nation. The Death of Privacy in The 21st Century*, Sebastopol (CA), O'Reilly & Associates, 2000.

Garfinkel, S. L., *Architects of the Information Society*, Cambridge, MIT Press, 1999.

Gelman, R. B. *et al.*, *Protecting Yourself Online*, New York, Harper Collins, 1998.

Gieske, Wolfram, *Sécurité et protection*, Düsseldorf, Data Becker GmbH & co., 1998.

Gurak, L. J., *Persuasion and Privacy in Cyberspace*, New Haven (CON), Yale University Press, 1997.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>

Juriscom.net droit des technologies de l'information

Hayden, M., *Les réseaux*, Paris, Campus Press France, 1999.

Icove D. *et al*., *Computer Crime, A Crime Fighter's Handbook*, Sebastopol (CA), O'Reilly & Associates, 1995.

Kosiur, D., *Understanding Electronic Commerce*, trad. par Dorseuil, Alain, Paris, Microsoft Press, 1997.

Larcher, É., *L'Internet sécurisé*, Paris, Eyrolles, 2000.

Lévy, P., *L'intelligence collective. Pour une anthropologie du cyberspace*, La découverte, Paris, 1995.

Lyon, D. et Zureik, E., *Computers, Surveillance & Privacy*, Minneapolis, University of Minnesota Press, 1996.

Mansfield, R., *Hacker Attack ! Shield Your Computer From Internet Crime*, Alameda (CA), Sybex, 2000.

Martin, D., *La Criminalité informatique*, Paris, Presses Universitaires de France, 1997.

McClure, S. *et al.*, *Hacking Exposed : Network Security Secrets and Solutions*, 2e ed., Berkeley (CA), Osborne/McGraw-Hill, 2001.

Meyer, J.-J., *Les réseaux*, Paris, Osman Eyrolles Multimédia, 2000.

Pansier, F.-J. et Jez, E., *La criminalité sur l'Internet,* Paris, Presses Universitaires de France, coll. « Que sais-je? », 2000.

Parker, D. B., *Fighting Computer Crime, A new framework for protecting information*, New-York, John Wiley and Sons, 1998.

Power, R., *Tangled Web. Tales of Digital Crime From the Shadows of Cyberspace*, Indianapolis , Que, 2000.

Von Neumann, J., *The Computer and the Brain*, trad. Par P. Engel, Paris, Flammarion, 1996.

Voss, A., *Dictionnaire de l'informatique et de l'Internet 2001*, Paris, Micro Application, 2000.

– **Revues, articles de journaux conventionnels, articles en ligne et communiqués**

Bell, S., « RCMP Probing 'Jihad' Websites » *National Post* (18 août 2001) A-1 et A-4.

Blackwell, G., « The Way the Cookie Crumbles » *Canadian Lawyer* (septembre 1998) 9.

Canada, Communiqué « *Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime* » (Moscou, 19-20 octobre 1999), en ligne : Ministère des affaires étrangère et du commerce international <http://www.g8.gc.ca/1999/moscow1-f.htm>

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>

(date d'accès : 9 novembre 2001).

Canada, Communiqué « Points saillants de la Loi antiterroriste » (Ottawa, 15 octobre 2001), en ligne, Ministère de la Justice <http://Canada.justice.gc.ca/fr/nouv/cp/2001/doc_27786.html> (date d'accès : 18 octobre 2001).

Canada, Industrie Canada, Communiqué « Le ministre Manley présente les grandes lignes de la politique en matière de cryptographie » (Ottawa, 1er octobre 1998), en ligne : <http://e-com.ic.gc.ca/français/releases/41d6.htm> (date d'accès : 28 avril 1999).

Eng, P., « Scouring Cyberspace. Tapping the Internet for Clues on the Attack on America » ABC News.com (13 septembre 2001), en ligne : <http://www.abcnews.go.com/sections/scitech/DailyNews/WTC_netsearch010913.html> (date d'accès : 13 septembre 2001).

Ipsos-Reid Canada, communiqué, « *Canadian Internet access continues to grow, and users say the Net has had a significant impact on their lives* », (26 juillet 2000), Ipsos-Reid, en ligne : <http://www.angusreid.com/media/content/displaypr.cfm?id_to_view=1061> (date d'accès :12 août 2001).

Mc Namara, J., « The complete, Unofficial TEMPEST Information Page », version du 3 août 2001, à : http://www.eskimo.com/~joelm/tempest.html (consulté le 6 septembre 2001).

Media Metrix Canada release June 2001, communiqué, « *Total Canada at Home Web Use Report on Internet Usage Stats* », (25 juillet 2001), *Media Metrix*, en ligne : <http://ca.mediametrix.com/press/releases/20010725.jsp> (date d'accès : 12 août 2001).

Tourangeau, Pierre, « Les gouvernements ont les internautes à l'œil » (2001), Radio-Canada.ca-Zone nouvelles, en ligne : <http://src.ca/url.asp?/nouvelles/index/nouvelles/200103/02/004-cookies.asp> (date d'accès : 2 mars 2001).

– **Sites Internet**

AbsoluteChat, en ligne : <http://www.absolutechat.com> (date d'accès :10 juillet 2001).

Alta Vista, en ligne : <http://www.altavista.com> (date d'accès : 24 avril 2001).

Anonymiser, en ligne : <http://www.anonymiser.com> (date d'accès : 14 novembre 2000).

AOL Instant Messanger, en ligne : <http://www.netscape.com/fr> (date d'accès : 19 juillet 2001).

ARIN, en ligne : <http://www.whois.arin.net/whois/arinwhois.html> (date d'accès : 5 septembre 2001).

ASA Networks, en ligne : <http://www.asacomp.com> (date d'accès : 15 août 2001).

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

Assentor, en ligne : <http://www.assentor.com> (date d'accès : 31 octobre 2000).

Big Brother Inside, en ligne : <http://www.bigbrotherinside.com> (date d'accès : 6 septembre 2001).

Carnivore, en ligne : <http://www.fbi.gov/hq/lab/carnivore/carnivore.htm> (date d'accès :24 août 2001).

CATALIST, en ligne : <http://www.lsoft.com/lists/listref.html> (date d'accès : 24 août 2001).

Chatalyst, en ligne : < http://www.chatalyst.com> (date d'accès : 10 juillet 2001).

Chat Net, en ligne : <http://www.chatnet.org> (date d'accès : 16 juin 2001).

CNET News.com, en ligne : <http://www.news.cnet.com/news/0-1005-200-7801931.html?tag=prntfr> (date d'accès : 12 novembre 2001).

Cogeco câble, en ligne : <http://www.cogeco.ca> (date d'accès : 20 juillet 2001).

Cogiciel, en ligne : <http://www.cogiciel.com> (date d'accès : 20 juin 2001).

Cookie Crusher, en ligne : <http://www.thelimitsoft.com/cookie.html> (date d'accès : 5 septembre 2001).

Cookie Monster, en ligne : <http://www.geocities.com/paris/1778/monster.html> (date d'accès : 5 septembre 2001).

Coolist, en ligne : <http://www.coolist.com> (date d'accès : 8septembre 2001).

Coolsig, en ligne : <http://www.coolsig.com> (date d'accès :13 août 2001).

Copernic, en ligne : <http://www.copernic.com> (date d'accès : 20 juin 2001).

CU-SeeMe, en ligne : <http://www.cuseemeworld.com> (date d'accès : 23 juillet 2001).

DALnet, en ligne : <http://www.dal.net> (date d'accès : 16 juin 2001).

Deja.com, en ligne : <http://deja.com/usenet> (date d'accès : 2 novembre 2000).

DirecPC, en ligne : <http://www.direcpc.com> ou <http://www.directpc.com> (dates d'accès : 5 août 2001).

DIRECTV, en ligne : <http://www.directv.com> (date d'accès : 5août 2001).

eCash Technologies Inc., en ligne : <http://www.digicash.com> ou <http://www.ecashtechnologies.com> (date d'accès : 8 novembre 2001).

EFNet, en ligne : <http://www.efnet.net> (date d'accès : 16 juin 2001).

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>

Juriscom.net
droit des technologies de l'information

Egroup, en ligne : <http://www.egroups.com> (date d'accès : 8 septembre 2001).

Excite, en ligne : <http://www.excite.com> (date d'accèes : 20 juin 2001).

Forum One, en ligne : <http://www.forumone.com> (date d'accèes 10 juillet 2001).

Francité, en ligne : <http://www.francite.com> (date d'accès :20 juin 2001).

Francopholistes, en ligne : <http://www.cru.fr/listes> (date d'accès : 24 août 2001).

Google, en ligne : <http://google.com> (date d'accès : 12 novembre 2001).

Hiersay, en ligne : <http://www.hiersay.net/robots.htm> (date d'accès : 23 juillet 2001).

Hot Bot, en ligne : <http://www.hotbot.com> (date d'accès : 20 juin 2001).

Ichat, en ligne : <http://www.ichat.com> (date d'accès : 9 juillet 2001).

ICQ, en ligne : <http://www.icq.com>, <http://www.icq.com/directconnection> et <http://www.icq.com/support/security/ipprivacy.html> (date d'accès :19 juillet 2001).

Infoseek, en ligne : <http://www.infoseek.com> (date d'accès : 2 novembre 2000).

Intel, en ligne : <http://www.intel.com> (date d'accès :5 septembre 2001).

L'*Internet Assigned Numbers Authority* (*IANA*), en ligne : <http://www.iana.org/assignments/port-numbers> (date d'accès : 3 août 2001).

Internet Explorer de Microsoft, en ligne : <http://www.microsoft.com/france/internet/produits/ie/ie5> (date d'accès : 11 juin 2001).

Internet Phone, en ligne : <http://www.eurocall.com/e/ip5/htm> (date d'accès : 23 juillet 2001).

Ircle, en ligne : <http://www.microsoft.com/France/internet/produits/chat> (date d'accès : 9 juillet 2001).

La toile du Québec, en ligne : <http://www.toile.qc.ca> (date d'accès : 20 juin 2001).

Listserv, en ligne : <http://www.lsoft.com> (date d'accès : 5 septembre 2001).

Lycos, en ligne : <http://www.lycos.com> (date d'accès : 24 avril 2001).

Mc Namara, Joel, « *The complete, Unofficial TEMPEST Information Page* », (2001), en ligne : <http://www.eskimo.com/~joelm/tempest.html> (dernière modification : 3 août 2001).

Mégagiciel, en ligne : <http://www.megagiciel.com> (date d'accès : 20 juin 2001).

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>

Juriscom.net
droit des technologies de l'information

Messenger de *Yahoo !*, en ligne : <http://www.messenger.yahoo.com/intl/fr> (date d'accès : 19 juillet 2001).

Meta Crawler, en ligne : <http://www.metacrawler.com> (date d'accès : 24 avril 2001).

mIRC, en ligne : <http://www.nirc.com> (date d'accès : 9 juillet 2001).

Mirc-X Boots & Add-on, en ligne : <http://www.mircx.com> (date d'accès : 23 juillet 2001).

Mondex, en ligne : <http://www.mondex.com/> (date d'accès : 12 novembre 2001).

MSN Messenger de *Microsoft*, en ligne : <http://www.messenger.fr.msn.ca> (date d'accès : 19 juillet 2001).

Navigator de Netscape, en ligne : <http://www.netscape.com/fr>(date d'accès : 11 juin 2001).

Net2Phone, en ligne : <http://www.net2phone.com> (date d'accès : 16 juillet 2001).

NetMeeting, en ligne : <http://www.microsoft.com/windows/netmeeting> (date d'accès : 23 juillet 2001).

Network Information Center, en ligne : <http://www.internic.net> (deate d'accès :5 septembre 2001).

Nomade, en ligne : <http://www.nomade.fr> (date d'accès : 20 juin 2001).

NUA Internet Surveys, *NUA*, en ligne : <http://www.nua.com/surveys/how_many_online/n_america.html> (date d'accès : 20 juin 2001).

Office de la langue française, 2001, *s.v.* « technologie de l'information », en ligne : <http://www.olf.gouv.qc.ca/ressources/internet/fiches/8875723.htm>, *s.v.* « nouvelle technologie de l'information et des communications », en ligne : <http://www.olf.gouv.qc.ca/technologies.html#expression>, *s.v.* « nouvelles TI », en ligne : <http://www.olf.gouv.qc.ca/ressources/internet/fiches/8874697.htm>, *s.v.* « Internet », en ligne : <http://www.olf.gouv.qc.ca/ressources/internet/fiches/2074841.htm>, *s.v.* « courriel », en ligne : <http://www.olf.gouv.qc.ca/ressources/internet/fiches/1299117.htm>, *s.v.* « cybercafé », en ligne : <http://www.olf.gouv.qc.ca/ressources/internet/fiches/2075030.htm> et *s.v.* « cyberespace », en ligne : <http://www.olf.gouv.qc.ca/ressources/internet/fiches/2071771.htm> (date d'accès : le 21 février 2001).

Opbot, en ligne : <http://www.chez.com/opbot> (date d'accès : 23 juillet 2001).

Outlook Express, en ligne : <http://www.microsoft.com/France/internet/produits/oe> (date d'accès : 11 juin 2001).

Pretty Good Privacy ou PGP, en ligne : <http://www.pgpi.com> (date d'accès : 22 novembre 2000).

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>

Juriscom.net
droit des technologies de l'information

Poste Canada, service PosteCS[MC] , en ligne : Postes Canada <http://www.canadapost.ca/business/offerings/postecs/can/default-f.asp> (date d'accès : 8 novembre 2001).

RFC 850 en ligne : <http://www.rfc-editor.org> (date d'accès : 14 août 2001).

RFC 997, en ligne : <http://www.normos.org/ietf/rfc/rfc977.txt> (date d'accès : 15 août 2001).

RFC 1459, en ligne : <www.normos.org/ietf/frc/rfc1459.txt> (date d'accès : 28 juillet 2001).

RFC 1855, en ligne : <http://www.faqs.org/rfcs/rfc1855.html> (date d'accès : 21 décembre 2001).

RFC 2109, en ligne : <http://www.normos.org/ietf/rfc/rfc2109.txt> (date d'accès : 5 septembre 2001).

Search Engine Watch, en ligne : <http://www.searchenginewatch.com> (date d'accès : 20 juin 2001).

Secure Electronic Transcaction Protocol (*SET*) : *Secure Electronic Transcaction Protocol* (*SET*), en ligne : <http://www.setco.org> (date d'accès : 8 novembre 2001).

Shareware.com, en ligne : <http://shareware.com> (date d'accès : 20 juin 2001).

Steganos, en ligne : <http://www.demcom.com/english/steganos> (date d'accès : 14 novembre 2000).

Symantec, en ligne : <http://www.symantec.com/sabu/qdeck/ncs/features.html> (date d'accès : 10 septembre 2001).

Sympatico édition haute vitesse, en ligne : <http://www.whv.sympatico.ca> (date d'accès : 20 juillet 2001).

TalkWay, en ligne : <http://www.talkway.com> (date d'accès : 20 juin 2001).

Telus, en ligne : <http://www.telusmobilite.com/qc/mike/mike_networks_home.shtml> (date d'accès : 2 juillet 2001).

The Palace, en ligne : <http://www.thepalace.com> (date d'accès : 29 juin 2001).

Tile.net, en ligne : <http://tile.net/ftp> (date d'accès : 20 juin 2001).

Trouvez !, en ligne : <http://www.trouvez.com> (date d'accès :20 juin 2001).

Ultimate ChatList, en ligne : <http://www.chatlist.com> (date d'accès : 10 juillet 2001).

Undernet, en ligne : <http://www.undernet.org> (date d'accès 16 juin 2001).

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

Vidéotron Ltée., en ligne : <http://www.videotron.com> (date d'accès : 20 juillet 2001).

Web Chat Broadcasting Service, en ligne : <http://www.pages.wbs.net> (date d'accès : 10 juillet 2001).

Web Talker, en ligne : <http://www.webtalker.com> (date d'accès : 10 juillet 2001).

Whowhere, en ligne : <http://whowhere.lycos.com> (date d'accès : 2 novembre 2000).

Windows 98 de *Microsoft*, en ligne : <http://www.microsoft.com/France/windows> (date d'accès : 11 juin 2001).

Winzip, en ligne : <http://www.winzip.com> (date d'accès :20 juin 2001).

World Pages, en ligne : <http://www.worldpages.com> (date d'accès : 24 avril 2001).

Ws_FTP, en ligne : <http://www.ipswitch.com/Products/WS_FTP> (date d'accès : 24 avril 1999).

Yahoo !, en ligne : <http://www.yahoo.ca> (date d'accès : 20 juin 2001).

– **Ouvrages de référence**

Beaud, Michel et Latouche, Daniel, *L'art de la thèse*, Montréal, Boréal, 1988.

Beaulieu, Sébastien, dir., *Manuel canadien de la référence juridique*, 4e éd., Scarborough (Ont.), Carswell, 1998.

Le nouveau petit Robert, 1993, *s.v.* « intrusion ».et *s.v.* « ubiquité ».

Létourneau, Jocelyn, *Le coffre à outils du chercheur débutant*, Toronto, Oxford University Press, 1989.

Luelles, Didier, *Guide de référence pour la rédaction juridique*, 6e éd., Montréal, Thémis, 2000.

Copyright © François BLANCHETTE
Juriscom.net, 3 février 2004, <http://www.juriscom.net>

Juriscom.net droit des technologies de l'information