Lex Electronica
Revue du Centre de recherche en droit public

L'avocat a-t-il l'obligation de chiffrer ses courriels confidentiels en vertu de l'article 34 de la *Loi concernant le cadre juridique des technologies de l'information* ?

Christine LEBRUN

Lex Electronica, vol. 14 n°2 (Automne / Fall 2009)

INTRODUCTION

L'utilisation de courriels contenant des informations confidentielles par les avocats a littéralement explosé au cours des dernières années. En 2006, 48,8% des avocats ayant répondu à un sondage de l'*American Bar Association* envoyaient des informations confidentielles ou privilégiées par courriel au moins une fois par jour et 90% d'entre eux le faisaient au moins deux fois par année. « *Shockingly* », seulement 16.4% de ces courriels étaient chiffrés, 76% des avocats américains se contentant d'un avertissement portant sur la confidentialité de leurs courriels[1].

Au Québec, la *Loi concernant le cadre juridique des technologies de l'information*[2] est entrée en vigueur le 1er novembre 2001[3]. Le premier alinéa[4] de l'article 34 de la LCJTI exige que la transmission de documents que la loi déclare confidentiels soit protégée par un « moyen approprié au mode de transmission » comme suit :

> 34. Lorsque la loi déclare confidentiels des renseignements que comporte un document, leur confidentialité doit être protégée par un moyen approprié au mode de transmission, y compris sur des réseaux de communication. [Nous soulignons]

Il n'est pas contesté que le terme « document » à l'article 34 LCJTI inclue un courriel et tout fichier qui lui est attaché[5]. Prenant pour acquis que des renseignements contenus dans des courriels non chiffrés peuvent être confidentiels[6] et que l'utilisation de courriels non chiffrés ne constitue pas une renonciation au secret professionnel[7], nous nous sommes demandé si les avocats québécois ont l'obligation en vertu de l'article

---

1 Ash MAYFIELD, « Decrypting the Code of Ethics : The Relationship between an Attorney's Ethical Duties and Network Security », (2007) 60 Okla. L. Rev. 54, p. 570.

2 L.Q. 2001, c. 32 (ci-après « **LCJTI** » ou « **Loi** ») maintenant L.R.Q. c. C-1.1. L'article 104 de la Loi est entré en vigueur deux semaines plus tôt.

3 *Tableau des entrées en vigueur, Lois sanctionnées entre le 1er janv. 1978 et le 1er déc. 2007*, en ligne : www2.publicationsduquebec.gouv.qc.ca/lois_et_reglements/tab_modifs/TEEV19782007Fr.pdf

4 Le second alinéa de l'article 34 LCJTI énonce des obligations en matière de documentation. Il ne fera pas l'objet de notre étude.

5 Claude MARSEILLE, « L'utilisation du courrier électronique à la lumière de la *Loi concernant le cadre juridique des technologies de l'information* », dans *Bulletin de Prévention du Fonds d'assurance responsabilité du Barreau du Québec*, Édition spéciale no 5, avril 2002, p. 1-2. En ligne : www.assurance-barreau.com/fr/pdf/bullPrevAvr2002.pdf. L'auteur réfère aux articles 3 et 74 de la LCJTI quant à la portée très large de la notion de « document » à la LCJTI.

6 Martine BOURET et Troy HARRISON, « E-Mail Confidentiality and Solicitor-Client Privilege Issue », (2002-2003) 26 Advoc. Q. 23, p. 35. Cette question serait loin d'être réglée en droit canadien mais les autorités concluent majoritairement qu'un courriel permet une « *reasonable expectation of confidentiality* ».

7 Voir Charles MORGAN et Julian SAULGRAIN, *E-mail Law*, Markham, Ont. LexisNexis, 2008, à la p. 139 : « These privileged communications may take the form of e-mail […] ». Voir aussi Martine BOURET et Troy HARRISON, préc., note 6, p. 39 : « It appears that the current view of Canadian legal regulators is that the solicitor-client privilege […] are not automatically defeated by the mere use of e-mail technology […] ».

34 alinéa 1 LCJTI de chiffrer les courriels qu'ils transmettent[8] et qui contiennent des renseignements confidentiels concernant leur clients[9].

Pour répondre à cette question, nous examinerons dans un premier temps, l'historique de l'article 34 de la Loi afin de tenter de déterminer quelle était l'intention du Législateur lors de son adoption. Nous vérifierons ensuite quelles sont les obligations de confidentialité des avocats québécois ainsi que les principaux risques qui sont associés à l'envoi de courriels confidentiels. Dans la dernière portion de ce travail, nous tenterons de répondre à la question de savoir si les avocats sont tenus de chiffrer leurs courriels confidentiels en examinant ce qu'est le « chiffrement » ainsi qu'en étudiant l'état du droit au Québec sur l'article 34 de la Loi. Nous étendrons ensuite notre examen aux obligations de confidentialité des avocats des provinces des autre provinces canadiennes, des États-Unis ainsi que du Royaume-Uni lors de l'envoi de courriels confidentiels afin de vérifier si le chiffrement des courriels y est devenu une « norme de l'industrie » pouvant désormais s'appliquer aux avocats québécois.

1. L'historique de l'adoption de l'article 34 LCJTI

L'étude de l'historique de l'article 34 LCJTI fournit très peu d'indices utiles pour déterminer si le Législateur québécois avait l'intention d'imposer le chiffrement des courriels confidentiels. Il est cependant intéressant de noter que, dans l'avant-projet de *Loi sur la normalisation juridique des nouvelles technologies de l'information* qui a précédé l'entrée en vigueur de la LCJTI, l'article 37 contenait un deuxième alinéa qui énonçait, entre autres moyens pour protéger la confidentialité d'un document, le chiffrement et l'utilisation de canaux de transmission dédiés :

> **37.** Lorsque la loi déclare confidentiels des renseignements que comporte un document, leur confidentialité doit être protégée par un moyen approprié au mode de transmission, y compris sur des réseaux de communication ouverts ou fermés.
>
> La confidentialité du document transmis peut être protégée, entre autres par le chiffrement du document avant sa transmission, par l'utilisation de canaux de communication munis de fonctions de chiffrement, par l'utilisation de canaux de communication dont une personne est responsable et qui sont dédiés à la transmission de ses documents ou de ceux provenant de personnes à qui elle donne accès à ces canaux ou par tout autre moyen convenu entre l'expéditeur et le destinataire. […] [Nous soulignons]

Ce second alinéa a été supprimé de la version finale de l'article 34 LCJTI sans que l'on ne sache pourquoi. En effet, lors de l'étude du *Projet de loi 161* par la

---

8 Nous excluons de notre travail la question des courriels, sollicités ou non, qui sont reçus par les avocats.

9 Sunny HANDA, Claude MARSEILLE et Martin SHEEHAN, *E-Commerce Legislation and Materials in Canada/Lois sur le commerce électronique au Canada et documents connexes*, Markham, Ontario, Lexis Nexis Butterworths, 2005-2006, 883 p., à la p. 258. Ces auteurs soulèvent cette question en regard de l'article 34 de la Loi sans toutefois y répondre : « Faut-il conclure que tous les courriels contenant de l'information déclarée confidentielle par la loi devraient être chiffrés? »

Commission permanente de l'économie et du travail, l'article 34 LCJTI n'a pas été discuté puisque les travaux de la commission ont été suspendus indéfiniment à cause de la lenteur de ses progrès et l'étude de la LCJTI s'est finalement terminée à l'article 25. Il est donc difficile de connaître quelle était l'intention du Législateur en adoptant l'article 34 LCJTI tel qu'il est rédigé dans sa version finale.

On trouve cependant sur le site web du *Ministère des services gouvernementaux*, une indication que le Législateur aurait voulu laisser aux personnes responsables le choix des moyens appropriés pour protéger la confidentialité des documents lors de leur transmission[10].

2. Les obligations de confidentialité des avocats

Il n'y a pas de doute, à notre avis, que l'article 34 LCJTI s'applique aux courriels confidentiels des avocats québécois. En effet, plusieurs articles de loi obligent ces derniers à protéger la vie privée de leurs clients et la confidentialité des secrets qui leurs sont confiés en raison de leur profession. Ces courriels constituent donc des documents comportant des renseignements que la loi déclare confidentiels aux termes de l'article 34 al. 1 LCJTI.

2.1. La protection de la vie privée

Au Québec, le droit à la vie privée est un droit fondamental en vertu de l'article 5 de la *Charte des droits et libertés de la personne*[11]. Nul ne peut porter atteinte à ce droit sans le consentement de la personne concernée ou sans que la loi ne l'autorise[12]. Le fait d'« [i]ntercepter ou utiliser volontairement une communication privée », de surveiller la vie privée d'une personne par quelque moyen que ce soit ou d'« [utiliser sa correspondance […] ou ses autres documents personnels » constituent des atteintes à la vie privée d'une personne[13].

La *Loi sur la protection des renseignements personnels dans le secteur privé*[14] ajoute qu'une personne qui exploite une entreprise doit prendre des mesures de sécurité pour assurer la protection des renseignements personnels communiqués « et qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support. »[15]. Or, l'avocat qui pratique en

---

10 Ministère des services gouvernementaux du Québec : « Le choix des moyens, quant à la façon d'assurer la protection des renseignements confidentiels lors de la transmission d'un document, est laissé à ceux qui en ont la responsabilité ». En ligne : http://www.msg.gouv.qc.ca/fr/enligne/loi_ti/articles/chap2/art34.asp.

11 L.R.Q. c. C-12 (ci-après « **Charte québécoise** »). Voir aussi les articles 3 et 35 C.c.Q.

12 Article 35 C.c.Q.

13 Article 36 C.c.Q., para (2), (4) et (6).

14 L.R.Q. c. P-39.1 (ci-après « **LPRPSP** »).

15 Article 10 LPRPSP.

cabinet privé exploite une entreprise aux termes de l'article 1525 C.c.Q. et serait donc assujetti à la LPRPSP[16].

Enfin, d'autres lois s'appliquent à la protection des renseignements confidentiels que possèdent les avocats exerçant leur profession dans le secteur public ou au sein d'entreprises de compétence fédérale et qui communiquent des renseignements personnels à des tiers à l'extérieur du Québec, notamment, par Internet[17].

2.2. Le secret professionnel : une obligation de moyens ou de résultat?

Le droit au droit au secret professionnel est un droit fondamental en vertu de l'article 9 de la Charte québécoise. La personne tenue par la loi[18] au secret professionnel ne peut en être relevée que par une disposition expresse de la loi ou par la personne qui lui a fait les confidences[19].

Les avocats sont bien entendus légalement tenus au secret professionnel. La *Loi sur le Barreau* prévoit que « [L]'avocat doit conserver le secret absolu des confidences qu'il reçoit en raison de sa profession. »[20]. Il doit également « s'assurer de la confidentialité de ses dossiers […] »[21].

À première vue, il semble que l'avocat soit tenu à une véritable obligation de résultat en ce qui concerne la préservation du secret professionnel[22]. Le problème est que « la sécurité absolue n'existe pas lorsqu'il est question de nouvelles technologies de l'information »[23].

Le caractère absolu de cette obligation de l'avocat est cependant atténué par le *Code de déontologie*[24], le règlement le plus important « pour les fins de la responsabilité civile

---

16 Voir Marie ST-PIERRE, Règles du jeu : l'avocat et les renseignements personnels dans *Développements récents en droit civil (2001), Service de la formation permanente du Barreau du Québec*, 2001, EYB2001DEV398, para 5.1.2 et 6.1 et Raymond DORAY, « Les devoirs et les obligations de l'avocat », *Éthique, déontologie et pratique professionnelle*, Collection de droit 2008-2009, École du Barreau du Québec, vol. 1, 2008, p. 29-71, à la p. 67.

17 Raymond DORAY, préc., note 16, p. 68-69.

18 Art. 60.4 al. 1 du *Code des professions*, L.R.Q. c. C-26.

19 Art. 9 al. 2 de la Charte québécoise. Voir aussi l'art. 131(2) de la *Loi sur le Barreau*, L.R.Q. c. B-1, l'art. 60.4 al. 2 du *Code des professions*, L.R.Q. c. C-26 et l'art. 3.06.02 du *Code de déontologie des avocats*, R.R.Q., 1981, c. B-1, r.1.

20 *Loi sur le Barreau*, L.R.Q. c. B-1, art. 131(1).

21 Art. 7, *Règlement sur les normes de tenue des dossiers et de domicile professionnel des avocats*, R.R.Q. c. C-26, r.19.2.2.

22 Robert CASSIUS DE LINVAL, « Le secret professionnel empêche-t-il l'utilisation du courrier électronique? », p. 2. En ligne : www.lex-electronica.org/docs/articles_197.html.

23 Robert CASSIUS DE LINVAL, « Déontologie et environnement informatiques: petit guide du praticien branché – 104 », dans *Développements récents en déontologie et responsabilité professionnelle (1998)*, Service de la formation permanente, Barreau du Québec, Cowansville, Yvon Blais, 1998, p. 164, à la p. 167.

24 R.R.Q., 1981, c. B-1, r.1.

» des avocats[25]. Ainsi, l'avocat n'a que l'obligation de prendre des moyens raisonnables pour faire respecter le secret absolu des confidences qu'il reçoit à l'égard de ses collaborateurs ou de ses collègues au sein de sa société :

> **3.06.03.** L'avocat doit prendre les moyens raisonnables pour faire respecter le secret absolu des confidences qu'il reçoit dans l'exercice de sa profession par toute personne qui coopère avec lui ou exerce ses activités au sein de la société où il exerce ses activités professionnelles.
>
> **3.06.04.** L'avocat qui emploie ou retient les services d'une personne ayant auparavant oeuvré ailleurs auprès d'un autre professionnel ou au sein d'une autre société doit prendre les moyens raisonnables pour que cette personne ne lui révèle pas les confidences des clients de cet autre professionnel ou société. [Nous soulignons]

Par ailleurs, l'article 2138 C.c.Q. ajoute que le mandataire doit « dans l'exécution de son mandat, agir avec prudence et diligence » ce qui milite également en faveur d'un argument que l'avocat ne serait tenu qu'à une obligation de moyens[26].

Il semble que la question de l'intensité de l'obligation de l'avocat relativement au secret professionnel n'ait pas encore été définitivement tranchée par la jurisprudence. Chose certaine, cependant, le fait pour un avocat de divulguer une information protégée par le secret professionnel sans autorisation de la loi ou du client constitue une faute à la fois civile et disciplinaire[27] :

> **2-136** — *Secret professionnel* — L'avocat, comme tout autre professionnel, doit aussi respecter les confidences reçues de son client […]. La violation du secret professionnel est une faute civile entraînant sa responsabilité. En raison probablement de la modicité des sommes pouvant être obtenues, les recours civils sont rares. Le recours le plus souvent employé est la citation en discipline. [Notes infrapaginales omises, nous soulignons]

L'avocat qui utilise le courriel devrait donc être au courant des risques associés à son utilisation…

3. Les principaux risques associés à l'envoi de courriels

Quels sont ces risques qui sont associés à la transmission de documents confidentiels par courriels? Sur cette question, les auteurs consultés ne s'entendent pas. Certains sont d'avis que les risques d'interception ou de divulgation des courriels sont énormes mais d'autres pensent qu'ils ne sont pas aussi importants qu'on le pense généralement.

---

25 Jean-Louis BAUDOUIN et Patrice DESLAURIERS, La responsabilité du conseiller juridique dans *La responsabilité civile, Volume II - La responsabilité professionnelle*, 7e édition, 2007, para 2-115.

26 Robert CASSIUS DE LINVAL, préc., note 22, p. 2 de la version informatisée. L'auteur cite par erreur, semble-t-il l'article 2828 C.c.Q.

27 Jean-Louis BAUDOUIN et Patrice DESLAURIERS, préc., note 25.

Tout cela est difficile à départager pour un avocat dont l'expertise est souvent très éloignée du domaine des technologies. Il semble toutefois que la plupart des auteurs s'entendent pour dire que le courriel qui circule en réseau fermé (*local area Networks (LANs)* est relativement bien protégé parce qu'il ne sort pas du réseau et n'est accessible que par des personnes autorisées[28].

Les principaux risques d'interception concernent les courriels confidentiels qui sont acheminés sur Internet. Or, c'est le cas de la plupart des courriels échangés par les avocats et leurs clients. Le principal risque est que, entre le destinataire et l'expéditeur, le message est transmis d'un ordinateur intermédiaire à l'autre et qu'à chaque fois il est copié sur chaque ordinateur intermédiaire avant d'être retransmis. Le message peut donc être intercepté chemin faisant sur chacun de ces ordinateurs intermédiaires ou même par un fournisseur d'accès internet[29] :

> An Internet e-mail message could be intercepted while it is temporarily stored in one of those intermediate computers. Perhaps even more significant is the fact that an Internet provider may intercept, disclose or use e-mail sent through its system to the extent necessary to render the service or protect its rights.

Un courriel non chiffré qui est envoyé par le biais d'Internet est donc, en quelque sorte, une carte postale donc le contenu peut être divulgué à toute personne qui le capte au passage[30] :

> Si la transmission par télécopieur a déjà été qualifiée de courrier décacheté puisqu'à chaque extrémité de la transmission, plusieurs personnes peuvent prendre connaissance du message, que penser du courrier électronique. À la différence du fax qui utilise habituellement une ligne de transmission privée, le courrier électronique, circule "à ciel ouvert", au vu et au su de quiconque parmi les millions de branchés voudra bien se donner la peine de capter au passage n'importe quel message lancé sur cette autoroute électronique. En ce sens, ne peut-on pas qualifier ces messages de cartes postales électroniques que tout un chacun peut lire n'importe où sur le réseau et n'importe quand entre le moment de leur expédition et celui de leur réception?
>
> Pour les juristes, avocats ou notaires, ces caractéristiques du courrier électroniques sont lourdes de conséquences. Soumis à de strictes et lourdes obligations en matière de protection des confidences données par le client - identifié comme le sacro-saint « secret professionnel » - le professionnel du droit peut-il se permettre l'utilisation d'un outil de communication qui, en apparence, offre aussi peu de garanties de confidentialité? [Note infrapaginale omise, nous soulignons]

Ces risques d'interception et de divulgation ne sont cependant peut-être pas si importants qu'on pourrait le croire. La *Law Society of United Kingdom* a identifié trois menaces à la sécurité des courriels. La menace de loin la plus fréquente est l'envoi d'un

---

28 Martine BOURET et Troy HARRISON, préc., note 6, p. 32. Voir aussi David HRICIK et Amy FALKINGHAM, « Lawyers Still Worry Too Much about Transmitting E-Mail over the Internet », (2005) Amy, 10 J. Tech. L. & Pol'y 265, p. 270

29 Martine BOURET et Troy HARRISON, préc., note 6, p. 33.

30 Robert CASSIUS DE LINVAL, préc., note 22.

courriel à la mauvaise personne par inadvertance. Ensuite, beaucoup moins probables mais techniquement possibles, sont les risques de mauvais acheminement technique du courriel ou d'interception par un tiers. De plus, il semble qu'en pratique les menaces proviennent bien plus souvent qu'autrement de l'intérieur et non pas de l'extérieur des bureaux d'avocats[31].

Certains auteurs soutiennent également qu'il ne serait pas si facile pour un tiers d'intercepter un courriel sur Internet[32] mais une autre affirme exactement le contraire[33]!

4. Le chiffrement des courriels confidentiels est-il obligatoire?

Au Québec, il y a une absence complète de jurisprudence sur l'article 34 LCJTI. Le Barreau du Québec est d'avis que le chiffrement des courriels n'est pas obligatoire mais le recommande lorsque les renseignements qu'ils contiennent sont hautement confidentiels.

Pour vérifier à quel point cette solution satisfait toujours aux exigences de l'article 34 de la Loi, nous examinerons brièvement ce qu'est le chiffrement, l'évolution de la doctrine sur cette question au Québec et dans d'autres États voisins.

4.1. Qu'est-ce que le chiffrement?

Un des moyens le plus souvent mentionné pour protéger la confidentialité des courriels des avocats est le chiffrement. Cette technologie a pour but de « rendre indéchiffrable des données pour les personnes qui ne disposent pas de la clé permettant de les lire »[34]. Ainsi, lorsqu'un courriel est chiffré, personne d'autre que le véritable destinataire ne peut en prendre connaissance[35]. Le chiffrement est donc utile, même s'il n'est pas parfaitement efficace, pour démontrer une volonté de préserver la confidentialité d'une information, pour contourner les problèmes de divulgation involontaire et pour éviter qu'un tiers prenne connaissance de cette information[36].

L'efficacité du chiffrement dépend toutefois de plusieurs facteurs. Des auteurs américains réfèrent aux propos d'un expert en la matière qui a conclu que le chiffrement n'est pas une panacée parce que son degré de protection varie grandement en fonction de plusieurs facteurs : « *weak algorithms, poor implementations of good algorithms or*

---

31 Law Society of United Kingdom, *The Law Society E-mail Guidelines for Solicitors,* Annexe B « E-mail security, » novembre 2005, p. 16. En ligne : www.lawsociety.org.uk/documents/downloads/emailguidelines.pdf.

32 David HRICIK et Amy FALKINGHAM, préc., note 28, p. 278-279.

33 Audrey JORDAN, « Does Unencrypted E-Mail Protect Client Confidentiality? », (2004) 27 *Am. J. Trial Advoc.* 623, p. 628.

34 Robert CASSIUS DE LINVAL, préc., note 23, p. 176.

35 Martine BOURET et Troy HARRISON, préc., note 6, p. 40.

36 *Id.*, p. 40-41.

poorly administered deployments of even robust products are equally hollow in their promises of protection.»[37]

4.2. Le Québec

4.2.1. La situation antérieure à l'entrée en vigueur de l'article 34 LCJTI

Bien avant l'adoption de la LCJTI, la question de la nécessité de la cryptographie des courriels des juristes faisait l'objet de diverses études. À titre d'exemple, en 1998, Robert Cassius de Linval expliquait qu'il était difficile d'évaluer les risques qu'un courriel tombe entre de mauvaises mains. Il identifiait deux obstacles à la généralisation de l'utilisation de la cryptographie : 1) la difficulté d'utilisation et la lenteur des logiciels de cryptographie et 2) le fait qu'en l'absence de norme répandue, le juriste ait à acheter plusieurs logiciels pour pouvoir être compatibles avec ceux de ses clients. Il concluait toutefois qu'« un minimum de protection pour le contenu du message semble approprié et sage. »[38].

Dans un autre article publié la même année, le même auteur mentionnait que « le chiffrement des courriels devrait toujours être utilisé lorsque l'information est hautement confidentielle »[39]. En dépit du manque de convivialité des logiciels de chiffrement, l'auteur se demandait si celui-ci n'était pas déjà obligatoire mais convenait que l'avocat prudent et diligent ne manquait pas à son devoir si un accident se produisait et qu'un courriel était intercepté[40].

Les *Bulletins Prévention* du Fonds d'assurance responsabilité du Barreau du Québec (ci-après « **Fonds** ») ont également abordé la question de l'utilisation des courriels à quelques reprises[41]. En mars 2000, un *Bulletin Prévention* déconseillait l'utilisation du courrier électronique dans les cas où des dommages pourraient résulter du fait que le courriel tombe entre les mains d'un tiers[42] :

> **8.** Ne pas utiliser le courrier électronique si l'information que contient le message peut être dommageable si elle tombe dans les mains d'un tiers. L'un des critères pouvant être utilisé est de s'interroger : «Est-ce de l'information qui pourrait être transmise par télécopieur?» Si la réponse à cette question est négative, il faut en conclure que le courrier électronique ne doit pas non plus être utilisé.

---

37 Bill PIATT et Paula DEWITTE, « Loose Lips Sink Attorney-Client Ships: Unintended Technological Disclosure of Confidential Communications », (2007-2008) 39 St. Mary's L.J. 781, p. 814

38 Robert CASSIUS DE LINVAL, préc., note 22 (p. 4 de la version informatisée).

39 Robert CASSIUS DE LINVAL, préc., note 23, p. 175.

40 *Id.*, p. 176

41 Un avis au bas de tous les bulletins Prévention indique qu'ils ne doivent pas être interprétés comme « suggérant des standards de conduite professionnelle. ».

42 « Faire usage du courrier électronique », texte adapté en partie de : *E-mail Guidelines for Law Firms, ISBA Mutual Bulletin, Summer, 1999, Vol. 10, no. 1,* et publié dans *Bulletin de prévention du Fonds d'assurance responsabilité du Barreau du Québec*, mars 2000, vol 1. No 2, p. 3. En ligne www.assurance-barreau.com/fr/pdf/bullPrevMars2000.pdf

Dans cet article, le Fonds rappelait que le Barreau n'avait pas encore pris une position officielle quant à l'usage du courrier électronique, mais que les barreaux de plusieurs États américains l'avaient fait. Ces avis étaient généralement conformes à celui de l'*American Bar Association* (« **ABA** »), du 6 mai 1999, lequel mentionne que « la transmission d'information, même confidentielle, par Internet est une forme acceptable de communication. »[43].

Par la suite en septembre 2001, le Fonds a abordé plus particulièrement la question du chiffrement des courriels. Il a rappelé que, dans son avis de 1999, l'ABA avait jugé que : « l'envoi de messages non cryptés ne constituait pas un manquement au devoir de confidentialité. On y recommande toutefois d'utiliser la cryptographie lorsque la teneur du message le justifie. »[44]. Au Canada seul le Barreau de l'Alberta avait pris position sur l'utilisation du courriel par les avocats dans le cadre de leurs relations avec leurs clients. On y avait décidé « que le seul fait de ne pas avoir crypté la communication ne constitue pas une faute. »[45].

Le Fonds a rappelé qu'« [à] ce jour, aucun avis n'émane officiellement du Barreau du Québec. »[46] mais qu'il est suggéré aux avocats de « crypter les messages hautement confidentiels »[47].

Paradoxalement, dans ce même bulletin, le Fonds recommandait l'adoption d'une politique d'utilisation des équipements informatiques dans les bureaux d'avocats qui énonçait que le courriel ne devait pas être utilisé pour transmettre de l'information confidentielle[48]!

4.2.2. La situation postérieure à l'entrée en vigueur de l'article 34 LCJTI

Le *Bulletin de prévention* d'avril 2002 explique que les obligations des avocats en regard du chiffrement de leurs courriels auraient changé avec l'adoption du nouvel article 34 LJTI[49]. Cet article créerait une obligation de moyens : « [p]uisque la Loi utilise l'expression « moyen approprié » et puisque, en matière de protection de données, la

---

43 *Id.*

44 A.B.A. Standing Committee on Ethics and Professional Responsibility, Formal Opinion No. 99-413, disponible à www.abanet.org/cpr/nosearch/99_413.pdf. *Bulletin de Prévention du Fonds d'assurance responsabilité du Barreau du Québec*, Édition spéciale n° 3, septembre 2001, p. 3. En ligne : www.assurance-barreau.com/fr/pdf/bullPrevSept2001.pdf

45 *Bulletin de Prévention du Fonds d'assurance responsabilité du Barreau du Québec*, Édition spéciale n° 3, septembre 2001, p. 3. Voir http://www.assurance-barreau.com/fr/pdf/bullPrevSept2001.pdf. Le Fonds réfère à «*Guidelines on Ethics and the New Technology – Part III*» disponible à www.lawsocietyalberta.com

46 *Bulletin de Prévention du Fonds d'assurance responsabilité du Barreau du Québec*, préc., note 44, p. 3.

47 *Id.*, p. 3.

48 *Id.*, p. 4.

49 Claude MARSEILLE, préc., note 5.

sécurité absolue n'existe pas, on peut croire que les tribunaux interpréteront cette obligation comme une obligation de moyens. »[50].

La LCJTI ne définit cependant pas quel est ce « moyen approprié ». Le gouvernement est habilité en vertu de cette loi à édicter des normes, mais à ce jour, le comité multidisciplinaire qui devait réglementer ce domaine n'a pas encore été mis en place[51]. Il faut donc examiner les différentes options qui s'offrent à l'avocat pour décider quels est le « moyen approprié » à l'article 34 LCJTI.

Dans un premier temps, il semble que l'absence de toute mesure de sécurité ne serait plus acceptable étant donné le libellé de l'article 34 LCJTI[52] :

> […] il faut présumer que le législateur ne parle pas pour ne rien dire, et toute disposition d'une loi est réputée imposer des obligations. Face au libellé de l'article 34, il semble difficile de soutenir que l'absence de toute mesure de protection d'un courriel contenant des renseignements protégés par le secret professionnel satisfait à l'obligation qu'elle impose; [Note de bas de page omise, nous soulignons]

Un simple avertissement que le courriel contient de l'information confidentielle mais que le courriel n'est pas protégé ne satisferait pas non plus aux exigences du nouvel article 34 :

> [….] Un tel avertissement avise peut-être le récipiendaire du caractère confidentiel du courriel, mais il semble difficile de soutenir qu'il s'agisse là d'un moyen qui permette d'en protéger la confidentialité, tel que requis par l'article 34 de la Loi[53];

L'utilisation d'un mot de passe pour pouvoir ouvrir un fichier attaché à un courriel serait un moyen susceptible de rencontrer les exigences de l'article 34 de la Loi mais cette protection n'offre pas la même protection que le chiffrement du courriel[54]. Cette méthode et l'utilisation de réseaux fermés et sécuritaires seraient par contre entièrement satisfaisantes[55]. En ce qui concerne plus particulièrement le chiffrement des courriels, le bulletin conclut comme suit :

> Il s'agit de la solution la plus efficace dans un contexte de réseau ouvert comme le Web. Différents logiciels de chiffrement sont disponibles sur le marché. Notons le service offert par Postes Canada, «PosteCS» […] De telles mesures de chiffrement, conformes aux standards actuels (algorithme à 128 bits, etc.), sont indubitablement suffisantes, selon nous, pour satisfaire le critère de l'article 34 de la Loi; [Nous soulignons]

En pratique, il semble que les problèmes se règlent souvent par la renonciation du client qui autorise l'avocat à communiquer avec lui par un simple courriel non chiffré. En

---

50 *Id.*, p. 2.
51 *Id.*
52 *Id.* L'auteur réfère à l'article 41 de la *Loi sur l'interprétation*, L.R.Q. c. I-16.
53 *Id.* p. 2.
54 *Id.*
55 *Id.*, p. 2-3.

effet, le client étant le bénéficiaire du secret professionnel, il peut y renoncer[56]. Ainsi, le bulletin conclut que « le client peut autoriser son avocat à utiliser le courriel non sécurisé pour communiquer avec lui, même pour des renseignements couverts par le secret professionnel. »[57]. L'autorisation du client pourrait même être implicite mais la réponse à cette question variera selon les circonstances de chaque espèce. Il serait donc préférable d'obtenir une renonciation expresse du client et d'obtenir une autorisation expresse dans la lettre mandat initial[58].

Dans un autre texte paru en 2002[59], M[e] Tétrault ajoutait plus de précisions sur la position de l'ABA concernant l'utilisation des courriels par les avocats. L'ABA a énoncé un test en trois volets pour déterminer si un avocat se conforme à son obligation de confidentialité en utilisant un mode de transmission de l'information. Ce test implique : 1) une analyse des standards reconnus 2) une analyse comparative du risque d'interception et 3) une vérification des risques associés à une divulgation non autorisée de même que des lois qui concernent l'interception d'information :

> Le test proposé par l'Association du Barreau américain, quant à savoir s'il y a respect du devoir de confidentialité concernant le mode de transmission d'information, comporte trois éléments:
>
> 1. Il faut analyser les standards reconnus par la profession en ce qui a trait à la protection de communications visées par le secret professionnel;
>
> 2. Il faut comparer le risque d'interception d'information non encryptée avec le risque d'interception d'autres outils de communication;
>
> 3. Il faut vérifier les différentes formes de transmission par ce mode de communication et les risques qui sont associés à une divulgation non autorisée de même que des lois qui visent l'interception d'information.

Appliquant ce test, l'ABA a conclu que l'utilisation des courriels, même non chiffrés, ne pose pas plus de risques d'interception que les autres moyens de communication habituellement utilisés par les avocats et pour lesquels on reconnaît une expectative raisonnable de confidentialité[60] :

> L'Association du Barreau américain indique que les courriels, même ceux qui ne font pas l'objet d'un encryptage, ne posent pas plus de risques d'interception ou de

---

56 Voir articles précités, note 19.

57 Claude MARSEILLE, préc., note 5, p. 3.

58 *Id.*

59 Michel TÉTRAULT, « Le praticien et les technologies de l'information : le silence est d'or », dans Service de la formation permanente, Barreau du Québec, vol. 176, *Développements récents en droit familial*, Cowansville, Éditions Yvon Blais, 2002, p. 35. EYB2002DEV247.

60 *Id.*, M[e] Tétrault mentionne en note de bas de page no 105 que l'ABA considère que la poste, le téléphone et le télécopieur seraient des modes de transmission qui respecteraient l'obligation de confidentialité des avocats. Par contre, le téléphone sans fil et le téléphone cellulaire seraient plus risqués que le courriel.

> divulgation que les autres modes de communication communément utilisés par les procureurs et pour lesquels on reconnaît une expectative raisonnable de confidentialité. La protection légale qui est accordée au courriel, comme celle accordée à d'autres modes de communication électronique, vient appuyer cette « raisonnabilité » quant à l'expectative de confidentialité du courriel. Les risques d'une interception non autorisée ou d'une divulgation existent dans presque tous les modes de communication utilisés, incluant le courriel.
>
> Toutefois, il n'est pas raisonnable d'exiger qu'un mode de communication soit éliminé tout simplement parce que l'interception est technologiquement possible, plus particulièrement si cette interception non autorisée peut constituer un acte criminel.
>
> L'Association conclut que compte tenu de la technologie existante et des lois qui la régissent, un procureur qui achemine de l'information visée par le secret professionnel par courriel non encrypté ne contrevient pas à son obligation de confidentialité.
>
> Par ailleurs, comme c'est le cas pour tout type de communication visant de l'information protégée par le secret professionnel, ceci n'a pas pour effet de diminuer l'obligation de l'avocat de considérer avec son client l'importance et les conséquences de la communication et de faire le choix le plus avisé possible quant à son mode de communication. [Notes de bas de page omises, nous soulignons]

Au Québec, l'avocat pourrait invoquer l'article 2858 C.c.Q. qui permet au tribunal de rejeter tout élément de preuve qui a été obtenu dans des conditions qui portent atteinte aux droits fondamentaux, comme le droit au secret professionnel. Les avocats devraient cependant prendre des mesures pour éviter qu'une information confidentielle devienne accessible : « Présentement l'encryptage n'est pas une condition *sine qua non* pour que l'avocat respecte son obligation de confidentialité. ». Par contre, certaines « précautions minimales » doivent être prises, dont l'utilisation d'un mot de passe et le cryptage des « messages hautement confidentiels ». L'auteur ajoute que [c]es mesures visent tant le courriel que les documents joints.»[61]. M[e] Tétrault conclut qu'il est cependant « trop tôt pour répondre avec certitude de l'aspect « confidentiel » des échanges d'informations par courriel. »

Dans un autre texte paru en 2002 et portant sur la protection des renseignements personnels dans le contexte du commerce électronique, M[e] Raymond Doray écrivait que l'article 34 LCJTI imposerait pratiquement une obligation de garantie aux entreprises qui font du commerce électronique[62] :

> Implicitement, cette disposition impose aux entreprises qui effectuent des transactions par voie électronique de prendre les moyens nécessaires pour garantir la sécurité des moyens de transmission et des réseaux de communication utilisés. Dans l'état actuel de la technologie, nous serions enclins à penser que cette obligation implique la mise en place de systèmes de codage ou autres moyens de sécurité visant à empêcher que des

---

61 *Id.*

62 Raymond DORAY, « Le respect de la vie privée et la protection des renseignements personnels dans un contexte de commerce électronique.», dans *Droit du commerce électronique*, Montréal, Thémis, 2002, p. 303-361, à la p. 359.

> tiers puissent prendre connaissance illégalement de renseignements personnels. [Nous soulignons]

Par la suite, dans le *Bulletin Prévention* de juillet 2005, 13 mesures ont été suggérées pour protéger les données informatisées dans un bureau d'avocats. Au sujet des courriels, il était conseillé aux avocats de les éviter[63]! Ce bulletin ajoutait que l'avocat et son personnel devaient « comprendre les dangers posés par le courriel et comment se servir de cet outil de façon sécuritaire » sans toutefois préciser les moyens qui devaient être mis en place pour préserver la confidentialité des courriels.

La Corporation des services du Barreau du Québec offre par ailleurs à ses membres de faire affaire avec le service de courriel sécurisé *Mail it safe*[64]. Il a d'ailleurs été recommandé aux avocats dans une Capsule déontologie du *Bref*[65] intitulée « Sécurisez l'envoi et la réception de courriels avec un logiciel comme *Mail it safe*, recommandé par la Corporation de services du Barreau »[66].

Au sujet de l'article 34 LCJTI, le *Guide de prévention en responsabilité professionnelle*[67] du Barreau du Québec paru en 2006 énonce que les avocats pourraient s'y conformer en utilisant un mot de passe, en utilisant un réseau fermé ou encore en chiffrant leurs courriels ce qui est présenté comme étant la solution la plus efficace. Le courriel non chiffré pourrait cependant être utilisé avec la permission du client seulement:

> Cette importante obligation de prendre les moyens appropriés pour assurer la confidentialité des transmissions effectuées, vise également les avocats. En effet, quotidiennement les avocats transmettent des documents que la Loi déclare confidentiels, car tenus au secret professionnel. La Loi n'identifie pas quels sont les moyens appropriés qu'il convient d'utiliser. Il pourrait s'agir de l'utilisation d'un mot de passe, de l'établissement d'un réseau fermé avec le client, ou encore du chiffrement de courriel, ce qui constitue certes la solution la plus efficace.
>
> L'avocat devrait donc convenir avec son client du mode de transmission qu'il entend utiliser, ainsi que des moyens qu'il prendra pour en assurer la confidentialité. Une clause appropriée lors du mandat initial pourrait dès lors s'imposer. Néanmoins, le

---

63 Daniel E. PINNINGTON, « Gestion de la sécurité et de la confidentialité des données informatisées dans un bureau d'avocat », dans *Bulletin de Prévention du Fonds d'assurance responsabilité du Barreau du Québec*, vol. 6, n° 3, juillet 2005, p. 5. : « 6. Soyez conscients des dangers du courriel et évitez-les ». En ligne www.assurance-barreau.com/fr/pdf/bullPrevJuillet2005.pdf

64 En ligne : www.barreau.qc.ca/avocats/services/personnels/index.html

65 « La confidentialité au Quotidien », Capsule INFO_DÉONTO publiées dans le cyberbulletin *Le Bref*. En ligne : http://www.barreau.qc.ca/avocats/meilleures-pratiques/info-deontologie/capsules/confidentialite.html

66 En ligne : www.csbq.ca/courriels_securises. Ce logiciel ne fait pourtant pas l'unanimité. Voir Vincent GAUTRAIS, « Contrat mailitsafe : pas si sûr », en ligne : www.gautrais.com/IMG/article_pdf/Contrat-mailitsafe-pas-si-sur.pdf et Dominique JAAR, « Mailitsafe à l'épreuve », en ligne : dominicjaar.blogspot.com/2007/07/mailitsafe-lpreuve.html.

67 Fonds d'assurance responsabilité professionnelle du Barreau du Québec, Octobre 2006, aux p. 13-14. En ligne www.assurance-barreau.com/fr/guide.html.

> client pourrait autoriser son avocat à utiliser le courriel non sécurisé pour communiquer avec lui, même pour des renseignements couverts par le secret professionnel.
>
> Évidemment, dans une telle situation, il est préférable pour l'avocat d'obtenir une autorisation expresse. […] [Nous soulignons]

Enfin, il semble que l'école du Barreau fasse peu de cas de l'article 34 LCJTI étant donné les autres dispositions législatives applicables en ce domaine. Dans la section D du livre du Barreau de 2008 portant sur « L'usage des nouvelles technologies et le devoir de confidentialité » des avocats, cet article est simplement cité et paraphrasé. On y conclut qu'« il va de soi » que l'article 34 LCTJI vise les avocats puisqu'il s'applique aux documents que la Loi déclare confidentiels et qui sont transmis au moyen d'Internet ou d'une autre technologie[68].

L'auteur de ce texte, M[e] Raymond Doray reprend plutôt les propos précités de M[e] De Linval selon lequel la sécurité absolue n'existe pas en matière de nouvelles technologies de l'information et selon lequel « le chiffrement des messages devrait toujours être utilisé lorsque l'information est hautement confidentielle. »[69]. M[e] Doray rappelle également la position de l'ABA selon laquelle « l'envoi de messages non chiffrés par courrier électronique ne constitue pas un manquement au devoir de confidentialité. L'avocat devrait cependant consulter son client et suivre ses instructions dans tous les cas où il doit lui transmettre des renseignements hautement confidentiels par voie électronique ».

M[e] Doray réfère ensuite à l'article 4.7 des *Principes énoncés dans la norme nationale du Canada intitulée Code type sur la protection des renseignements personnels*[70] qui est reproduite à l'annexe I de la loi fédérale sur la protection des renseignements personnels et les documents électroniques[71] et qui énonce ce qui suit[72] :

> « 4.7. Septième principe – Mesure de sécurité
>
> Les renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondant à leur degré de sensibilité.
>
> 4.7.1. Les mesures de sécurité doivent protéger les renseignements personnels contre la perte ou le vol ainsi que contre la consultation, la communication, la copie, l'utilisation ou la modification non autorisées. Les organisations doivent protéger les renseignements personnels quelle que soit la forme sous laquelle ils sont conservés.
>
> 4.7.2. La nature des mesures de sécurité variera en fonction du degré de sensibilité des renseignements personnels recueillis, de la quantité, de la répartition et du format des renseignements personnels ainsi que des méthodes de conservation. Les renseignements

---

68 Raymond DORAY, préc., note 16, p. 71.

69 *Id.*, p. 69.

70 CAN/CSA – Q830 – 96

71 *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, c. 5, sanctionnée le 13 avril 2000.

72 Raymond DORAY, préc., note 16, p. 70.

> plus sensibles devraient être mieux protégés. La notion de sensibilité est présentée à l'article 4.3.4.
>
> 4.7.3. Les méthodes de protection devraient comprendre :
>
> a) des moyens matériels, […]
>
> b) des mesures administratives […]; et
>
> c) des mesures techniques, par exemple l'usage de mots de passe et du chiffrement. […]
> [Nous soulignons]

Bien que ces règles ne s'appliquent qu'aux activités extraprovinciales des entreprises fédérales situées au Québec, M[e] Doray a jugé utile de les reproduire. Il nous semble, également qu'elles pourraient être utilisées comme grille d'analyse pour déterminer le « moyen approprié » pour protéger la confidentialité des renseignements transmis par courriels en vertu de l'article 34 LCJTI, à défaut d'autres indications à la LCJTI.

M[e] Doray conclut, à cet égard, qu'en raison des règles de protection des renseignements personnels, du secret professionnel et du devoir de discrétion de l'avocat, ce dernier et ses employés « doivent prendre des précautions lorsqu'ils utilisent les nouvelles technologies de l'information pour transmettre tout renseignement ou document relatif à leurs clients. »[73].

4.3. Le reste du Canada

4.3.1. Les provinces de *common law*

Tout comme les avocats québécois, les avocats des provinces de *common law* sont tenus à des obligations très strictes en matière de secret professionnel.

Une des premières autorités à s'être prononcée sur la question de l'utilisation des courriels par les avocats est le sous-comité sur la responsabilité professionnelle de la *Law Society of Alberta.* Ses « *guidelines* » ont par la suite été adoptées telles quelles ou avec des modifications mineures par la *Fédération des ordres professionnels de juristes du Canada*[74] ainsi que par les Barreaux de plusieurs provinces canadiennes[75] sauf le Québec et l'île du Prince Edouard[76].

Dans ces lignes directrices, après avoir rappelé le devoir de confidentialité des avocats il est écrit que « *3. A lawyer must take reasonable steps to ensure the*

---

[73] *Id.*, p. 70.

[74] *Guidelines on Ethics and New Technology,* novembre 1999. En ligne : www.flsc.ca/en/pdf/EthicsGuidelines.pdf

[75] Nous n'avons pu retracer les *guidelines* de la Nouvelle-Écosse.

[76] Cette province n'est pas mentionnée dans la liste du document de l'ABC et nous n'avons pas non plus retracé les *guidelines* sur le site web the la *Law Society of Prince Edward Island,*.

maintenance of confidentiality by all persons engaged or employed by the lawyer. »[77]. Il semble que la norme applicable soit celle que les autres avocats utilisent pour ces communications :

> A lawyer using electronic means of communication must ensure that communications with or about a client reflect the same care and concern for matters of privilege and confidentiality normally expected of a lawyer using any other form of communication. This would include e-mail, whether via the Internet, internal e-mail or otherwise, or the use of cellular telephones or fax machines to transmit confidential client information. [Nous soulignons]

Un avocat n'a toutefois pas l'obligation de chiffrer tout courriel confidentiel concernant son client. En fait, la position de la fédération semble calquée sur celle de l'ABA[78] puisqu'elle énonce ce qui suit :

> Second, while initially there seems to have been much debate on this topic, the better view today is that there is no basis to conclude that Internet communications are any less private than those using traditional land-line telephones. There does not seem to be a ready and apparent danger that e-mail is less confidential than fax machines or cellular telephones, so anyone using the Internet to communicate has a reasonable and justified expectation of privacy, and it cannot be said as a simple rule that a lawyer must encrypt anything that the lawyer believes the client would not want to read in the local newspaper.
>
> Third, lawyers communicating on the Internet without encrypting their transmissions do not violate the principle of confidentiality. While encryption makes theft or interception more difficult, even strong encryption can be technically defeated. The vulnerability to theft and interception therefore remains. However, in ordinary circumstances, a lawyer is not expected to anticipate the criminal activity of theft of solicitor-client communications on the Internet any more than mail theft. [Nous soulignons]

Il est ensuite rappelé aux avocats que l'utilisation d'outils électroniques est sujette à des interceptions ou des divulgations involontaires. Les avocats doivent demeurer raisonnablement conscients des risques d'interception et de divulgation par inadvertance des courriels et des moyens pour les minimiser. Les avocats doivent se tenir à jour raisonnablement au sujet de ces risques. Le chiffrement du courriel est par contre obligatoire lorsque l'intérêt du client le justifie[79] :

> A lawyer using such technologies must develop and maintain a reasonable awareness of the risks of interception or inadvertent disclosure of confidential messages and how they can be minimized.
>
> Encryption software is available and must be used, if electronic means of communication are used, for those confidences that may be so valuable or sensitive that it is in the client's interest to take the extraordinary step of encrypting to protect them. The challenge, as in so many ethical areas, is to recognize those extraordinary situations and exercise sound judgment in relation to them.

---

77 *Guidelines on Ethics and New Technology*, préc., note 74.
78 Michael GEIST, *Internet Law in Canada*, North York, Ontario, Captus Press, 2000, p. 703.
79 *Guidelines on Ethics and New Technology*, préc., note 74, « part 3 », p. 4.

> When using electronic means to communicate in confidence with clients or to transmit confidential messages regarding a client, a lawyer must:
>
> (1) develop and maintain an awareness of how technically best to minimize the risks of such communications being disclosed, discovered or intercepted;
>
> (2) use reasonably appropriate technical means to minimize such risks;
>
> (3) when the information is of extraordinary sensitivity, advise clients to use encryption software to communicate with their lawyer, and use such software;
>
> and
>
> (4) develop and maintain such law office management practices as offer reasonable protection against inadvertent discovery or disclosure of electronically transmitted confidential messages. [Nous soulignons]

Dans son chapitre intitulé « *Legal Services and the Internet* », Michael Geist réfère à la position prise par la *Law Society of Alberta* et souligne que cette position ne fait pas l'unanimité (« *some members of the legal profession remain unconvinced* ») sans toutefois identifier les opinions qui seraient en sens contraire[80].

En 2002-2003, des auteurs canadiens qui ont également étudié la question du chiffrement des courriels des avocats ont conclu que l'utilisation de cette technologie n'était pas encore répandue (« *widespread* »). Cependant, à mesure que cette technologie deviendra plus courante et facilement accessible, les avocats verront leurs obligations augmenter en faveur du chiffrement. Ces auteurs prédisent qu'il est de plus en plus probable, sinon inévitable, qu'un jour, un tribunal canadien conclura que le défaut de chiffrer un courriel constituera un comportement négligent[81] :

> These trends make the possibility that a court will eventually find negligence in the failure to encrypt increasingly likely and, arguably, inevitable. Indeed, there may be an adverse assumption that having chosen not to use encryption meant that a lawyer or client did not intend the communication to be confidential. Given the state of PKI this interpretation is likely some distance in the future. [Nous soulignons]

Il semble en effet que la pression en faveur du chiffrement des courriels soit de plus en plus forte, si on considère la position récente de l'Association du Barreau Canadien (« **ABC** ») sur la question.

4.3.2. L'Association du Barreau Canadien

Depuis septembre 2008, l'ABC recommande aux avocats de chiffrer leurs courriels confidentiels[82]. L'ABC rappelle d'abord que l'avocat a le devoir de garder le

---

80 Michael GEIST, préc., note 78, p. 703.

81 Martine BOURET et Troy HARRISON, préc., note 6, p. 41.

82 *Lignes directrices pour un exercice du droit conforme à la déontologie dans le cadre des nouvelles technologies de l'information*, septembre 2008. En ligne www.cba.org/abc/activities_f/pdf/guidelines-fr.pdf

secret le plus absolu sur ce qu'il a appris de son client[83]. Elle rappelle ensuite que l'avocat doit veiller à ce que les communications électroniques avec leurs clients se fassent en toute sécurité et que toutes les mesures raisonnables soient utilisées afin de réduire les risques de divulgation[84] :

> **Les pratiques exemplaires en matière de confidentialité**
>
> […] Les avocats doivent veiller à ce que toute communication électronique avec leurs clients ou au sujet de ceux-ci se fasse en toute sécurité et que des tiers non autorisés ne puissent y avoir accès. Lorsqu'ils transmettent des renseignements confidentiels à leurs clients ou au sujet de leurs clients, les avocats doivent utiliser toutes les mesures raisonnables qui s'imposent afin de réduire autant que possible les risques que ces renseignements ne soient dévoilés ou interceptés. Afin de déterminer s'ils doivent ou non utiliser un certain type de technologie de l'information pour transmettre des renseignements confidentiels à leurs clients ou au sujet de leurs clients, les avocats doivent évaluer la situation de différents points de vue. Quels sont les risques de divulgation ou d'interception par inadvertance liés à l'utilisation de cette technologie? Quelles seront les répercussions du choix de cette technologie à l'égard du client en termes de coûts, d'accessibilité et de facilité d'utilisation? […] [Nous soulignons]

L'ABC traite ensuite de la position de la Fédération des ordres professionnels de juristes du Canada précitée mais ajoute qu'en raison de l'évolution des technologies, tous les renseignements confidentiels envoyés par courriels (et non plus seulement les informations très délicates) devraient dorénavant être chiffrés[85] :

> **3. Le cryptage**
>
> **Les lignes directrices des ordres professionnels de juristes sur le cryptage**
>
> Les « Lignes directrices sur la déontologie et la nouvelle technologie » de la Fédération des ordres professionnels de juristes du Canada, qui ont été adoptées par un grand nombre d'ordres professionnels de juristes sous la forme dans laquelle elles ont été publiées ou sous une forme révisée (voir l'annexe 1, Les sources documentaires, 3 i)), conseillent aux avocats d'utiliser le cryptage lorsqu'il est question de renseignements « très délicats ». Toutefois, l'évolution des technologies et du droit permettent d'utiliser le cryptage pour protéger tous les renseignements confidentiels. Il s'agit d'une question qui est amenée à évoluer.
>
> […]
>
> **Les pratiques exemplaires en matière de cryptage**
>
> Il est donc recommandé aux avocats de prendre les mesures suivantes :
>
> • utiliser le cryptage pour protéger les renseignements confidentiels qui sont transmis par voie électronique (*p. ex.*, les courriels); […] [Nous soulignons]

---

83 *Id.*, p. 6.

84 *Id.*

85 *Id.*, p. 7.

L'ABC constate ensuite qu'une norme de chiffrement semble s'imposer pour les courriels, soit le *Pretty Good Privacy*[86] :

> Il y a diverses méthodes de cryptage, mais le « cryptage à clé publique » est une méthode courante et efficace de cryptage. OpenPGP est la norme de cryptage pour courriel la plus répandue. Les programmes GnuPG et PGP sont conformes à cette norme. [Nous soulignons]

4.4. Les États-Unis

Nous avons déjà exposé dans les sections précédentes la position de l'ABA qui a jugé en 1999 que les avocats n'étaient pas tenus de chiffrer leurs courriels pour satisfaire à leurs obligations de confidentialité.

Cette position a déjà fait l'objet de critiques par le passé[87] mais au moins deux auteurs américains continuent de soutenir cette position de l'ABA. Dans une publication datant de 2005, ils notent qu'aucun Barreau d'un État américain n'interdit actuellement à ses membres d'envoyer des courriels non chiffrés[88]. Étant donné qu'il est illégal d'intercepter un courriel et que ce n'est pas non plus une chose si facile à faire, les risques d'interception sont trop faibles pour obliger les avocats à chiffrer leurs courriels[89]. Ensuite, bien qu'un professionnel puisse commettre une faute en n'adoptant pas une pratique non-généralisée (ils donnent l'exemple de l'arrêt Hooper concernant l'utilisation d'une radio sur un bateau), la situation n'aurait pas encore atteint ce point de non-retour. Ce point ne sera pas franchi tant qu'il n'y aura pas une preuve démontrée de risques véritables et d'absence de protection juridique[90].

Certains écrits récents remettent cependant en question cette opinion[91] probablement en raison de la plus grande efficacité des nouveaux logiciels de chiffrements courants. Ceux-ci seraient également plus faciles à utiliser et moins dispendieux[92].

Ainsi, dans une publication récente sur le site web de l'ABA, l'auteur rappelait qu'à la suite de l'adoption de l'opinion formelle 99-413 par l'ABA, les comités d'éthique Barreaux de plusieurs États américains avaient conclu qu'il n'était pas nécessaire de

---

86 *Id.*, p. 35.

87 John Christopher ANDERSON, « Transmitting Legal Documents over the Internet : How to Protect Your Client and Yourself », (2001) 27 Rutgers Computer & Tech. L.J. 1 (2001)

88 David HRICIK et Amy FALKINGHAM, préc., note 28, p. 299.

89 *Id.*, p. 299.

90 *Id.*

91 Voir aussi Audrey JORDAN, préc., note 33, p. 628. L'auteur recommande le chiffrement de tout courriel confidentiel par un avocat.

92 Voir Joshua COLBURN, « Don't Read This If It's Not for You: The Legal Inadequacies of Modern Approaches to E-Mail Privacy », (2006-2007) L. 91 Minn. L. Rev. 241, p. 260.

chiffrer les courriels[93]. Cela dit, lorsqu'il a adopté cette règle en 1998, le Barreau de New York, par exemple, a averti ses membres que le jugement de l'avocat devait être raisonnable en fonction de la sensibilité des informations confidentielles et du risque d'interception propre à chaque cas particulier. Ses membres devaient également se tenir à jour quant à l'apparition de nouvelles technologies qui permettraient un jour de diminuer les risques à un coût relativement bas[94].

Or, dans cet article il est signalé que le logiciel Outlook 2003 offre la possibilité de chiffrer des courriels de façon très efficace[95] :

> […] Also, Microsoft Outlook has the capacity to encrypt e–mail using a process called Pretty Good Privacy (PGP). For example, in Outlook 2003 it can be found under Tools > Options > Security. It is useful to search Outlook's help file for "encryption" to obtain specific instructions for your version. The name of the technology actually understates its effectiveness. […]

Un autre auteur a récemment expliqué les différentes positions des Barreaux des États américain en les répartissant entre « *Weaker Security Model States* » qui on suivi la position de l'ABA et les « *Stronger Model States* »[96]. Les premiers ont tendance à imposer une plus grande responsabilité aux clients des avocats en matière de sécurité de l'information. A son avis, la position des seconds, bien que moins nombreux, « *is more technologically sound* »[97] parce qu'elle impose plutôt à l'avocat qui transmet des renseignements confidentiels sur Internet la responsabilité d'adopter des mesures proactives pour protéger cette confidentialité[98].

À son avis : « *[b]ecause of the frequency with which attorneys use e-mails that contain confidential information and the ease of configuring enhanced security, attorneys should be required to encrypt e-mails that contain confidential information.* »[99]. Il termine son article en ajoutant : « *it may be worth the slight configuration burden to enable some light form of encryption. Even light encryption would make an intercepting and reading e-mail more difficult*. »[100].

---

93 Steven MASUR, *Confidentiality in a High-Tech World,* American Bar Association General Practice, Solo & Small Firm Division, juillet-août 2007.

94 *Id.*

95 *Id.* Robert CASSIUS DE LINVAL, préc., note 23, p. 177 avait fait mention de ce logiciel de chiffrement à clé public disponible sur internet en 1998. Il avait cependant ajouté qu'il était cependant « impossible de parler d'un logiciel de chiffrement universellement reconnu ».

96 Ash MAYFIELD, préc., note 1, p. 566-569.

97 *Id.*, p. 570.

98 *Id.*, p. 552.

99 *Id.*, p. 570.

100 *Id.*, p. 602.

Il constate enfin que l'État de l'Oklahoma, un État modèle selon cet auteur, imposerait aux avocats l'obligation suivante (très similaire à l'article 34 LCJTI, nous semble-t-il)[101] :

> Oklahoma Rules of professional Conduct 16, Comment 17: « [w]hen transmitting a communication that included [confidential information], the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients ». [Nous soulignons]

Cette règle s'applique vraisemblablement aux courriers électroniques des avocats mais l'auteur ne précise pas si elle leur impose le chiffrement ou non. En fait, En fait, l'auteur conclut que la question des mesures précises de sécurité qui devraient être imposées aux avocats fasse partie des améliorations que ce Barreau devrait apporter à ses règles de conduite[102]!

Un autre auteur rapporte que les Barreaux des différents États américains ne modifieront probablement pas leurs exigences relativement au chiffrement des courriels tant que le chiffrement ne sera pas devenu une pratique généralisée. Or, cet état de chose serait sur le point de changer puisque presque le tiers des grands cabinets auraient déjà adopté le chiffrement de leurs courriels[103]. À son avis, un avocat prudent « *should thoroughly consider using encryption, especially for particularly sensitive communication* »[104].

Par ailleurs, d'autres auteurs rappellent que les avocats doivent prendre des mesures de sécurité raisonnables. Leurs obligations en matière de sécurité des données devraient varier en fonction de la grandeur des cabinets et de l'importance des dossiers traités[105]. En ce qui concerne le chiffrement des données confidentielles des bureaux d'avocats, « *there are no mandatory, industry-wide encryption standard* »[106]. Ces auteurs ajoutent en note de bas de page que « *Today a host of powerful encryption tools are readily available as open source programs* ». De plus, il semble qu'un algorithme aurait été adopté par le gouvernement fédéral américain en tant que *Advanced Encryption Standard (AES)* et serait devenu une norme *de facto* de l'industrie[107].

4.5. L'Angleterre

La *Law Society of United Kingdom* a adopté en 2005 les *E-Mail guidelines for solicitors* qui contiennent plusieurs indications intéressantes quant à la question de la sécurité des courriels. Tout d'abord, le Barreau du Royaume-Uni souligne l'importance

---

[101] *Id.*, p. 579.
[102] *Id.*, p. 582-583.
[103] Joshua COLBURN, préc., note 92., p. 261.
[104] *Id.*, p. 261.
[105] Bill PIATT et Paula DEWITTE, préc., note 37, p. 802- 803.
[106] *Id.*, p. 813.
[107] *Id.*, note de bas de page no 153.

d'adopter une politique écrite concernant les courriels[108]. Ensuite, elle recommande dorénavant aux cabinets de chiffrer automatiquement tous leurs courriels destinés à des personnes qui sont capables de les déchiffrer[109] :

> 8. Firms are recommended to adopt systems that:
>
> (a) provide the facility for retrieving (and automatically decrypting) encrypted incoming mail; and
>
> (b) automatically encrypt all outgoing e-mail to those offering similar facilities.
>
> […]
>
> 10. Firms should be aware that encryption software using strong cryptography is widely available, and that such software is available on the Internet free for non-commercial use. (This may enhance the willingness of clients to take advantage of it where use by the client would be non-commercial, as in most criminal, family and residential conveyancing cases). [Nous soulignons]

CONCLUSION

Il ressort de notre étude que l'obligation de chiffrer les courriels confidentiels s'impose de plus de plus dans les communautés juridiques nord-américaines et du Royaume-Uni. Depuis septembre 2008, l'ABC recommande le chiffrement de tous les courriels confidentiels des avocats et non plus seulement de ceux contenant des informations hautement sensibles. Cette recommandation aura sans doute des impacts au Québec puisqu'il serait étonnant que les cabinets pan-nationaux adoptent une politique différente pour leurs bureaux situés dans notre province.

Le Barreau du Royaume-Uni recommande également le chiffrement automatique des courriels des avocats destinés à des personnes qui sont en mesure de les déchiffrer. Aux États-Unis, la position de l'ABA selon laquelle l'avocat n'est pas tenu de chiffrer ses courriels confidentiels est de plus en plus critiquée par la doctrine récente. Il semble que ce changement d'opinion résulte du fait que les principaux obstacles à l'utilisation du chiffrement sont de moins en moins importants. Tout d'abord, les logiciels de chiffrement seraient plus faciles à utiliser. Ensuite, certaines normes semblent se dégager. Enfin, le coût de ces logiciels ne serait plus un obstacle au chiffrement, certains étant même disponibles gratuitement sur Internet. Le fait que le tiers des grands cabinets auraient déjà adopté le chiffrement de leurs courriels nous indique également qu'une tendance se dessine en faveur du chiffrement.

Au Québec, en l'absence de jurisprudence sur l'article 34 LCJTI, il est bien difficile de prévoir quelles sont les obligations des avocats quant à la confidentialité de

---

[108] Law Society of United Kingdom, préc., note 31.
[109] *Id.* Voir Annexe B, p. 17-18.

leurs courriels. Par contre, en raison du changement récent de position de l'ABC, il nous semble que le Barreau du Québec devrait réexaminer à nouveau cette question. Un « moyen approprié » aux termes de l'article 34 LCJTI est sûrement un moyen qui tient compte de l'évolution technologique. Or, tout indique que le chiffrement des courriels est sur le point de devenir une norme généralisée auprès des avocats nord-américains…