Le statut juridique du courriel au Canada et aux États-Unis

René PÉPIN(*)

***Lex Electronica*, vol. 6, n°2, Hiver / Winter 2001**

Synopsis

This essay examines the level of protection that North American justices have attributed to issues of privacy surrounding personal e-mail. The author takes a close look at the relevant jurisprudence from both Canadian and American Courts, while concentrating his efforts on analysing an employee's right to privacy and an employer's right to access personal email received on company terminals. While Canadian Courts try to fill the legislative void by underlining the differences and similarities between emails and more traditional means of communication that have already been subject to legislative control (i.e. the telephone and regular mail), American justices have taken a constitutional approach to the question in adapting their interpretation of the 4th amendment to the U.S. Constitution to this relatively new technology. They have also relied on the *Electronic Communications Privacy Act* of 1986, and the *Privacy Protection Act* of 1986, to establish the legal status of emails. Unfortunately, the author concludes that these efforts are not sufficient, for the actual legislation does not consider the true essence of emails.

Résumé

Cet article aborde le degré de protection en matière de vie privée accordé au courrier électronique par les tribunaux nord-américains. L'auteur dresse un portrait général de la jurisprudence canadienne et américaine actuellement disponible en la matière, en concentrant ses propos sur l'expectative de vie privée des employés ainsi que sur les droits de l'employeur d'accéder à leurs courriels dans un contexte de relations de travail. Alors que les tribunaux canadiens abordent la problématique en procédant par analogie, c'est-à-dire par comparaison du courriel avec des modes de communication plus traditionnels (i.e. le téléphone et le courrier), les tribunaux américains font une analyse interprétative du 4ème amendement de la constitution des États-Unis et des droits statutaires accordés par l'*Electronic Communications Privacy Act* de 1986 et le *Privacy Protection Act* de 1986. L'auteur précise que les dispositions législatives actuelles présentent d'importantes lacunes rendant difficile leur application aux courriels.

Table des matières

Introduction

1. Le courrier électronique, ou courriel, est l'un des services les plus répandus du réseau Internet. On calcule que, grâce à sa rapidité et son coût presque nul, il aura été utilisé en Amérique du Nord plus d'un milliard de fois cette année[2]. L'un des principaux problèmes juridiques qu'il soulève consiste à déterminer le degré de protection qui lui est applicable en matière de vie privée. Les utilisateurs sont-ils en droit de s'attendre à ce que leur courrier électronique, de par son statut juridique, soit protégé tout autant qu'une lettre confiée au service postal canadien ou qu'une conversation téléphonique[3] ? Aucune disposition législative ne répond parfaitement à cette question. Nous devrons donc nous tourner vers la jurisprudence pour déterminer le statut juridique qu'elle est prête à reconnaître au courrier électronique. Nous n'étudierons pas ici la question plus traditionnelle des protections que le droit civil offre à une personne dont des éléments de sa vie privée mentionnés dans un courriel auraient été révélés au grand jour par un tiers. Celle-ci a déjà fait l'objet d'études, certes peu nombreuses, mais excellentes[4].

2. Notre sujet se concentre plutôt sur les droits de la personne face à l'État et dans le contexte des relations de travail. Il s'agira plus précisément de répondre à la question suivante : jusqu'à quel point le statut juridique du courriel protège le citoyen contre la volonté de la police ou d'un employeur d'en fouiller le contenu ? Le problème est bien réel : dans une conférence prononcée à Sherbrooke en juin dernier, Me Ralph D. Farley, du bureau d'avocats *Heenan Blaikie*, rapporta les conclusions d'un sondage réalisé par l'*American Management Association* auprès de 2133 directeurs de ressources humaines dans des grandes entreprises. Il en ressort que 74% des employeurs passent en revue les courriels des employés, enregistrent leurs appels téléphoniques, surveillent leurs connexions à Internet ou consultent leurs fichiers informatiques[5] !

3. Les juges qui ont dû se prononcer sur cette question ont été confrontés au choix suivant : identifier le concept juridique traditionnel duquel le courriel se rapproche le plus et décréter un arrimage forcé, plus ou moins parfait, entre les deux ou proposer une règle de leur propre crû, totalement nouvelle. Voyons ce qu'il en est au Canada (I) et aux États-Unis (II).

I. Le statut juridique du courriel au Canada

Le statut juridique du courriel sera étudié à travers l'analyse des droits de la personne face à l'État (A) et dans ses relations de travail (B).

A. Les droits de la personne face à l'État

4. Il y a encore très peu de décisions au Canada sur notre sujet. Une affaire importante est cependant survenue en 1998, dans le cadre d'un litige devant les tribunaux de juridiction criminelle *: R.* c. *Weir*[6]. Il vaut la peine d'en rappeler brièvement les faits. L'accusé, un résidant de la province d'Alberta, se plaignit à la compagnie *Supernet*, son fournisseur d'accès, de difficultés pour accéder à son courrier électronique. Un employé diagnostiqua que le problème était dû à des « pièces jointes » trop nombreuses, et trop volumineuses. En effectuant son travail, il a ouvert un certain nombre de ces documents, et il découvrit qu'ils contenaient des images qui pouvaient être considérées comme de la pornographie impliquant des enfants. Il en avisa son employeur qui fit part de ses soupçons à la police. Celle-ci, après une première vérification des faits, obtint un mandat de perquisition en bonne et due forme et saisit 190 fichiers contenus sur des disquettes et dans l'unité centrale de l'ordinateur de M. Weir. Il fut accusé par la suite de possession de pornographie juvénile, laquelle contrevient à l'article 163.1 du Code criminel du Canada.

5. Lors du procès devant le juge Smith, de la *Alberta Court of Queen's Bench*[7], l'avocat de la défense souleva principalement des questions relatives aux libertés fondamentales. On prétendit que le fournisseur d'accès, de par son rôle, était un agent de l'État, ce qui signifiait que la *Charte canadienne des droits et libertés* lui était applicable, vu le libellé de son article 32. On contesta également les agissements de la police avant l'obtention du mandat de perquisition et l'on prétendit également qu'elle avait effectué une perquisition et une saisie abusives au sens de l'article 8 de la Charte. On plaida aussi violation de l'article 7, puisqu'il y a eu interception de courrier privé. Finalement, on avança que l'administration de la justice serait mal servie, au regard de l'article 24(2) de la Charte, si on admettait en preuve les fichiers saisis.

6. Le juge Smith décida que la Charte était applicable au litige du fait que la police avait effectué une saisie de documents. Il fallait donc se demander si la saisie avait été validement faite, compte tenu de son article 8 qui accorde une « expectative raisonnable » de vie privée[8]. Cette expectative dépend de ce qui est saisi et de l'endroit où la saisie est effectuée[9]. Les citoyens sont en droit de s'attendre au plus haut niveau de protection lorsqu'ils sont dans leur domicile. Cette attente du respect de la vie privée doit être atténuée lorsqu'une personne se trouve dans un autre contexte comme, par exemple, sur les lieux du travail, à l'aéroport ou en voiture. Le magistrat a donc dû étudier la question de savoir si le courrier électronique est porteur d'une expectative raisonnable de vie privée. On sait que

le droit canadien prévoit une excellente protection pour ce qui est du courrier et des appels téléphoniques[10]. Dans ces deux cas, la police doit avoir obtenu un mandat de perquisition après avoir convaincu un juge indépendant et impartial des motifs sérieux de croire qu'une telle perquisition apportera la preuve qu'une infraction criminelle a été commise ou est sur le point de l'être. Mais qu'en est-il du courrier électronique ?

7. Faute de texte législatif ou réglementaire à l'appui, le juge Smith fit un parallèle entre le courrier électronique, le courrier postal et les appels téléphoniques. S'appuyant sur la doctrine américaine[11], il établit les similitudes suivantes avec le courrier de première classe[12] : (a) les deux médiums établissent une communication écrite de personne à personne, (b) ils utilisent un système de boîte postale privée, (c) ils peuvent avoir un contenu très volumineux, (d) il y a un délai entre l'envoi, la réception et la réponse éventuelle du message, (e) le destinataire ne peut empêcher l'expéditeur d'effectuer son envoi, (f) le destinataire sait généralement qui est l'expéditeur par l'adresse de retour sur l'enveloppe ou l'en-tête du message, (g) le contenu des messages peut être facilement copié et ré-adressé, (h) les deux moyens de communication sont peu coûteux, (i) une fois la « mise à la poste » faite, le message ne peut être approprié à nouveau, (j) l'expéditeur ne sait pas immédiatement si son message va arriver à bonne destination et, (k) dans les deux cas on peut recevoir du courrier en vrac, non-sollicité, et qui peut être l'œuvre de fraudeurs.

8. Quant aux affinités possibles avec les appels téléphoniques[13], le juge nota les éléments suivants : (a) la technologie utilisée est très semblable, faisant appel le plus souvent aux lignes téléphoniques, (b) l'expéditeur n'a pas à quitter son foyer pour « poster » son envoi, (c) ce médium peut être utilisé plusieurs fois par jour, (d) le message n'a pas besoin, pour être livré, de l'intervention humaine, et (e) les deux médiums permettent des échanges quasi-simultanés.

9. Le courriel possède aussi ses caractéristiques propres[14] : c'est peut-être le moyen de communication le moins dispendieux, le message peut être envoyé anonymement et il est très facile, grâce à la technologie, d'y répondre.

10. Le juge n'a pas eu à trancher la question de savoir si le statut juridique du courriel s'apparentait davantage à une lettre qu'à un appel téléphonique, puisqu'il conclut que, manifestement, il comportait une certaine expectative d'intimité. La police avait donc besoin d'un mandat pour effectuer une perquisition et une saisie. Cependant, il précisa sa pensée au sujet du statut juridique du courriel lorsqu'il est sous contrôle du fournisseur d'accès en faisant une distinction importante entre les trois éléments suivants[15] : le « titre » du message, c'est à dire l'annonce dans une boîte de courrier électronique qu'un message a été reçu et l'indication de sa provenance, le message lui-même, qui peut être lu à l'écran quand on l'ouvre électroniquement, et la ou les pièces jointes. À son avis, le titre du message et son contenu sont tels qu'ils ne peuvent être assimilés parfaitement au courrier postal puisque la technologie actuelle permet trop facilement l'interception et la lecture de ce message par un grand nombre de personnes. Pour qu'on puisse parler d'un niveau de sécurité vraiment semblable au courrier postal, il faudrait qu'un courriel soit encrypté.

11. Le juge conclut que les citoyens ont une expectative raisonnable de vie privée en utilisant le courriel, mais que la technologie actuelle fait qu'elle doit être moindre que pour le courrier postal. Cependant, cette vulnérabilité du courriel constitue en quelque sorte sa force, puisque, pour le protéger, le juge décida que l'État a besoin de l'autorisation d'un juge avant d'effectuer une saisie[16].

B. Les droits de la personne dans les relations de travail

12. Il n'est plus question, dans le domaine des relations de travail dans le secteur privé, de conflit possible avec l'État. La situation est donc différente. Il y a encore peu de jurisprudence sur le sujet mais, à l'heure actuelle, elle est très défavorable aux employés. Ces derniers doivent considérer que, sauf situation exceptionnelle, leurs courriels, comme l'ensemble des outils de production mis à leur disposition par l'employeur, peuvent impunément être consultés par leur patron sans que celui-ci n'ait à justifier une crainte d'utilisation frauduleuse.

13. Les tribunaux ont jugé que les employés n'ont pas d'expectative raisonnable de vie privée au niveau du courriel[17]. Ils ont établi une distinction importante avec les appels téléphoniques : une fois composé ou lu, le courriel est « déposé » dans un dossier appartenant à l'employeur. Celui-ci peut donc le consulter, comme il peut le faire pour tout document se trouvant dans un classeur en métal. Bien sûr, il ne peut vérifier les effets tout à fait personnels de l'employé sans motif particulier, comme ses vêtements ou ses aliments, ni exiger un échantillon de salive ou d'urine. C'est la limite que l'employeur ne peut franchir. Les arbitres de griefs, devant qui ces litiges se plaident pour la plupart, estiment que le droit de l'employeur émane des termes de la convention collective ou, plus généralement, de son droit de gérance[18].

14. Il se pourrait que le courriel soit légalement protégé, mais uniquement lorsqu'il est en transit. On pourrait alors prétendre qu'il s'agit d'une conversation privée, comme une conversation téléphonique, dont l'interception est interdite par les articles 184 et suivants du Code criminel. Cette disposition, dans son premier paragraphe, prévoit qu'est coupable d'un acte criminel « …*quiconque, au moyen d'un dispositif électromagnétique, acoustique, mécanique ou autre, intercepte volontairement une communication privée*. ». Comme il n'y a pas de jurisprudence spécifique sur cette question, l'employeur prudent n'a qu'à attendre, pour visionner les courriels, qu'ils se retrouvent dans le logiciel de courrier électronique de ses employés[19].

15. Le seul cas où les employés peuvent considérer que leurs courriels sont légalement protégés serait celui où l'employeur adopte une politique stipulant que les courriels sont confidentiels et qu'il ne les consultera pas sans motifs. Cependant, dans les entreprises où il existe une politique de l'employeur, les dispositions de celle-ci prévoient généralement le contraire.

II. Le statut juridique du courriel aux États-Unis

Nous étudierons tout d'abord l'application du 4ème amendement de la constitution des États-Unis aux courriers électroniques (A) avant d'analyser les protections accordées à la personne par le droit statutaire (B).

A. La protection constitutionnel des courriers électroniques

16. Relativement peu de décisions portent, aux États-Unis, sur la protection juridique du courrier électronique. Cela peut nous surprendre, lorsqu'on pense qu'il s'agit d'un pays dix fois plus peuplé que le Canada et où les citoyens ont la réputation de recourir aux tribunaux pour régler le moindre conflit juridique. Ce qui ne surprendra pas, par contre, c'est de voir que les tribunaux se sont lancés dans toutes sortes de distinctions et de nuances d'ordre constitutionnel lorsqu'il s'est agi d'appliquer le 4ème amendement de la constitution aux courriels.

17. La doctrine semble divisée sur le caractère suffisant des lois et de la constitution pour protéger la confidentialité du courriel. Certains sont d'avis qu'il suffirait que les juges interprètent plus généreusement les textes législatifs existants[20], mais d'autres, comme le professeur Laurence Tribe, de la Faculté de droit de l'Université Harvard, estiment nécessaire l'adoption d'un amendement constitutionnel spécifique pour protéger le caractère privé des communications faites par moyens électroniques[21].

18. Aussi, la limite du domaine d'application du quatrième amendement est-elle difficile à définir. C'est pourquoi nous traiterons des cas impliquant tantôt le secteur public, tantôt le secteur privé. En effet, une fouille effectuée par un employeur privé mettra tout de même en jeu le 4ème amendement s'il agit de connivence avec la police ou s'il a simplement l'intention d'aider les policiers dans leur travail[22]. La protection convoitée par les particuliers se trouve peut-être plutôt dans le droit statutaire américain, comme nous le verrons dans la seconde section de cette partie.

19. Tous s'entendent cependant pour affirmer que la protection juridique du courrier électronique se trouve, à la base, dans ce 4ème amendement de la constitution prévoyant le droit des citoyens « …*to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures*… ». Son libellé prévoit aussi qu'aucun mandat de perquisition ne doit être émis, sauf à la suite d'une demande faite sous serment à l'effet qu'il y a des motifs sérieux de croire qu'une offense a été commise. Le mandat doit décrire spécifiquement l'endroit à être perquisitionné et les personnes et choses à saisir[23].

20. En 1967, la *Cour suprême des États-Unis*, dans *Katz* c. *U.S.*[24] a reconnu que le 4ème amendement protégeait autant les choses intangibles, comme des conversations téléphoniques, que les choses tangibles. Elle a aussi réaffirmé le principe que cette disposition reconnaît généralement aux citoyens une expectative raisonnable de vie privée. À ce sujet, le juge Harlan a formulé la règle suivante, qui n'a jamais été modifiée : pour qu'une expectative de vie privée soit raisonnable, il faut qu'elle satisfasse à deux critères. Tout d'abord, la personne concernée doit véritablement croire que le moyen qu'elle utilise pour communiquer ses pensées bénéficie de la protection de la loi. Ensuite, il faut que cette perception soit considérée comme raisonnable par le reste de la société[25]. Le critère

retenu a donc un élément subjectif et un élément objectif. On comprend que la seconde partie du critère laisse en réalité une grande latitude aux tribunaux. Ces derniers doivent déterminer, si, dans tel ou tel cas, la société estime qu'un moyen de communication donné mérite une protection juridique. Il ne s'agit donc pas vraiment d'une norme objective. Une juge ne peut certes pas appliquer sa propre perception des choses, il est cependant amené, ici, à devoir appliquer ce qu'il perçoit être le consensus social existant à un moment donné.

21.Au niveau des grands énoncés de principes, la jurisprudence américaine considère que le courrier électronique bénéficie d'une importante protection juridique dans la mesure où il est susceptible de contenir des informations très personnelles. Dans l'affaire *Chan*[26], on a fait une analogie entre les données se trouvant dans un ordinateur et les objets se trouvant dans un « *closed container* », c'est à dire un contenant hermétiquement fermé, que la loi protège fortement, puisqu'il est susceptible de contenir des renseignements personnels. Sont visés par ce concept jurisprudentiel : un casier métallique où un employé range ses vêtements, une boîte à lunch, un sac à main ou un porte-documents. D'autres juges ont établi un lien conceptuel entre les ordinateurs et une filière[27]. Tout comme une filière qui contiendrait des dizaines et des dizaines de dossiers, un ordinateur ne pourra faire l'objet d'une perquisition qu'à la suite de l'obtention d'un mandat en bonne et due forme, précisant l'objet de la fouille et saisie éventuelle.

22. Il a également été dit qu'un ordinateur personnel situé ailleurs que chez soi pouvait toujours bénéficier de la protection juridique accordée aux « *closed containers* ». En outre, il suffit que l'utilisateur de l'ordinateur en ait la possession pour bénéficier des protections légales. Il n'est donc pas nécessaire qu'il en soit le propriétaire[28]. Selon l'arrêt *Katz*, le 4ème amendement protège aussi les ordinateurs des intrusions effectuées à distance, tout autant que les intrusions « physiques ». Dans cet arrêt, le gouvernement américain plaida qu'il n'y avait pas eu intrusion physique dans la cabine téléphonique où se trouvait l'accusé lorsqu'on avait capté ses conversations téléphoniques[29].

23. La décision *Maxwell*[30], rendue par un tribunal militaire, est l'une des quelques décisions où un juge, comme dans l'affaire *Weir* au Canada, a tenté d'établir un parallèle entre le courrier électronique et les autres moyens de communication que sont la poste ou le téléphone. Ici, un colonel de l'armée américaine se trouvait mêlé à une affaire de pornographie juvénile. Il possédait un ordinateur personnel qu'il avait lui-même acheté et qu'il utilisait uniquement à son domicile. Un résidant de la Californie s'était plaint aux médias, puis auprès des forces de police, du fait que des photos représentant de la pornographie juvénile circulaient sur le réseau Internet. L'enquête policière s'est concentrée sur le fournisseur d'accès *America On Line* (AOL) puis, plus spécifiquement, sur un groupe de 80 personnes auquel appartenait le colonel Maxwell. Comme la perquisition et la saisie ont été effectuées au bureau-chef de AOL, et non au domicile de Maxwell, s'est posée la question de savoir jusqu'à quel point il avait une expectative raisonnable de vie privée lorsqu'il utilisait le système de courrier électronique fourni par AOL.

24. Le juge Cox estima que l'accusé bénéficiait de cette expectative raisonnable de vie privée en se basant, d'une part, sur la ressemblance, du point de vue technologique, entre

le courriel et la conversation téléphonique et, d'autre part, sur les termes du contrat passé entre Maxwell et AOL. La politique clairement énoncée de la compagnie était de ne pas lire les courriels de ses clients, ni d'en dévoiler le contenu à d'autres personnes[31]. Le juge Cox a relevé également des ressemblances entre le courrier électronique et le courrier postal. Dans les deux cas, une fois le message « scellé » et envoyé, il ne devrait pas être intercepté par qui que ce soit. Seul le destinataire doit en principe en lire le contenu.

25. Des différences entre ces deux moyens de correspondances subsistent néanmoins. Dans le cas du courriel, le message est conservé dans la mémoire d'un ordinateur jusqu'à ce que le récipiendaire le télécharge sur son écran. Il y a donc plus de dangers qu'un employé de l'entreprise de télécommunications, du fournisseur d'accès ou du maître de site, lise le message, malgré les belles promesses faites à la clientèle. Il se peut aussi que le message soit éventuellement détruit si le destinataire ne l'ouvre pas pendant un certain délai.

26. Il existe un élément commun entre les courriels, les lettres et les conversations téléphoniques : une fois le message arrivé à destination, le récipiendaire peut très bien révéler impunément à d'autres la teneur de ce qu'il a lu ou entendu. Il n'y a pas de protection juridique contre un interlocuteur qui ne saurait garder un secret. Dans le contexte de l'électronique, ceci signifie que l'expectative de vie privée est quasiment réduite à néant lorsqu'une personne envoie des messages dans un forum de discussions ou lorsque le message initial est réadressé à plusieurs autres personnes.

27. La cour ordonna un nouveau procès pour le colonel Maxwell puisqu'il y avait eu violation de ses droits constitutionnels. Cependant, il faut retenir de cette affaire que les courriels envoyés dans un forum de discussions ou réadressés à un grand nombre de personnes ne bénéficient plus de la protection du 4ème amendement de la constitution américaine[32].

28. Les protections fournies par le 4ème amendement sont limitées par le libellé même du texte et par l'interprétation que les tribunaux en ont fait. Ces derniers ont élaboré deux concepts juridiques qui sont tout aussi applicables dans un environnement électronique que dans les autres domaines, soit la doctrine dite du « *plain view* » et la question du consentement à la saisie.

29. Selon la doctrine du « *plain view* », plus un document est laissé à la vue des gens de façon ostensible, moins son propriétaire peut prétendre à une expectative importante de vie privée[33]. À la limite, la police n'a plus besoin d'un mandat de perquisition dans de tels cas. Une question se pose avec acuité dans les cas où plusieurs employés se partagent des ordinateurs et où les fichiers de l'un d'entre eux ne sont pas protégés par un mot de passe personnel : doit-on considérer que ces fichiers sont « à la vue de tous » ? Pour y répondre, les tribunaux ont à vérifier le nombre de personnes susceptibles d'utiliser un ordinateur et un même mot de passe[34].

30. La question du consentement à la saisie pose davantage de problèmes. Il a notamment été jugé que la politique de l'employeur pouvait tenir lieu de consentement implicite pour chaque employé. Dans l'affaire *Simons*[35], un employé du *Foreing Bureau of Information*

Services (FBIS), une agence gouvernementale affilié à la *Central Intelligence Agency* (CIA), avait utilisé un logiciel permettant de faire des recherches par mots clés dans les fichiers de l'agence. En tapant le mot « *sex* », il obtint un taux de réponses positives très appréciable. Il identifia les employés dont l'ordinateur contenait le plus grand nombre de ces fichiers, dont Mark Simons. Après vérification, l'on découvrit sur son disque dur plusieurs fichiers contenant de la pornographie juvénile. Marc Simon fut alors accusé au criminel. La Cour s'est fortement appuyée sur la politique officielle de l'employeur pour conclure que Simons ne possédait pas d'expectative raisonnable de vie privée dans ses dossiers électroniques. Cette politique énonçait que les employés devaient s'attendre à ce que des vérifications des systèmes soient effectuées pour détecter les « activités non autorisées ». Elle mentionnait aussi que l'employeur se reconnaissait le droit d'enregistrer les sites Internet visités par les employés.

31. Le cas du consentement donné par une tierce partie[36] est encore plus troublant, en particulier lorsque les tribunaux valident une autorisation donnée par les membres d'une même famille ou par une personne avec laquelle on entretient une relation intime. Dans le cas d'un ordinateur familial, les tribunaux limitent toutefois cette notion de consentement mutuel aux seuls cas où des précautions ont été prises par des membres de la famille pour créer des « zones » exclusives pour l'utilisation de l'ordinateur. Ils ont ainsi rendu une décision éminemment déplorable, à notre avis, dans l'affaire *Smith*[37], où le consentement de l'amie de cœur de l'accusé, qui vivait chez lui à ce moment, a été jugé suffisant. La cour a été influencée par le fait que l'ordinateur, qui se trouvait dans leur chambre à coucher, était accessible aux autres membres de la maisonnée, dont la jeune sœur de l'accusé, et que son contenu n'était pas protégé par un mot de passe. Cette insistance sur l'existence d'un mot de passe laisse comprendre qu'*a contratio* l'une des façons efficaces de se protéger dans l'intimité de son foyer serait de toujours en utiliser un.

32. De nombreuses décisions jurisprudentielles portant sur les limites au droit à la vie privée proviennent de la dernière partie du quatrième amendement laquelle prévoit qu'un mandat doit décrire avec suffisamment de précision les endroits à perquisitionner et les choses qui peuvent être saisies. Nous ne traiterons pas en détail de ces arrêts, forts nombreux du reste, car nos tribunaux ne semblent pas avoir des exigences aussi élevées en ce qui concerne l'émission d'un mandat[38]. Nous devons simplement rester conscient de l'existence d'une série de problèmes soulevés par cette question.

33. En ce qui concerne les endroits à être perquisitionnés, un problème majeur surgit immédiatement du fait que la règle 41(a) de la *Federal Rule of Criminal Procedure* prévoit que « *[A] search warrant […] may be issued […] by a federal magistrate […] for a search of property or for a person […] within the district* ». Comment appliquer cette disposition à celui ou celle qui est reliée au réseau Internet et dont les fichiers peuvent se trouver dans des serveurs situés dans un autre État ou un autre pays ? Et*quid* des appareils portatifs, qui peuvent tantôt se trouver dans l'État où le mandat est émis, tantôt ailleurs ? Il n'y a pas encore de réponses précises à ces questions, mais la doctrine suggère aux tribunaux de s'aligner sur les règles applicables aux conversations téléphoniques[39].

34. Quant à ce qui peut être saisi, la situation est encore plus délicate. Il est clair que le texte même du 4ème amendement ne permet pas aux tribunaux de donner à la police carte blanche en émettant un mandat de saisir « tout ce qui est pertinent » ou « tous les dossiers » du suspect[40], surtout lorsqu'il s'agit d'un ordinateur localisé au foyer familial. Cette exigence se comprend encore mieux lorsqu'une entreprise est visée. Elle peut en effet détenir, dans ses ordinateurs, des listes de clients, des états financiers, les dossiers des employés, des inventaires, etc. Il est donc difficile de concilier l'exigence de précision, au niveau du mandat, avec le fait qu'un ordinateur peut contenir de grandes quantités d'informations et le fait que le nom d'un fichier n'est pas suffisant pour en deviner le contenu[41]. Rappelons aussi la règle, également valable au Canada, à l'effet qu'un mandat peut avoir été validement émis mais que la façon dont la perquisition, la fouille ou la saisie ont été effectués ne respectent pas les exigences constitutionnelles, ce qui les rend également invalides.

B. Les protections accordées par le droit statutaire

35. Deux lois américaines, pour lesquelles nous n'avons pas d'équivalence parfaite au Canada, accordent aux citoyens des protections additionnelles à celles fournies par la constitution. Il s'agit de *l'Electronic Communications Privacy Act* (*ECPA*), de 1986, et de la *Privacy Protection Act*, de 1980.

36. La première, l'*ECPA*, a créé, pour le monde de l'électronique, deux protections importantes. Le *Title I*[42] prohibe l'interception non autorisée de communications électroniques, alors que le *Title II* prohibe l'accès non autorisé aux messages et données qui sont dans la mémoire (la loi dit :« *stored* ») d'un ordinateur. Le *Title I* utilise des concepts semblables à ceux que l'on retrouve dans la partie VI du Code criminel canadien, sur les « atteintes à la vie privée ». On y a élargi des protections initialement prévues dans la *Federal Wiretap Act* pour interdire toute interception non-autorisée d'une communication faite au moyen de l'électronique. Le champ d'application de ce texte dépasse maintenant les conversations audibles pour une tierce oreille. On y protège la transmission de données numériques et il n'est pas nécessaire que cette transmission ait été effectuée au moyen des équipements des sociétés de télécommunications. La loi interdit aussi la fabrication, la vente et la possession d'équipements destinés essentiellement à faire de l'espionnage électronique[43]. Elle prévoit également l'exigence d'un mandat de perquisition pour qu'une interception soit légale[44] et l'autorisation judiciaire est valide pour un temps limité seulement[45].

37. En doctrine, les avis sont partagés sur l'efficacité de cette partie de la loi[46]. Tous s'entendent, cependant, pour dire qu'il faudra encore attendre les décisions des tribunaux pour trancher des points litigieux, car la loi renferme des exceptions et des exemptions d'importance. Ainsi, pour ne mentionner que les principales difficultés, la loi probablement pour éviter d'empiéter sur les compétences des États ne vise que les communications qui « affectent » le commerce inter-étatique ou international[47]. On peut d'emblée se demander si cette disposition les systèmes qui utilisent des réseaux d'ordinateurs reliés par des fils ou câbles qui ne traversent pas de frontières. L'opérateur d'un système de communications est pour sa part exempté de l'exigence du mandat s'il

soupçonne une utilisation inappropriée (« *misuse* ») ou lorsque les utilisateurs ont explicitement ou implicitement consenti à un système de surveillance[48]. Il peut aussi divulguer impunément à la police les informations incriminantes qu'il découvre par inadvertance ou dans le cours normal des affaires.[49] Il faudra donc que les tribunaux se prononcent sur la portée du concept de « *cours normal des affaires* ». Il semble que la seule protection véritable dont peuvent bénéficier les citoyens en vertu du *Title I* est l'interdiction généralisée de surveillance du courrier électronique.

38. Le *Title II* vise les communications qui ne sont plus en transit. Il cherche à les protéger de tout accès non autorisé.En effet, il interdit l'accès à « *... a facility through which an electronic communication is provided and thereby obtains […] an electronic communication while it is in electronic storage* »[50]. La loi interdit aussi à celui qui fournit au public un service de communications par l'électronique de divulguer le contenu d'une conversation qui est en « *mémoire électronique* ». Ces communications sont donc mieux protégées que celles qui sont en transit[51]. La loi va jusqu'à interdire le simple fait d'avoir accès à des communications ou des données privées, sans qu'il soit nécessaire que la personne fautive les télécharge ou altère de quelque façon les dossiers. Elle prévoit plusieurs garanties procédurales à l'égard des agences gouvernementales qui veulent accéder à ces dossiers. Le *Title II* interdit, sans l'existence d'un mandat, de révéler l'identité de l'émetteur et du récepteur d'un message, la longueur du message, le service utilisé pour le transmettre et la localisation des personnes concernées[52]. Deux exceptions importantes sont prévues dans la loi : l'opérateur du système peut entretenir ses équipements et, sur une base routinière, le « *monitorer* ». Il peut également « *prendre des mesures disciplinaires* » s'il découvre des informations illicites qui affectent des utilisateurs du système. Enfin, dans des cas très limités, l'opérateur peut révéler des informations à la police, comme, par exemple, celles qui témoignent du fait qu'un crime est en train d'être commis[53].

39. Le *Privacy Protection Act*[54] présente moins d'applications directes pour ce qui est des courriels. Il cherche esssentiellement à protéger les éditeurs des fouilles policières.Une disposition cruciale est à l'effet suivant : « *... it shall be unlawful for a government officer or employee, in connection with the investigation or prosecution of a criminal offense, to search for or seize any work product materials […] possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication…* »[55]. La loi peut indirectement toucher, par ces derniers mots, le monde de l'électronique. Les babillards électroniques pourraient être visés, quoiqu'il n'y ait pas encore de jurisprudence sur ce point. Cependant, les courriels eux-mêmes ne seraient pas visés, puisque les utilisateurs veulent, la plupart du temps, que leurs messages demeurent une affaire privée entre l'émetteur et le récepteur.

Conclusion

40. La conclusion suivante s'impose : les protections légales ou réglementaires relatives aux courriels doivent être renforcées. Comme nous l'évoquions en introduction, ce mode de communication est appelé à se répandre davantage et ses utilisateurs désirent, bien légitimement, qu'il soit juridiquement protégé tout autant que le sont le courrier postal et les conversations téléphoniques.

41. Malheureusement, force est de constater que cela n'est pas encore le cas. Dans une situation typique, la *Charte canadienne* ne peut être invoquée. On ne fait pas tous les jours l'objet de filatures policières pour avoir été soupçonné d'un crime grave. C'est dans le domaine des relations de travail que des protections juridiques renforcées s'avèrent nécessaires.

42. On pourrait penser que le droit civil québécois est déjà doté des instruments nécessaires à cette fin au regard de l'affirmation du principe générale du droit au respect à la vie privée. En effet les articles 3 et 35 du Code civil prévoient que « *[t]oute personne est titulaire de droits de la personnalité, tels le droit […] au respect […] de sa vie privée* », et « *[t]oute personne a droit au respect de sa réputation et de sa vie privée* ». L'article 5 de *la Charte des droits et libertés de la personne* réaffirme également, et simplement, le principe du droit au respect de la vie privée.

43. Selon nous, la situation présente illustre de manière idéale que l'énoncé d'un principe général n'est pas toujours suffisant pour atteindre le but recherché. On a tendance à croire qu'il est toujours préférable d'énoncer des principes dans des termes généraux, ce qui permet de viser un plus grand nombre de cas, dont des situations qui ne pouvaient être prévues lors de l'adoption de la loi. Cela a le désavantage de forcer les juges à accomplir une tâche très difficile, celle qui consiste à dire si une pratique ou une façon de faire détaillée est valide par rapport à un principe flou à souhait. Prenons deux exemples dans le domaine médical pour illustrer notre propos.

44. Depuis l'implantation du programme d'assurance-médicaments, les systèmes informatiques des pharmaciens sont reliés à ceux de laRégie d'assurance maladie du Québec (RAMQ), ce qui leur permet de savoir quel montant doit être facturé au client ou à la cliente. Les pharmaciens ont ainsi accès à davantage de renseignements sur la consommation de médicaments par leur clientèle. Supposons qu'une personne contesterait en justice ce nouveau système au motif du non-respect de sa vie privée. Un juge aurait alors à déterminer si l'ensemble des règles établies par laRAMQ, qui peuvent contenir des protections vis-à-vis de la vie privée des personnes, sont valides ou non à l'égard du grand principe que « chacun a droit au respect de sa vie privée ».

45. Dans la même veine, les hôpitaux ont informatisé ces dernières années les dossiers médicaux des patients. Il est donc plus facile pour un médecin non traitant et pour l'ensemble du personnel médical d'avoir accès aux informations colligées dans le dossier médical d'une personne. Là encore, si quelqu'un contestait ce système pour motif de non-respect de sa vie privée, un juge aurait à jauger les différentes règles élaborées par les hôpitaux pour déterminer quel renseignement se trouvera dans le dossier électronique, qui y aura accès, comment etc..., pour dire si ce système est globalement valide ou vicié parce que contraire au principe du respect de la vie privée. Si tel était le cas, quel remède le juge pourrait-il appliquer ? On voit mal nos juges dire aux gouvernements quelles règles détaillées ils doivent adopter pour assurer le respect de la vie privée. C'est pourtant ce qu'il faudrait faire, car un jugement qui accorderait une indemnité monétaire ne donnerait certes pas entière satisfaction au plaignant.

46. À notre avis il en va de même pour le courrier électronique. Si les gouvernements estiment sincèrement qu'il doit être protégé juridiquement, ils devront, selon nous, adopter une série de mesures détaillées. Nous avons besoins de normes qui précisent ce qu'il en est au niveau des relations de travail et dans les autres contextes. Il faudrait préciser la responsabilité juridique des principaux acteurs dans ce domaine, qu'il s'agisse du fournisseur d'accès, du maître de site ou encore de l'entreprise de télécommunications. Ce serait préférable à une situation qui délègue cette tâche aux tribunaux, lesquels ne sont pas particulièrement bien outillés pour l'accomplir.

Notes

(*) Professeur à la Faculté de droit de l'Université de Sherbrooke (Canada - Qc). Email :rpepin@droit.usherb.ca.

[1] *United States c. Barth* 26 F. Supp. 2d, 929, p. 936 , Juge Furgeson.

[2] chiffres publiés dans le *Journal du Barreau*, éd. 1er sept. 1998. On prévoyait à ce moment que le nombre d'utilisateurs du réseau Internet à travers le monde se chiffrerait entre 500 millions et 1 milliard en l'an 2000.

[3] Au Canada, est considéré comme un acte criminel le fait d'intercepter le courrier d'autrui (arts. 356 et 358 C. cr.) ou d'épier ses conversations téléphoniques (art 184 C. cr.). L'art. 184 (2) C. cr. permet à un fournisseur de service de télécommunications d'intercepter une conversation privée si elle est nécessaire pour la fourniture du service, ou si cela est fait à l'occasion d'un contrôle au hasard de la qualité du service. Sur le plan du droit civil, l'article 48 de la *Loi sur la Société canadienne des postes*(S.R.C. c. C-10) protège la confidentialité des envois postaux ; la *Loi sur les télécommunications*, (S.R.C. c-T-3.4) pour sa part, interdit en son article 35 à toute entreprise de télécommunications de « *régir le contenu […] des télécommunications qu'elle achemine pour le public* ».

[4] F. Themens, *Internet et la responsabilité civile*, Montréal, Yvon Blais, 1998, P. Trudel et al, *Droit du Cyberespace* , Montréal, Thémis, 1997, chaps. 5.2, 5.3, 11.2

[5] *La Tribune*, jeudi 8 juin 2000, p. A4. Voir aussi K. Noël, « Le nouveau visage de la surveillance au travail », *Journal Les Affaires*, 27 mai 2000, p.3.

[6] *R. c. Weir* (1998) A.J. 155, 59 Alta. L. R. (3d) 319, (1998) W.W.W. 228.

[7] C'est l'équivalent, au Québec, de la Cour supérieure.

[8] Voir les parag. 44-55.

[9] Rappelons que la Cour suprême du Canada a jugé, depuis l'affaire *Hunter c. Southam* (1984) 2 R.C.S. 145, que la Charte doit recevoir une interprétation contextuelle ; les droits qui y sont garantis n'ont pas toujours la même portée. L'article 8 nous fournit l'exemple parfait : l'expectative de vie privée à laquelle on peut s'attendre est la plus grande dans l'intimité de son foyer, mais elle est différente pour celui qui se trouve au volant de sa voiture (*Wilson c. R.* (1990) 1 R.C.S. 1291), dans une chambre d'hôtel (*R. c. Wong* (1990) 120 N. R. 34), au travail (*Comité paritaire de l'industrie de la chemise c. Potash* (1994) 115 D.L.R. 702), à la douane (*Simmons c. R.* (1988) 2 R.C.S. 495) ou en prison (*Conway c. R.* (1993) 2 R.C.S. 872).

[10] *supra*, note 3.

[11] *Mega c. Berton*, « Home is Where Your Modem Is : an Appropriate Application of Search and Seizure Law to Electronic Mail », (1996) 34 *A.M.C. L. rev*. 163.

[12] *R. c. Weir*, *précité*, note 6, parag. 62.

[13] *Ibid*, parag. 63.

[14] *Ibid*, parag. 64.

[15] *Ibid*, parags. 74 ss.

[16] La décision *Weir* a été portée en appel, mais il n'y a actuellement qu'une décision intérimaire permettant de soulever un nouvel argument relatif à validité constitutionnelle de certains articles du code criminel relatifs à la pornographie juvénile : voir(1999) 27 C. R. (5th) 333, 73 Alta. L. R. (3d) 303.

[17] Sur cette question, voir H. L. Rasky, « Can an Employer Search the Contents of Its Employees' E-Mail? » (1998) 20 *Advocates' Q*. 221.

[18] Voir par exemple *Goodyear Can. Inc. and U.W.R.*, local 189 (1994) 44 L.A.C. (4th) 203.

[19] Notons que les tribunaux considéraient aussi qu'une personne n'a pas d'expectative raisonnable de vie privée au niveau des appels effectués sur téléphones cellulaires : *R. c. Solomon*, (1992) 77 C.C.C. (3d) 264, p. 284. C'est pour contrer cette décision que l'article 184.5 C. cr. aurait été ajouté en 1993, interdisant l'interception malicieuse de toute « *communication radiotéléphonique* ».

[20] R. Winnick, « Searches and Seizures of Computers and Computer Data », 8 *Harv. J. L. & Tech.* 75, p. 77.

[21] Voir M. Goldsmith, « Privacy Laws Urged for Dats Superhighway », *N.Y.L.J.*, 1994, p.1.

[22] *United States c. McAllister* 18 F 3d 1412 (1994) .À l'inverse, le quatrième amendement de la constitution ne sera pas en jeu dans le cas du particulier qui agit sans la connaissance ni la participation des autorités gouvernementales ou qui livre à la police le fruit de ses fouilles dans les courriels d'autrui : *United States c. Attson* 900 F2d 1427 (1990).

[23] Le texte se lit comme suit : « *…and no warrant shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized* ».

[24] (1967) 389 U.S. 347.

[25] *Ibid*, p. 361.

[26] 830 F. Supp. 531 (N. D. Cal. 1993).

[27] *O'Connor c. Ortega* 480 U.S. 707 (1987).

[28] *Rakas c. Illinois* 439 U. S. 128 (1978).

[29] *Katz c. U.S.* 389 U. S. 352 (1967).

[30] *U. S. c. Maxwell* 45 M. J. 406 (1996).

[31] Dans l'affaire *Monroe*, (*U. S. c. Monroe*, 52 M. J. 326) on jugea que ce sergent de l'armée américaine n'avait pas d'expectative raisonnable de vie privée dans ses courriels en s'appuyant sur la décision Maxwell et sur le fait que, chaque fois qu'il se connectait au réseau Internet, il devait accepter le message suivant : « *Users logging into this system consent to monitoring by the hostadm* ».

[32] Voir dans le même sens la décision *Charbonneau* : *U. S. c. Charbonneau* 979 F. Supp. 1177 (S. D. Ohio 1997).

[33] *Katz, précité*, note 29, p. 361.

[34] *Bohach c. City of Reno*, 932 F. Supp. 1232 (D. Nev. 1996) où cette question a été largement débattue.

[35] *United States c. Simons*29 F. Supp. 2d, 324 (E.D. Va. 1998).

[36] La décision de base de la Cour suprême sur cette question se trouve dans l'affaire *United States c. Matlock* 94 S. Ct. 988 (1970).

[37] *United States c. Smith* 27 F. Supp. 2d 1111 (C.D. Ill. 1998).

[38] L'art. 487 C. cr. laisse une grande latitude aux tribunaux dans l'émission d'un mandat de perquisition une fois qu'un juge est convaincu qu'il y a des motifs raisonnables de croire

qu'il existe dans un lieu une chose quelconque dont on pense qu'elle fournira la preuve de la commission d'une infraction. Cette disposition a été analysée par la Cour suprême notamment dans C.*B.C. c. Att. Gen. of New-Brunswick* (1991) 3 R.C.S. 459.

[39] S. Bayens, « The Search and Seizure of Computers: Are We Sacrificing Personal Privacy for the Advancement of Technology?»48 *Drake L. Rev*. 239, p. 259.

[40] *Coolidge c. New Hampshire* 403 U.S. 443 (1971).

[41] Voir S. Bayens, *loc. cit.*, note 39, p.263.

[42] Le *Title I* est codifié dans le *United States Code* à 18 U. S. C. 2510- 2522 ; le *Title II* l'est à 18 U. S. C. 2701-2711.

[43] Art. 191 C. cr.

[44] Art. 184.2 C. cr.

[45] La période normale est de 60 jours : art. 184.2, par. 4(e) *in fine*.

[46] S. Bayens, *loc. cit.*, note 39, p. 277, croit que les protections en vertu du *Title I* s'avèreront inutiles en pratique, justement parce qu'il y a trop de garanties procédurales. Il suffit aux autorités policières d'attendre une fraction de seconde qu'un message ne soit plus en transit pour que s'applique le *Title II*, où elles ont les coudées plus franches.

[47] 18 U.S.C. s. 2510(12).

[48] *Ibid*, s. 2511 (2)(a)(i).

[49] *Ibid*, s. 2511 (3)(b)(iv).

[50] *Ibid*, s. 2702) (1)-(2).

[51] R. Winick, *loc. cit.*, note 20, p. 94.

[52] 18 U.S.C. s. 2703(C) (1)(A).

[53] *Ibid*, s. 2701(a).

[54] 42 U.S. C. s. 2000aa-2000-aa-12.

[55] *Ibid*, s. 2000aa(a).

ISSN 1480-1787