Actualités informatiques pour la magistrature

AIM

LES JUGES SE PENCHENT SUR LES QUESTIONS DE SURVEILLANCE ET DE SÉCURITÉ

Le Conseil canadien de la magistrature a approuvé les recommandations du Comité consultatif sur l'utilisation des nouvelles technologies par les juges visant la mise en place de la sécurité informatique au premier rang du programme des juges en chef à travers le Canada, l'adoption de programmes de formation et la création du plan détaillé des procédures de sécurité recommandées pour tous les tribunaux.

À l'hiver 2000-2001, le Sous-comité sur la sécurité informatique du Comité consultatif sur l'utilisation des nouvelles technologies par les juges a mené un sondage de 208 questions auprès des tribunaux fédéraux et provinciaux et des membres du personnel responsables de la technologie judiciaire. Le sondage comprenait des questions se rapportant à la sensibilisation à l'égard des préoccupations en matière de sécurité informatique et à la priorité qui leur était accordée, à la façon dont les politiques de sécurité étaient élaborées au sein des tribunaux, à la formation en matière de sécurité, à la protection de l'équipement portatif et à la séparation des utilisateurs d'ordinateurs se trouvant au sein ou à l'extérieur du système judiciaire.

Les résultats du sondage ont porté le Comité consultatif sur l'utilisation des nouvelles technologies par les juges à présenter une série de recommandations, lesquelles ont été approuvées par le Comité exécutif du Conseil en novembre 2001. On a notamment demandé au Conseil de consacrer son colloque de mars 2002 aux questions de sécurité informatique.

Michael Geist, professeur de droit à l'Université d'Ottawa, et Martin Felsky, président de Commonwealth Legal Inc., tous deux conseillers du Comité consultatif sur l'utilisation des nouvelles technologies par les juges, ont donné des présentations lors du colloque. On a également assisté à des discussions menées par l'hon. Frances Kiteley, présidente du Sous-comité, de même que par l'hon. Adelle Fruman, membre du Sous-comité.

Le présent numéro des *Actualités informatiques pour la magistrature* traite du colloque et contient le guide en dix points sur la sécurité informatique à l'intention des juges établi par le Dr Felsky. Le numéro présente le résumé d'un document sur la surveillance informatique préparé pour le Conseil par le professeur Geist, ainsi que celui d'un nouveau document sur les questions de transmission et d'accès électronique préparé par la Cour suprême de la Colombie-Britannique. Les AIM se penchent également sur les développements relatifs aux sites Web des tribunaux à travers le pays et sur certains plans en cours visant l'amélioration de ces sites.

Voir ...

VERS UNE MEILLEURE SÉCURITÉ INFORMATIQUE : LES RECOMMANDATIONS DU COMITÉ CONSULTATIF SUR L'UTILISATION DES NOUVELLES TECHNOLOGIES PAR LES JUGES SONT APPROUVÉES PAR LE CONSEIL

Le rapport sur la sécurité informatique du Comité consultatif sur l'utilisation des nouvelles technologies par les juges a été distribué à tous les juges en chef et aux sous-procureurs généraux, leur demandant de collaborer à la mise en œuvre des recommandations.

Les recommandations comprennent ce qui suit :

- une demande à l'effet que l'Institut national de la magistrature et le Bureau du Commissaire à la magistrature fédérale coordonnent la formation relative aux questions de sécurité informatique à l'intention des juges fédéraux et provinciaux et du personnel de technologie de l'information;
- une demande à l'effet que les juges en chef aient comme priorité l'adoption de systèmes assurant la sécurité des renseignements judiciaires, étudient l'élaboration précoce d'une politique de sécurité dans le cadre de la conversion vers des environnements électroniques, obtiennent les ressources nécessaires aux mesures de sécurité et nomment un membre du personnel de technologie qui est responsable des opérations de la sécurité;
- l'autorisation accordée par le Comité consultatif sur l'utilisation des nouvelles technologies par les juges et visant l'élaboration du plan détaillé des procédures de sécurité recommandées et à l'intention des tribunaux canadiens.

Plan détaillé de la sécurité

Le plan détaillé doit comprendre un protocole traitant des questions de sécurité liées à l'utilisation des ordinateurs portatifs lors des voyages d'affaires.

On a également demandé au Comité consultatif sur l'utilisation des nouvelles technologies par les juges de travailler avec des éditeurs juridiques et autres, afin d'établir des procédures visant à empêcher la communication de jugements contenant des parties supprimées ou modifications et pour adopter un protocole relatif au retrait des jugements contenant des suppressions antérieures ou ayant été communiqués par erreur.

Le plan détaillé, qui pourrait également être désigné par les expressions « meilleures pratiques » ou « normes minimales », sera destiné à tous les tribunaux et juges, en vue du partage des réseaux dans plusieurs juridictions. Dans le même ordre d'idées, le Comité consultatif sur l'utilisation des nouvelles technologies par les juges recommande que la formation et certains programmes éducatifs visent tant les juges que le personnel de technologie supérieur, afin que tous entendent le même message.

LA SURVEILLANCE : PAS BELLE À VOIR?

Professeur Michael Geist
Faculté de droit, Université d'Ottawa

Tiré de son document *Surveillance des ordinateurs et du courrier électronique en milieu de travail au Canada : de l'attente raisonnable en matière de respect de la vie privée à la surveillance raisonnable* :

L'ubiquité de l'informatique et des communications par Internet a propulsé la surveillance des ordinateurs et du courrier électronique sur le devant de la scène publique. Dans le milieu du travail, des millions d'employés disposant d'un ordinateur et connaissant bien leurs applications de traitement de texte et de courrier électronique peuvent en savoir très peu sur les programmes de surveillance qui enregistrent silencieusement leurs activités sur le réseau ou, pire encore, chacune de leurs frappes.

De tels programmes peuvent générer des rapports personnalisés qui affichent la façon dont les employés utilisent leurs ordinateurs. Par exemple, la plupart des programmes surveillent le temps passé sur Internet et fournissent des rapports détaillés au sujet du courrier électronique.

- Les programmes axés sur les serveurs sont installés directement sur le réseau informatique de l'employeur et mettent surtout l'accent sur l'utilisation du réseau, laquelle comprend l'utilisation du courrier électronique

et d'Internet. Certains programmes peuvent empêcher le téléchargement de types de fichier particuliers, tels que les fichiers de films, les fichiers graphiques ou les fichiers musicaux.

- Les programmes axés sur les clients sont installés directement sur les ordinateurs des employés et génèrent des journaux qui enregistrent toutes les activités dans un fichier ou une base de données en vue d'un examen futur. Ils peuvent enregistrer toutes les frappes au clavier, y compris celles qui sont effacées par la suite.

Les entreprises de toutes tailles ont commencé à installer des technologies de surveillance informatique qui ciblent plus particulièrement l'utilisation des ressources de l'information par les employés. Par ailleurs, la surveillance informatique ne se limite pas qu'au milieu de travail ordinaire. En 2001, la Judicial Conference of the United States a suscité la controverse au sein de l'appareil judiciaire américain après avoir recommandé la surveillance généralisée de tous les ordinateurs utilisés par la magistrature et son personnel. La question a éventuellement été réglée par suite de l'adoption d'une proposition modifiée.

Droit de l'employeur?

La question de savoir si les employeurs ont légalement le droit de surveiller l'utilisation des ordinateurs par leurs employés demeure sujette à débat. Les entreprises invoquent plusieurs motifs à l'appui de l'installation de systèmes de surveillance en milieu de travail :

- La lutte contre l'utilisation d'Internet à des fins personnelles pendant les heures de bureau. D'après un sondage effectué au Canada, les employés canadiens gaspillent presque 800 millions d'heures de travail chaque année à naviguer sur Internet à des fins personnelles.
- Le maintien du rendement du réseau. L'efficacité du réseau est liée à la largeur de bande et les ralentissements sont causés par les employés qui téléchargent de grands fichiers audio et vidéo.
- La responsabilité. Les employeurs peuvent être tenus légalement responsables de l'utilisation malveillante des ordinateurs, notamment des atteintes au droit d'auteur et de l'utilisation de logiciels non autorisés.
- Les préoccupations en matière de confidentialité et de secrets commerciaux. Les entreprises ont subi de lourdes pertes financières en raison du vol de renseignements exclusifs.
- Les délits informatiques. La surveillance de réseau peut également aider à mettre au jour des crimes tels que le détournement de fonds et la fraude.
- L'obligation légale. Dans certaines circonstances, le droit positif impose aux employeurs l'obligation de surveiller l'utilisation des ordinateurs, comme dans le cas des compagnies médicales, lesquelles sont tenues de protéger les renseignements personnels des patients.

Au Canada, la source la plus importante de droits à la vie privée dans le secteur privé est la nouvelle *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE). Bien que la loi n'entre pleinement en vigueur que le 1er janvier 2004, ses principes fondamentaux ont déjà un effet sur des milliers d'organisations canadiennes.

La nouvelle jurisprudence et les nouvelles lois et politiques donnent à penser qu'une perspective équilibrée entre les droits d'interception et le droit à la vie privée est rapidement en voie d'apparaître au Canada. Bien que les lois canadiennes mettent l'accent sur des critères liés au respect de la vie privée de l'utilisateur, il semble s'opérer une transition graduelle vers des critères liés au « caractère raisonnable » de la surveillance informatique.

Les critères de « caractère raisonnable » sont les suivants :

(i) La cible de la surveillance. Il faut se demander si la surveillance devrait être effectuée de manière à viser tous les employés de façon égale. Certains employés peuvent déjà faire état de leur emploi du temps par l'entremise de procédures de rapport existantes. Il peut être inutile de surveiller les employés n'ayant pas accès à des renseignements de nature délicate. Certaines personnes ne peuvent faire l'objet d'une surveillance que dans des circonstances limitées, en raison de leurs fonctions; la magistrature en est un bon exemple, puisque certaines formes de surveillance de la magistrature soulèvent non seulement des préoccupations quant au respect de la vie privée, mais aussi des considérations d'indépendance judiciaire.

(ii) L'objet de la surveillance. Les motifs (rendement des employés et du réseau, responsabilité, préoccupations en matière de secrets commerciaux, délits informatiques, etc.) ont été énumérés ci-haut.

(iii) L'utilisation préalable de solutions de rechange à la surveillance. Selon les décisions arbitrales et judiciaires, il faut tout d'abord étudier des solutions de rechange à la surveillance moins intrusives.

(iv) La technologie utilisée. Les organisations devraient choisir la technologie qui satisfait le mieux à leurs objectifs tout en portant le moins possible atteinte à la vie privée.

(v) L'avis donné à la cible. Étant donné les exceptions relatives au consentement prévues par le Code criminel, un consentement pleinement éclairé est nécessaire pour s'assurer que la surveillance en milieu de travail ne viole pas le droit criminel.

(vi) La protection de la vie privée une fois les renseignements obtenus par voie de surveillance. La LPRPDE exige la désignation, au sein de l'organisation, d'une personne chargée des questions relatives à la vie privée.

UNE QUESTION POUR LES JUGES

De nos jours, l'ordinateur est un outil indispensable pour la grande majorité des juges. Dans plusieurs provinces, presque tous les juges ont leur propre ordinateur personnel, qu'ils utilisent à des fins diverses, notamment le travail se rapportant aux jugements, la communication et la recherche juridique.

Le travail informatique se rapportant aux jugements comprend l'entrée de notes prises au procès, la rédaction et révision de mémoires de recherche, ainsi que la rédaction de jugements. Lorsque plusieurs membres de la formation participent conjointement à la rédaction d'un seul jugement, les capacités de traitement de texte en collaboration ainsi qu'une fonctionnalité de comparaison de documents s'avèrent d'une très grande valeur. Les juges ont parfois recours à la communication par voie électronique dans le cadre de discussions hautement confidentielles. La recherche informatisée est devenue un élément essentiel du processus de recherche juridique.

Les juges doivent examiner la façon dont la surveillance devrait être adoptée au sein de la magistrature canadienne. Si l'on se fie aux conventions internationales et à la jurisprudence canadienne, on peut conclure que la surveillance des ordinateurs et du courrier électronique de la magistrature n'est autorisée par la loi que dans des circonstances très limitées. La surveillance du contenu des courriels et des documents créés par traitement de texte doit obligatoirement bénéficier d'une confidentialité absolue. Toute surveillance portant atteinte à la confidentialité des délibérations serait illégale. Y serait incluse l'utilisation de programmes de surveillance axés sur les clients, tels que les programmes enregistreurs de frappes pouvant capter tous les renseignements entrés dans un ordinateur personnel.

Le professeur Geist est spécialiste des questions juridiques afférentes à Internet et au commerce électronique à la Faculté de droit de l'Université d'Ottawa. Il est directeur des questions juridiques afférentes au commerce électronique au sein du cabinet d'avocats canadien Goodmans LLP et a écrit plusieurs articles et rapports gouvernementaux au sujet d'Internet et le droit.

LA SURVEILLANCE : UNE JOURNÉE À L'ORDINATEUR

En se fondant sur sa propre recherche d'un jour sur les membres de la magistrature travaillant à l'ordinateur, le professeur Geist a illustré ce qui était susceptible de faire l'objet d'une surveillance, selon la portée du programme de surveillance.

En tant que juge, vous pouvez :	**Ce que peuvent faire les programmes de surveillance :**
• initialiser le système et y entrer avec un mot de passe qui vous branche à votre réseau;	• suivre l'entrée dans le système;
• faire démarrer les programmes de traitement de texte (par ex., Microsoft Word);	• identifier l'utilisation de Word;
• commencer une recherche en droit des assurances en vue de rédiger un mémoire;	• lire le texte du mémoire, y compris chaque frappe au clavier;
• vérifier le courrier électronique (par ex., en utilisant Outlook Express) et rédiger un courriel à l'intention d'un collègue à l'extérieur de votre système;	• enregistrer le texte du courriel et la pièce jointe;
• faire démarrer le navigateur Web et vous rendre au site « CANLII.ORG » pour obtenir une liste de décisions, en corrigeant votre erreur typographique ayant donné « CANLII.ORF »;	• enregistrer toutes les activités de navigation sur Internet, y compris les termes de recherche;
• effectuer une recherche sur le site Web du *Globe and Mail* pour obtenir des décisions; le site donne un lien à « bad faith insurance. com », lequel porte sur les recours collectifs contre des compagnies d'assurances américaines;	• enregistrer tous les sites que vous avez visités, y compris ceux visités par erreur;
• prendre une pause; vérifier la mention d'un programme de télévision appelé « storefront » et taper accidentellement « stormfront », un site de propagande haineuse;	• par ailleurs, les programmes n'établissent aucune distinction entre les activités intentionnelles et les sites visités par erreur;
• vérifier les résultats d'un litige américain sur le site Web anti-avortement « Nuremburgfile.com » et être automatiquement réacheminé vers « pervertedlinks.com », un site pornographique;	• les programmes peuvent afficher ce que vous voyez en temps réel (par ex., à toutes les cinq ou dix minutes).
• tenter de vous rendre au site de la Cour suprême du Canada en tapant « supremecourt.ca » et obtenir le site Web du Parti Marijuana de la Colombie-Britannique.	

LA SURVEILLANCE : DE SÉRIEUSES QUESTIONS POUR LA MAGISTRATURE

L'hon. Frances Kiteley
Juge de la Cour supérieure de justice de l'Ontario

Tiré de ses observations présentées au colloque du Conseil :

La surveillance de l'utilisation des ordinateurs par la magistrature soulève des préoccupations particulières et sérieuses en matière d'indépendance, d'impartialité et de confidentialité judiciaires.

Certaines décisions judiciaires font valoir que la confidentialité des renseignements judiciaires est essentielle à l'indépendance judiciaire.

Les juges devraient pouvoir contrôler la communication de leurs travaux confidentiels, y compris les notes prises sur le vif au sujet des témoins. Ils doivent être en mesure d'effectuer des recherches sur des idées inhabituelles et de raffiner leur analyse dans plusieurs projets de jugement. Par ailleurs, il est inutile d'exempter les juges de toute surveillance si, au même moment, le personnel judiciaire qui partage les renseignements confidentiels des juges fait l'objet d'une surveillance.

Le Comité consultatif sur l'utilisation des nouvelles technologies par les juges est en voie de préparer des recommandations portant sur la surveillance des juges et du personnel judiciaire au Canada. Les recommandations traiteront notamment des questions relatives aux menaces externes, à la surveillance du contenu et au rendement du réseau.

Tous les juges en chef doivent bien comprendre les questions relatives à l'utilisation des ordinateurs par les juges et à la sécurité des renseignements créés par les juges. Dans plusieurs provinces, les juges nommés par le fédéral et ceux nommés par les provinces partagent les mêmes ressources. Dans la mesure où ils le font, ils se doivent d'adopter une approche similaire en matière de sécurité. Dans tout environnement électronique, la force du système ne dépasse jamais celle du maillon le plus faible. Le Comité consultatif sur l'utilisation des nouvelles technologies par les juges prévoit que tous les tribunaux canadiens profiteront de ses travaux visant à créer un plan détaillé des procédures de sécurité recommandées et à l'intention des tribunaux.

L'hon. Frances Kiteley est présidente du Sous-comité sur la sécurité informatique du Comité consultatif sur l'utilisation des nouvelles technologies par les juges.

LA PROTECTION EN DIX POINTS DES DONNÉES JUDICIAIRES INFORMATISÉES

Guide établi par le Sous-comité sur la sécurité informatique du Comité consultatif sur l'utilisation des nouvelles technologies par les juges

1. Si vous vous servez d'un ordinateur portatif, il faut le protéger comme votre propre portefeuille. Ne le laissez jamais sans surveillance. Si possible, attachez-le avec un câble anti-vol.

2. Instaurez un « mot de passe de mise sous tension (mise en marche) » pour l'ordinateur portatif, et un mot de passe d'économiseur d'écran pour le portatif et l'ordinateur de table.

3. Ne dites à personne votre nom de connexion, votre compte d'abonné ou vos mots de passe.

4. Choisissez un mot de passe compliqué, quelque chose qui ne soit ni un nom ni un mot du dictionnaire. Une combinaison de lettres (majuscules et minuscules), de chiffres et de signes de ponctuation serait un parfait mot de passe. Plus celui-ci est long, moins il sera pénétrable. Par exemple, « .d'A,.2Suisse » est un mot de passe difficile à pénétrer et facile à retenir. C'est l'acronyme de « Point d'argent, point de Suisse ». Changez votre mot de passe régulièrement, par exemple tous les 90 jours.

5. Veillez à sauvegarder les documents et travaux importants sur du matériel serveur, un dérouleur de bande magnétique, des disques compacts, des disquettes de haute qualité, ou tout autre support sûr et fiable. Demandez au gestionnaire des systèmes de vous recommander la meilleure procédure de sauvegarde.

6. Il faut absolument équiper votre ordinateur d'un anti-virus. Demandez à l'administrateur des systèmes de s'assurer que les définitions de virus sont périodiquement mises à jour, et que le programme est réglé de façon à balayer automatiquement

les disquettes, le courrier électronique d'arrivée, les pièces jointes et les fichiers téléchargés.

7. Si vous vous servez du système Microsoft Word, demandez à l'administrateur des systèmes de veiller à ce que les documents transmis à l'extérieur du réseau judiciaire ne renferment pas des informations cachées comme les révisions et les suppressions sur des projets précédents, ou des renseignements personnels (méta-données). Communiquez-lui les guides suivants de Microsoft :

- Pour Word 2000 : *How to Minimize Metadata in Microsoft Word Documents* (Knowledge Base Article Q237361). Pour Microsoft Word 2002, voir Q290945, et pour Microsoft Word 97, voir Q223790. Trouvez Microsoft Knowledge Base Articles à : http://support.microsoft.com/default.aspx?scid=fh;EN-CA; kbinfo

8. Il faut utiliser une technologie de chiffrement fiable pour protéger les données de nature particulièrement délicate, mémorisées dans votre ordinateur, qu'elles soient en cours de transmission ou non. Demandez au besoin l'aide de l'administrateur des systèmes.

9. Quand il s'agit de vous débarrasser de vos ordinateurs, lecteurs ou disquettes, il faut observer les méthodes approuvées à cet effet par l'administrateur des systèmes — par exemple, il faut vider le support de toutes les données supprimées et dans certains cas, il faut même le détruire. Il ne suffit pas d'« effacer » des fichiers d'une disquette avant de la recycler ou de la réutiliser.

10. Le suivi de l'usage des ordinateurs par les juges soulève de sérieuses questions en matière de vie privée, de confidentialité et d'indépendance des juges. Les juges en chef doivent demander à l'administrateur des systèmes compétent de leur expliquer dans quelle mesure et de quelle façon l'usage des ordinateurs par les juges et par le personnel judiciaire fait l'objet d'un suivi.

Pour plus de détails, prière de consulter les conseillers techniques du Sous-comité : Martin Felsky, président et conseiller juridique, Commonwealth Legal, (416) 703-3755, poste 226, mfelsky@commonwealthlegal.com, ou Jennifer Jordan, greffière, Cour d'appel de la Colombie-Britannique, (604) 660-3237, Jennifer.jordan@courts.gov.bc.ca

TRANSMISSION ÉLECTRONIQUE : ÉQUILIBRE ENTRE LA TRANSPARENCE JUDICIAIRE ET LE RESPECT DE LA VIE PRIVÉE

L'hon. Donald I. Brenner
Juge en chef de la Cour suprême de la Colombie-Britannique

M^me^ Judith Hoffman, conseillère juridique
Cour suprême de la Colombie-Britannique

Tiré de leur rapport préparé pour le Comité d'administration de la justice du Conseil canadien de la magistrature et intitulé *Transmission électronique, accès aux dossiers judiciaires et respect de la vie privée* :

Les tribunaux ne devraient adopter la transmission électronique des dossiers judiciaires qu'après avoir élaboré des politiques qui établissent un équilibre entre les considérations fondamentales de responsabilité, de respect de la vie privée et de droit d'accès.

La transmission électronique et l'accès électronique aux dossiers judiciaires amélioreront grandement l'efficacité des tribunaux et l'administration de la justice. Cependant, la nouvelle technologie modifiera également l'équilibre actuel entre la nécessité d'obtenir une transparence judiciaire et le droit des citoyens à la protection des renseignements personnels. De telles répercussions doivent être pleinement étudiées et des protections mises en place avant que les systèmes ne soient mis en oeuvre.

Les règles actuelles en matière d'accès tiennent pour acquis que tous les dossiers judiciaires sont à la disposition du public, sauf dans certaines circonstances limitées. En réalité, la vie privée des individus participant au processus judiciaire a été protégée par les difficultés, les efforts et le coût que comportent l'accès aux dossiers. L'accès aux dossiers nécessite habituellement une visite au greffe du tribunal, la récupération du dossier – parfois d'un autre lieu – et le paiement de frais de recherche. Les renseignements personnels sont donc protégés par ce qu'on appelle l'« obscurité pratique ».

L'accès électronique peut changer tout cela. Les recherches générales à distance sont rendues possibles sur simple pression d'un bouton. Les renseignements peuvent être récupérés, téléchargés, copiés, mis sous forme de tables et manipulés. Les renseignements potentiellement disponibles peuvent comprendre les détails se rapportant à

l'emploi, aux antécédents matrimoniaux ou médicaux, à la date de naissance, à l'identificateur personnel et aux renseignements financiers détaillés d'une partie à un litige. Les dossiers judiciaires peuvent exiger la communication de renseignements confidentiels ou de secrets commerciaux en cas d'ordonnance préventive.

Un conflit apparaît entre le droit à la vie privée des individus et le droit de la société à la transparence au sein de l'administration de la justice. Pour obtenir un équilibre, les tribunaux devraient élaborer des politiques d'accès afin de s'assurer qu'ils maintiennent le contrôle efficace des dossiers. Ces politiques devraient mettre en équilibre trois valeurs fondamentales :

- Responsabilité – le droit du public d'observer le fonctionnement du système judiciaire et de savoir comment et pourquoi les décisions sont prises par les tribunaux.
- Respect de la vie privée – le respect de la vie privée des parties au litige devant le tribunal.
- Accès – le droit d'accès aux tribunaux dont disposent les citoyens pour régler leurs différends de manière efficace.

Plusieurs approches de base en matière d'accès peuvent être adoptées en vue de l'élaboration d'un modèle de transmission et d'accès électronique.

- Une approche « de non-intervention » maintiendrait les présentes dispositions relatives à l'accès, mais obligerait la partie au litige à demander une ordonnance plaçant des dossiers sous pli scellé en cas de préoccupations en matière de vie privée. Les parties au litige risquent de ne pas avoir les ressources ou connaissances nécessaires pour défendre leurs propres intérêts.
- Une approche « de prise de contrôle » oblige le tribunal à analyser les renseignements contenus dans les dossiers et à supprimer les parties qui soulèvent des préoccupations en matière de vie privée. Une telle approche serait susceptible d'exiger un accroissement important du personnel du greffe du tribunal.
- Une troisième approche « axée sur les utilisateurs » accorderait l'accès à distance en fonction de l'identité de la personne demandant un tel accès. Une telle approche oblige également le tribunal à limiter l'accès.
- Une quatrième approche limiterait l'accès en fonction du type d'affaires. Par exemple, l'accès aux affaires pénales serait plus restreint que l'accès aux affaires au civil; l'accès aux affaires de faillite et familiales serait plus limité en raison des renseignements financiers et données d'identification de nature délicate.

Peu importe le modèle utilisé, toute politique d'accès électronique devrait se pencher sur les questions liées au contenu, à la forme, à l'accès et à l'utilisation des dossiers électroniques.

Contenu : les identificateurs personnels devraient-ils être supprimés? Dans l'affirmative, par qui? Certains types d'affaires ou catégories de documents devraient-ils faire l'objet d'une interdiction totale d'accès?

Forme des dossiers électroniques : les images de dossiers seront-elles disponibles?

Droit d'accès : l'accès sera-t-il octroyé au grand public sur Internet ou limité à des usagers inscrits? Dans le dernier cas, lesquels parmi les usagers inscrits auraient droit d'accès?

Utilisation des renseignements électroniques : l'utilisation à des fins commerciales ou de recherche, ou à d'autres fins ne se rapportant pas directement à l'administration de la justice; une telle utilisation nécessite l'adoption d'ententes d'accès établissant des restrictions relatives à l'utilisation.

La Cour suprême de la Colombie-Britannique a préparé sa propre ébauche de politique d'accès électronique à des fins de consultation avec les utilisateurs éventuels d'un système de transmission et d'accès électronique et avec le grand public. Les sept sections de l'ébauche se penchent sur les types de renseignements accessibles, la nature de l'accès et des recherches, la sécurité et l'authentification, les frais de service, les ententes d'accès électronique, l'accès à des fins commerciales et l'accès à des fins de recherche. Chaque section comprend un énoncé de principe, un énoncé de politique et une discussion des questions en jeu.

Le rapport de la Colombie-Britannique a été envoyé au Comité consultatif sur l'utilisation des nouvelles technologies par les juges et recommande que le Comité étudie la possibilité d'élaborer un modèle de base qui servirait de guide aux tribunaux confrontés à des questions de transmission et d'accès électronique.

LES TRIBUNAUX SUR INTERNET

De grands changements se sont produits au niveau du nombre, de la portée et de la qualité des sites Web exploités par les cours supérieures.

Le tableau suivant illustre les progrès obtenus jusqu'à présent au niveau de l'incorporation des caractéristiques clés.

PROGRÈS ET PLANS DES SITES WEB DES TRIBUNAUX

	Survol	Contacts	Règlement de cour	Formulaires	Jugements	FAQ	Discours	Rapports annuels
Cour suprême du Canada http://www.scc-csc.gc.ca	✔	✔	✔	✔	✔	✔	✔	✔
Cour fédérale du Canada http://www.fct-cf.gc.ca	✔	✔	✔		✔			✔
Cour d'appel de la Cour martiale du Canada http://www.cmac-cacm.ca	✔	✔	✔	✔				
Cour canadienne de l'impôt http://www.tcc-cci.gc.ca	✔	✔	✔	✔	✔	✔		✔
Terre-Neuve et Labrador http://www.gov.nf.ca/just/lawcourt/lcourt.htm	✔							
Île-du-Prince-Édouard http://www.gov.pe.ca/courts/supreme	✔	✔	✔	✔	✔			
Nouvelle-Écosse http://www.courts.ns.ca	✔	✔	✔	✔		✔		
Québec http://www.justice.gouv.qc.ca	✔	✔			✔			
Ontario http://www.ontariocourts.on.ca	✔	✔	✔		✔	✔	✔	
Manitoba http://www.manitobacourts.mb.ca	✔	✔	✔	✔	✔	✔		✔
Saskatchewan http://www.sasklawcourts.ca	✔		✔		✔			
Alberta http://www.albertacourts.ab.ca	✔		✔	✔	✔			
Colombie-Britannique http://www.courts.gov.bc.ca	✔	✔	✔		✔	✔		✔
Nunavut http://www.nunavutcourtofjustice.ca	✔	✔	✔		✔			

Le site de la Nouvelle-Écosse, qui a été lancé le 13 mai, comprend la visite virtuelle d'une salle d'audience, dans le cadre de son Projet de classe pour les enseignants et étudiants. L'Ontario étudie la possibilité d'ajouter une visite virtuelle d'Osgoode Hall.

La Cour fédérale du Canada prévoit ajouter des FAQ, des formulaires et des discours d'ici la fin de l'été. La Cour de justice du Nunavut prévoit ajouter des FAQ ainsi que son rapport annuel.

Un comité des services judiciaires étudie la possibilité de créer un site Web au Nouveau-Brunswick.

Dans le numéro 28 des *Actualités informatiques pour la magistrature* (http://www.cjc-ccm.gc.ca/francais/aim/aim_28.htm) (Automne-Hiver 1999-2000), Marilyn J. Hernandez et Susan Baer ont précisé ce qui suit :

Plusieurs raisons expliquent pourquoi les tribunaux veulent développer des sites web : pour faciliter l'accès aux tribunaux, aux documents et aux actes de procédure; pour accroître l'efficience du personnel; pour réduire la reproduction de l'information et les erreurs possibles et, en particulier, pour diffuser l'information qui a déjà été produite en format électronique par les tribunaux.

Le numéro 28 a offert la liste suivante des types de renseignements que les utilisateurs veulent obtenir sur les sites Web des tribunaux :

- annuaire et liste de personnes-ressources;
- décisions, en format standard, entièrement interrogeables en fonction d'une variété de champs à l'aide d'opérateurs booléens et de proximité;
- règlement du tribunal;
- horaire de la cour ou des auditions;
- formulaires juridiques/judiciaires;
- biographies ou liste des juges, avec photographies;
- personnel clé;
- instructions relatives à la pratique;
- avis à l'intention de la profession;
- renseignements historiques sur le tribunal, les juges, l'administration de la justice dans la province ou le territoire;
- aperçu de chaque tribunal ou cour;
- documents clés disponibles (par ex., lignes directrices en matière de pensions alimentaires);
- foire aux questions, c'est-à-dire une section où l'on répond aux questions posées par le public.

MARQUEZ D'UN SIGNET LES SITES SUIVANTS!

Bureau du Commissaire à la magistrature fédérale :

http://www.fja.gc.ca/

comprenant :
- l'accession à la magistrature;
- les liens aux sites Web des tribunaux fédéraux et provinciaux;
- les lois fédérales, provinciales et territoriales.

Conseil canadien de la magistrature :

http://www.cjc-ccm.gc.ca

comprenant :
- les rapports annuels;
- les numéros d'*Actualités informatiques pour la magistrature*;
- les publications, rapports et communiqués;
- les règlements du Conseil;
- FAQ.

Le Comité consultatif sur l'utilisation des nouvelles technologies par les juges du Conseil canadien de la magistrature publie les *Actualités informatiques pour la magistrature* à l'intention des juges. Les opinions exprimées sont celles des auteurs et ne reflètent pas nécessairement les vues du comité ou du Conseil. Les textes publiés peuvent être reproduits sans autorisation, pourvu qu'on fasse mention de leur origine.

On peut trouver les *Actualités informatiques pour la magistrature* dans Internet à www.cjc-ccm.gc.ca.