Ordinateurs : Modèle de règles d'utilisation acceptable pour le personnel judiciaire

Approuvé par le Comité exécutif du Conseil canadien de la magistrature
Le 5 décembre 2003

1.0 Aperçu général

1. Le gouvernement <fédéral/provincial> met des moyens informatiques à la disposition des juges et du personnel de soutien judiciaire dans l'exercice de leurs fonctions.

2. Les présentes règles énoncent, en ce qui concerne l'utilisation des moyens informatiques, des lignes directrices qui serviront à protéger ces moyens contre les actions illicites ou dommageables, qu'elles soient délibérées ou non, à assurer le rendement optimum des systèmes d'ordinateur pour tous les juges et le personnel de soutien judiciaire, et à permettre aux juges et au personnel de soutien judiciaire de faire un certain usage de ces moyens à des fins personnelles, contribuant à renforcer leur efficacité et productivité.

3. Le premier objectif est de protéger l'appareil judiciaire et la sécurité des données judiciaires par le maintien d'une protection efficace, ce qui requiert la participation et la coopération de chacun des juges et des membres du personnel de soutien qui fait usage des données et/ou des systèmes d'information. Un abus des moyens informatiques expose l'appareil judiciaire à certains risques, tels les attaques virales, la compromission des systèmes et services du réseau, les problèmes légaux, les atteintes éventuelles à la sécurité et la diminution de l'efficacité du réseau.

2.0 Objet

Les présentes règles ont pour objet de définir l'usage acceptable et les pratiques exemplaires concernant les moyens informatiques au sein de la <désignation de la juridiction concernée>.

3.0 Champ d'application

Les présentes règles s'appliquent aux juges et au personnel de soutien judiciaire. Le juge en chef peut les étendre aux fournisseurs, aux consultants, aux employés judiciaires temporaires et autres, en les incorporant par référence dans les contrats ou mémoires d'entente à titre de condition pour l'utilisation des moyens informatiques.

4.0 Définitions

Aux fins des présentes règles les définitions qui suivent s'appliquent

Moyens informatiques s'entend notamment des ordinateurs portatifs, des ordinateurs personnels et de leurs périphériques, du logiciel, de la connectivité Internet, de l'accès aux services Internet/Intranet/Extranet/VPN, et du courriel. Cette liste donne juste quelques exemples de moyens informatiques soumis aux présentes règles; elle n'est pas exhaustive.

Temps libre de l'employé s'entend des périodes où le personnel de soutien judiciaire n'est pas censé exercer ses fonctions, comme par exemple les heures hors service qui précèdent ou suivent une journée de travail, les pauses-déjeuner ou autres pauses autorisées.

Personnel de soutien judiciaire s'entend des employés qui sont directement sous les ordres des juges : adjoints judiciaires, secrétaires, consultants, étudiants stagiaires et clercs.

Usage personnel restreint s'entend de l'utilisation des moyens informatiques par les juges et le personnel de soutien judiciaire en dehors de l'exercice de leurs fonctions, par exemple pour les activités professionnelles, le perfectionnement, et l'usage personnel accessoire dans les limites du raisonnable. Est exclue la modification des moyens informatiques en usage, par exemple la modification de la configuration.

Surcroît de dépenses minimal s'entend du fait que l'usage des moyens informatiques ne doit avoir pour autre résultat que l'usure normale ou la consommation de très peu d'électricité, d'encre, de poudre imprimante ou de papier. À titre d'exemple, il s'agit de se servir de l'imprimante de l'ordinateur pour imprimer un nombre limité de pages, d'envoyer rarement des courriels et d'utiliser l'Internet occasionnellement.

5.0 Règles

5.1 Sécurité et renseignements exclusifs

1. Les juges et le personnel de soutien judiciaire qui utilisent des moyens informatiques fournis par le gouvernement <fédéral/provincial> ont la responsabilité de se familiariser avec les présentes lignes directrices et de les respecter dans l'exercice de leurs activités.

2. Les juges et le personnel de soutien judiciaire doivent prendre toutes les mesures nécessaires pour prévenir l'accès non autorisé aux renseignements confidentiels.

3. Les juges et le personnel de soutien judiciaire doivent chiffrer les renseignements à protéger, conformément aux lignes directrices de la Cour en matière de sécurité.

Les projets de jugement doivent être chiffrés avant d'être envoyés par courriel au personnel de soutien judiciaire ou à d'autres juges, à moins que la transmission ne se fasse dans JUDICOM ou un système de courriel interne sûr.

4. Le service <fédéral/provincial> de Technologie de l'information peut, avec le consentement du juge en chef, exercer une surveillance limitée sur les moyens et les systèmes informatiques ainsi que sur le trafic sur le réseau informatique, conformément aux lignes directrices en matière de contrôle approuvées par le Conseil canadien de la magistrature, et conformément aux présentes lignes directrices. Dans le but d'assurer l'intégrité des ressources partagées du réseau et de protéger les systèmes informatiques contre les menaces à leur sécurité, des procédures peuvent être mises en œuvre pour surveiller le trafic sur le réseau, consigner les erreurs et les exceptions, et assurer la maintenance des moyens informatiques conformément aux normes de l'industrie. Par contre, aucune surveillance fondée sur le contenu des données n'est autorisé.

5. Les juges et le personnel de soutien judiciaire sont responsables de la sécurité de leur mot de passe et de leur compte. Les mots de passe doivent être protégés, et les comptes ne doivent pas être partagés. Les mots de passe doivent être changés tous les trimestres au niveau du système, et tous les six mois au niveau individuel. Il ne faut pas utiliser le même mot de passe pour différents comptes, et il ne faut pas le consigner dans l'ordinateur ou le navigateur Web. Le mot de passe doit comprendre au moins six caractères en une combinaison de chiffres, de lettres et de caractères alphanumériques; il ne faut pas que ce soit un mot ayant une signification.

6. Tous les ordinateurs, ordinateurs portatifs et postes de travail doivent être sécurisés au moyen d'un économiseur d'écran protégé par mot de passe avec activation automatique toutes les 10 minutes ou moins, ou par la fermeture de la session si l'ordinateur est laissé sans surveillance.

7. Les données mémorisées dans les ordinateurs portatifs étant particulièrement vulnérables, il ne faut jamais laisser ces derniers sans surveillance mais, si possible, les protéger par un mot de passe d'accès ou par un câble anti-vol.

8. Les juges et le personnel de soutien judiciaire doivent mettre fin à leur système et éteindre leur ordinateur à la fin de la journée de travail.

9. Tous les ordinateurs utilisés par les juges et le personnel de soutien judiciaire et branchés sur le réseau Internet/Intranet/Extranet/VPN de la Cour, qu'ils leur appartiennent en propre ou soient la propriété du <gouvernement fédéral/provincial>, doivent exécuter continuellement un programme approuvé et à jour de détection des virus.

10. Les juges et le personnel de soutien judiciaire doivent être prudents lorsqu'il s'agit d'ouvrir les pièces jointes au courriel envoyé par des inconnus, car elles peuvent contenir des virus.

11. Les documents importants et les travaux produits doivent être sauvegardés pour mémoire dans un serveur ou autre support sécurisé et fiable, conformément aux modalités de sauvegarde fixées par la Cour.

12. Il faut observer les procédures appropriées pour s'assurer que les jugements et autres documents transmis à l'extérieur de l'environnement sécurisé de la Cour ne renferment ni information cachée ni méta données, tels les révisions ou ratures sur des projets antérieurs ou des renseignements confidentiels.

13. Lorsqu'il s'agit de se débarrasser des ordinateurs, lecteurs, disquettes ou autres supports de mémoire, il faut observer des procédures qui soient adaptées à la sensibilité des données mémorisées. Il ne suffit pas d'effacer les fichiers, il faut les formatter avant de recycler ou de réutiliser les supports de mémoire. Dans certains cas, il faut détruire ces supports, conformément aux politiques en la matière de la Cour.

5.2 Usage personnel restreint

1. Les moyens informatiques servant dans l'exercice des fonctions judiciaires peuvent être utilisés à des fins personnelles à condition que cet usage ne coûte rien ou très peu aux contribuables. Pareil usage peut ajouter à l'efficacité et à la productivité des juges et du personnel de soutien judiciaire dans leur vie professionnelle et personnelle. Il peut aussi être utile aux juges qui doivent se déplacer pour présider des audiences à l'extérieur de leur ville de résidence.

2. Un usage personnel restreint des moyens informatiques est permis aux membres du personnel de soutien judiciaire s'il n'entrave pas l'exercice de leurs fonctions et n'occasionne qu'un surcroît de dépenses minime. Il ne peut avoir lieu que pendant leur temps libre, et peut être supprimé ou réduit à n'importe quel moment par le juge en chef.

3. Un usage personnel restreint des moyens informatiques est permis aux juges s'il n'entrave pas l'exercice de leurs fonctions et n'occasionne qu'un surcroît de dépenses minime.

4. Lorsqu'ils utilisent à titre personnel et de façon restreinte les moyens informatiques mis à leur disposition, les juges et le personnel de soutien judiciaire doivent toujours se garder de donner l'impression qu'ils le font à titre officiel. Si cet usage personnel restreint est susceptible d'en donner l'impression, il faut ajouter un désaveu, par exemple : « Le contenu de ce message est personnel et ne représente pas les vues des juges ou de la Cour. »

5. Les contributions que les juges ou le personnel de soutien judiciaire envoient à partir d'une adresse électronique de la Cour à un forum privé doivent comprendre l'avertissement que les opinions exprimées sont strictement celles de l'auteur et non pas nécessairement celles de la Cour, à moins que cette contribution ne soit faite dans le cadre de ses fonctions officielles.

Les usagers doivent s'abstenir d'utiliser les adresses électroniques de la Cour relativement à leurs contributions personnelles à un forum public ou aux messages personnels qu'ils affichent sur un babillard public. La raison d'être de cette règle est que de telles contributions ou de tels messages accroissent les risques de ciblage à des fins de marketing ou à des fins malveillantes.

5.3. Usage inacceptable

L'usage inacceptable des moyens informatiques s'entend de ce qui suit :

5.3.1. Manœuvres visant à déjouer la protection

a) contourner l'authentification de l'usager ou la protection d'un ordinateur, réseau ou compte, quel qu'il soit.

b) entraver ou empêcher le service pour tout autre usager.

c) utiliser un programme/script/commande, quel qu'il soit, ou envoyer des messages, quels qu'ils soient, pour entraver ou désactiver une session de tout autre usager, par quelque moyen que ce soit, localement ou par Internet/Intranet/Extranet/VPN.

5.3.2. Atteinte au rendement

a) tout usage personnel qui pourrait causer l'encombrement, le retard ou l'interruption du service pour le système de quelque juridiction ou gouvernement que ce soit, par exemple le téléchargement de gros fichiers audio ou vidéo.

b) l'utilisation des moyens informatiques de façon à causer une perte de productivité, à entraver l'exercice des fonctions officielles, ou à causer un surcroît de dépenses appréciable pour le Trésor public.

5.3.3. Actes illicites ou immoraux

a) l'utilisation des moyens informatiques à des fins illicites, ce qui s'entend des infractions criminelles, des contraventions aux lois et règlements non pénaux, fédéraux et provinciaux, et de toute action qui expose un individu ou une institution à une action civile.

b) la transmission non autorisée de données judiciaires aux forums, babillards ou autres sites publics, y compris toute utilisation qui pourrait donner l'impression que la communication a été faite à titre officiel.

c) la création ou l'envoi de lettres en chaîne, de courriel spam ou autres messages à diffusion massive, quel qu'en soit le sujet, sans y être autorisé ou sans que les destinataires en aient fait la demande.

d) l'utilisation des moyens informatiques à des fins professionnelles ou commerciales privées.

e) Les activités suivantes sont aussi interdites, sauf dans la mesure où elles sont requises dans l'exercice des fonctions judiciaires :

   i) la création, le téléchargement, la visualisation, la sauvegarde, ou la transmission de représentations explicites d'actes sexuels, de documents inappropriés ou offensants pour les collègues ou pour le public, par exemple la propagande haineuse, ou de documents touchant aux jeux de hasard illégaux et à d'autres activités illégales ou interdites.

   ii) la communication, à des gens de l'extérieur qui ne font partie ni de la Cour ni du ministère de la Justice, de données confidentielles de la Cour ou de données judiciaires confidentielles, notamment des listes de juges ou de membres du personnel de soutien judiciaire.

5.3.4. Atteinte à la protection du système

a) l'introduction dans les réseaux ou serveurs des programmes destructeurs, tels les virus.

b) la révélation du mot de passe d'un compte à autrui, à moins que ce ne soit à un usager autorisé et conformément à la politique de la Cour.

c) le fait de permettre à d'autres, y compris aux membres de la famille et du ménage, de se servir du mot de passe d'un compte ou de se servir d'un ordinateur connecté au VPN ou à l'Extranet de la Cour, en cas de travail fait à la maison.

d) le fait d'essayer d'accéder sans autorisation à d'autres systèmes.

5.3.5. Infractions techniques

a) créer des brèches de sécurité ou perturber les communications dans le réseau. Brèche de sécurité s'entend entre autres de l'accès aux données qui ne sont pas destinées au juge ou au membre du personnel de soutien

judiciaire concerné, accéder à un serveur ou un compte auquel il ne possède pas les permissions d'accès, à moins que ces activités soient requises dans le cadre normal de ses fonctions.

b) exploration du point d'accès ou du dispositif de protection, sauf autorisation préalable du service de Technologie de l'information.

c) toute manoeuvre de surveillance du réseau qui intercepte des données qui ne sont pas destinées au juge ou à l'employé concerné.