Lignes directrices sur la surveillance informatique

Recommandées par le Comité consultatif des juges sur la technologie, juillet 2002
Approuvées par le Conseil canadien de la magistrature, septembre 2002

[1] En général, la surveillance informatique consiste à utiliser un logiciel pour suivre les activités informatiques. La surveillance peut inclure le suivi des activités dans un réseau, des menaces à la sécurité, de l'usage d'Internet, de l'entrée de données, du courriel et des autres activités informatiques des utilisateurs individuels. La surveillance est effectuée par une personne autre que l'utilisateur, et elle peut se faire à la connaissance ou à l'insu de l'utilisateur. Dans l'un ou l'autre cas, l'utilisateur n'a aucun contrôle sur les activités de surveillance ni sur les données qui en résultent.

[2] La protection efficace des réseaux informatiques contre les menaces à la sécurité exige certaines activités de surveillance. Cependant, certaines formes de surveillance informatique peuvent compromettre gravement l'indépendance judiciaire et constituer également une atteinte illégale à la vie privée. Ces lignes directrices ont pour but d'aider les juges et les administrateurs de système à établir des pratiques de surveillance appropriées.

[3] Par principe, il est primordial que toute surveillance informatique des juges et du personnel judiciaire qui relève directement des juges ait un but bien défini et justifiable qui n'empiète pas sur le secret du délibéré, la confidentialité, le droit à la vie privée ou l'indépendance judiciaire.

[4] La surveillance du contenu des appareils informatiques des juges et du personnel judiciaire n'est pas permise en aucune circonstance. Les activités interdites comprennent l'enregistrement de frappe, la surveillance du courriel, de documents de traitement de texte ou d'autres fichiers informatiques, et le suivi des recherches juridiques, des sites Internet consultés et des dossiers téléchargés par les utilisateurs individuels.

[5] Afin de protéger l'intégrité des ressources des réseaux partagés et de protéger les systèmes informatiques contre les cyberpirates et d'autres menaces à la sécurité, des procédures peuvent être établies pour surveiller le trafic des réseaux, consigner les erreurs et les anomalies, et effectuer des travaux de maintenance selon les normes de l'industrie.

[6] Toute surveillance des systèmes pour en assurer l'intégrité et la sécurité doit :

- Être faite seulement pour des raisons légitimes liées à la performance des réseaux ou à la gestion de la sécurité des réseaux;

- Employer la méthode la moins intrusive qui soit raisonnablement disponible. Par exemple, si une certaine activité a un effet sur les ressources du réseau, les administrateurs de système doivent s'efforcer d'obtenir la conformité volontaire des juges et du personnel judiciaire en les informant de leurs préoccupations spécifiques concernant les technologies de l'information.

- Recueillir seulement de l'information en forme agrégée. Il est interdit de surveiller les activités informatiques et les habitudes d'utilisation des juges individuels et du personnel judiciaire, sauf pour s'assurer que les utilisateurs sont connectés légitimement.

[7] La surveillance des données doit demeurer confidentielle. L'accès doit être limité au personnel de technologies de l'information qui a besoin des données pour résoudre les problèmes d'intégrité et de sécurité des systèmes. Les registres de surveillance électronique et les autres fichiers doivent être effacés régulièrement. Il est permis de conserver de l'information statistique tirée des données de surveillance, à condition que cette information soit en forme agrégée et qu'elle ait rapport seulement à des questions d'intégrité et de sécurité des sytèmes.

[8] Aucune surveillance informatique ne peut être faite sans le consentement du juge en chef de la cour. Les juges et le personnel judiciaire doivent jouer un rôle fondamental dans l'élaboration et la gestion des pratiques de surveillance qui sont conformes aux présentes lignes directrices. Toute surveillance doit être administrée par un personnel qui relève directement du juge en chef de la cour et qui n'est responsable que devant ce dernier.

[9] Les juges et le personnel judiciaire doivent être informés des pratiques de surveillance au moyen d'avis clairs, précis et cohérents. Les cours devraient établir des politiques d'utilisation acceptable et les communiquer aux juges et au personnel judiciaire lorsqu'on leur donne accès à un ordinateur pour la première fois. Lorsque les utilisateurs se connectent au réseau, un message devrait s'afficher à l'écran pour leur rappeler régulièrement les politiques en vigueur et les raisons de ces politiques.