



## Dossier Utilisation de l'informatique au travail

# Une problématique toujours d'actualité

## Histoire d'une intervention ratée

### Quoi faire et ne pas faire

*On aurait cru, après l'avènement d'Internet au travail et la multiplication de politiques et procédures en matière d'utilisation des équipements informatiques qui en a découlé, que la problématique de l'usage abusif ou inapproprié d'Internet au travail était, à toutes fins pratiques, réglée. Or, il n'en est rien. Même avec une politique claire, les coûts liés au vol de temps de travail dû à la navigation à des fins personnelles ne cessent d'augmenter.*

Dans une décision récente, la Commission des relations du travail a donné raison à l'employeur et maintenu le congédiement d'un employé. L'employé en question était responsable du réseau informatique. Une politique concernant l'utilisation des systèmes informatiques et du courrier électronique a été adoptée en juin 2003.

L'employé en a reçu une copie, et comme tous les employés, il a dû la signer.

La preuve a révélé qu'entre le 30 octobre 2007 et le 9 janvier 2008, l'employé a utilisé l'ordinateur mis à sa disposition à des fins personnelles durant les heures de travail pour une durée moyenne quotidienne, établie de façon très conservatrice, d'une heure et demie. L'employé a tenté régulièrement et systématiquement d'avoir accès à des sites à caractère sexuel et pornographique, ainsi qu'à des sites de rencontres, de musique et de clavardage, dont l'accès lui était interdit.

Pendant la période de six mois comprise entre janvier et juin 2007, on a constaté qu'on naviguait sur le poste opéré exclusivement par l'employé pendant environ 45 heures par mois, avec une pointe culminante de plus de 82 heures, en mai 2007.

Entre janvier et juin 2007, l'employé a passé environ 50 % de son temps de travail, au bureau, à naviguer sur Internet. On a également constaté que l'utilisation que faisait l'employé de son poste représentait, mois après mois, plus de 10 % du nombre d'heures totales utilisées par les quelque 90 ordinateurs de l'employeur.

Une rencontre d'information au printemps 2007 n'empêche pas l'employé, quelques semaines plus tard, de briser tous les records d'utilisation d'Internet, sans compter, au mois d'août suivant, ses 1766 tentatives bloquées, dont plusieurs sur des sites de rencontres pour célibataires.

La Commission souligne que l'employé n'a pas contesté avoir navigué sur Internet plus de 25 000 fois en quelque trente mois, admettant lui-même que 96 % de ses navigations étaient de nature personnelle.

On voit que l'existence d'une politique peut s'avérer insuffisante pour prévenir les abus. Cependant, la découverte d'une utilisation répréhensible, voire criminelle, d'un poste ou du réseau informatique d'une entreprise par un employé ou un collègue a de quoi confondre tout gestionnaire. Surtout lorsque l'employé suspecté est l'administrateur réseau.

📖 Comment s'y retrouver entre preuve numérique, encapsulation, volatilité des données et chaîne de possession?

📖 Connaissez-vous la bonne façon de colliger la preuve afin qu'elle réponde aux critères établis par les tribunaux en matière de délit informatique?

📖 Qui intervient en premier lieu? Et comment?

Pour répondre à ces questions, SIRCO vous propose un dossier thématique en trois volets :

1. Petite histoire d'une intervention manquée;
2. Règles spécifiques à la collecte d'une preuve informatique;
3. Quoi faire et ne pas faire sur une scène d'incident ou de délit informatique.

## Étude de cas : l'opération Pinson

### Appel initial des TI

Le superviseur TI avise le département des ressources humaines qu'un employé navigue sur Internet de façon abusive. Il ne peut, pour le moment, définir quels sites sont consultés, mais le nombre et la durée du temps de navigation semblent problématiques.

### Demande d'analyse par les ressources humaines

Les ressources humaines demandent au superviseur TI de faire enquête.

Le superviseur TI décide de rester au travail un peu plus tard afin de procéder à une analyse partielle du poste de l'employé.

Il démarre le poste et accède au compte de l'employé. Le superviseur passe une partie de la soirée à vérifier le contenu du poste, les logiciels installés ainsi que les navigations Internet à partir de l'historique de navigation contenu dans le fureteur. Une fois la vérification terminée, le superviseur TI procède à la fermeture de la session Windows et quitte.

Le matin suivant, il rencontre les ressources humaines et leur fait part de ses découvertes :

- Plusieurs logiciels non reliés au travail et possiblement piratés sont installés sur le poste de l'employé;
- Plusieurs navigations Internet mènent vers des sites de clavadage et de pornographie.

### Décision des RH

Après discussion avec la direction, les RH décident de suspendre l'employé.

### Journée de la suspension

Un représentant des RH, accompagné d'un gardien de sécurité, rencontre l'employé et l'avise, personnellement et par écrit, de sa suspension, effective immédiatement.

### Mandat d'enquête aux TI

Les RH mandatent le superviseur TI pour saisir le poste de l'employé, procéder à l'analyse et produire un rapport.

### Saisie du poste informatique

Le superviseur TI va dans le bureau de l'employé et :

- ferme le système d'exploitation en initiant la séquence de fermeture.;
- débranche tous les connecteurs à l'arrière du poste et apporte le poste dans son bureau pour procéder à l'analyse;
- retire le disque dur du poste et le branche sur sa station de travail.

### Analyse

Le superviseur TI procède à l'analyse des données contenues sur le disque dur de l'employé. Il collecte les éléments de preuve et les compile sur un DVD.

Une fois la collecte des données terminée, le superviseur TI produit un rapport d'enquête.

*À suivre...*

Le responsable TI a, sans le savoir, commis plusieurs erreurs pouvant compromettre la preuve recueillie et la légalité de son intervention. Dans notre prochain numéro, nous verrons les règles applicables à la collecte d'une preuve informatique.