

LA SURVEILLANCE ÉLECTRONIQUE DES EMPLOYÉS SOUS L'ANGLE DU DROIT DU TRAVAIL

Il est incontestable que les outils de communication informatiques permettent aux entreprises de réduire leurs coûts et d'accroître leur productivité. Toutefois, l'utilisation induite de ces moyens technologiques peut s'avérer dommageable pour les employeurs; notamment, impact négatif sur le temps de travail, transfert de données sensibles, surcharge de la capacité de stockage, risques d'infiltration de virus. L'image de la société peut s'en trouver ternie selon les manipulations frauduleuses exécutées.

Un règlement d'utilisation? Sur le lieu de travail, les employés n'ont aucun droit à l'utilisation électronique des moyens de communication à des fins privées. A tout le moins, les employés doivent utiliser ces moyens de communication de façon raisonnable eu égard à leur devoir de diligence et de fidélité selon l'art. 321 a CO. La portée pratique de cette règle dans le cas d'espèce est toutefois limitée en l'absence d'instructions de l'employeur. Ce dernier a la faculté de donner des directives aux travailleurs concernant notamment l'exécution du travail, en vertu de l'art. 321 d al. 1 CO. Il peut interdire complètement l'utilisation privée d'Internet ou en restreindre l'usage au moyen d'un règlement d'utilisation. Celui-ci doit être suffisamment clair et précis afin de définir concrètement l'utilisation abusive des moyens informatiques par un employé et d'en présenter les conséquences (sanctions). Il est évident que les collaborateurs doivent être informés de l'existence d'un règlement d'utilisation à ce sujet et en avoir connaissance.

Analyse anonyme de l'activité électronique? L'employeur peut faire usage (a) de mesures préventives dans le but de minimiser les risques (mise en place d'un programme anti-virus, système de blocage de certains sites web, mesures de sauvegarde automatique, entre autres) ou (b) de mesures de surveillance afin de constater et de sanctionner les éventuels abus. Il est toutefois proscrit de mettre en place un système de contrôle visant à surveiller le comportement des travail-

leurs à leur poste de travail (art. 26 al. 1 Ordonnance 3 relative à la loi sur le travail, OLT 3). Le système de surveillance ne doit ainsi pas porter atteinte à leur santé et à leur liberté de mouvement (art. 26 al. 2 OLT 3). Sont ainsi exclus, les enregistreurs de frappes et les programmes d'enregistrement de l'activité de l'employé à son poste de travail. Le moyen de contrôle doit être aléatoire et anonyme. Un pseudonyme peut par exemple être attribué aux employés sous la forme d'une combinaison de lettres et/ou de chiffres afin de garantir une analyse anonyme de l'activité informatique globale de la société. En cas de constatation d'abus uniquement, une liste de correspondance confidentielle permettrait d'identifier l'employé fautif.

Mesures à la disposition de l'employeur. Les sanctions découlant du droit du travail à disposition de l'employeur en cas d'abus vont de l'avertissement au licenciement pour les cas graves et répétés. Ces sanctions doivent figurer dans le règlement d'utilisation. De plus, «le travailleur répond du dommage qu'il cause à l'employeur intentionnellement ou par négligence» (art. 321 e al. 1 CO). L'employeur peut en outre emprunter la voie pénale selon les infractions commises. A l'inverse, si le système de contrôle a pour conséquence une atteinte illicite à la personnalité de son collaborateur, l'employeur peut engager sa responsabilité. Un éventuel licenciement pourrait être considéré comme abusif et exposer l'employeur au paiement de potentielles indemnités de salaire.

Dernièrement, le Tribunal administratif fédéral a validé le système de surveillance d'un employeur (arrêt A-5641/2014 du 8 décembre 2015). Préventivement, le système envoyait un avertissement (sous forme de fenêtre intrusive, *pop-up window*) informant l'utilisateur qu'il consultait une catégorie de site interdit, garantissant son anonymat. Cet avertissement comportait un lien au règlement interne d'utilisation d'Internet et précisait «l'infraction» commise ainsi que la sanction afférente. Dans les faits, l'abus était manifeste puisque l'employé avait passé plus de 80 heures de consultation sur ces sites interdits en 17 jours de travail. ■



ROMAIN DELAVY,
JURISTE,
FJF FAVRE JURIDIQUE
ET FISCAL SA,
LAUSANNE/VD