Droit & Technologies

Depuis 1997, le Portail du Droit des Nouvelles Technologies

Cybersurveillance des travailleurs: synthèse de la réglementation belge

25/06/2004 Lu par 6910 visiteur(s)

Thème(s) : Propriété littéraire et artistique (droits d'auteur)

Chronique « droit & multimédia » parue le 3 juin dans l Echo

Il y a quelques jours, l actualité se faisait encore l écho de cet épineux problème que constitue la surveillance des travailleurs par le biais des ressources informatiques qui sont mises à leur disposition par leur employeur.

Ainsi, la presse n a pas manqué de relater les faits survenus ces derniers mois chez Electrabel où une équipe de spécialistes en sécurité informatique, accompagnée du président du conseil d administration d Electrabel, pénétrait de nuit dans les locaux de la société pour vérifier la fiabilité du système informatique ainsi que les soupçons de divulgation de documents par un cadre.

Cet incident illustre le problème de la cybersurveillance du travailleur par l employeur ou comment concilier des droits divergents.

Ainsi, sous l angle de l employeur, il est tout à fait justifié et légitime de contrôler la productivité de ses employés. Ce principe est par ailleurs consacré par la loi du 3 juillet 1978 relative au contrat de travail qui stipule que l employeur dispose du droit de veiller à ce que l employé exécute le travail pour lequel il est rémunéré.

Les technologies de l information et de la communication et leur évolution nécessitent des mesures accrues pour assurer la sécurité des informations et de l infrastructure mais permettent également de multiplier et de raffiner les contrôles qui peuvent être opérés.

Cependant, de tels contrôles doivent être conciliables avec le droit de l employé au respect de sa vie privée. En effet, il est désormais admis que le travailleur bénéficie d une sphère de vie privée sur son lieu de travail. A à ce titre, il jouit donc d une certaine protection contre un contrôle intempestif de la part de l employeur de l usage qu il fait des moyens de communications mis à sa disposition pour l exécution de son contrat de travail.

L équilibre entre ces exigences divergentes est délicat à trouver et a fait l objet d un dialogue entre les différents partenaires sociaux. Le résultat de ce dialogue est matérialisé par la convention collective de travail n° 81 du 26 avril 2002, conclue au sein du Conseil national du Travail, relative à la protection de la vie privée des travailleurs à l égard du contrôle des données de communication électronique en réseau, rendue obligatoire par arrêté royal du 12 juin 2002 (ci-après CCT 81).

Portée de la CCT 81

L article 1er de la CCT 81 établit la portée de la convention comme suit : « *§ 1er. La présente convention collective de travail a pour but de garantir le respect du droit fondamental des travailleurs au respect de leur vie privée dans la relation de travail, en définissant, compte tenu des nécessités d'un bon fonctionnement de l'entreprise, pour quelles finalités et à quelles conditions de proportionnalité et de transparence un contrôle des données de communication électroniques en réseau peut être installé et les modalités dans lesquelles l'individualisation de ces données est autorisée. Elle ne porte pas préjudice aux dispositions plus favorables prévues au niveau de la commission paritaire ou de l'entreprise. § 2. La présente convention collective de travail ne vise pas les modalités d'accès et/ou d'utilisation des moyens de communication électroniques en réseau de l'entreprise qui sont de la prérogative de l'employeur. Cette convention laisse donc en l'état les règles et pratiques d'information voire de consultation éventuellement en vigueur dans les entreprises. Elle ne porte pas non plus préjudice aux règles et pratiques existant dans les entreprises en ce qui concerne l'exercice des activités syndicales.* ».

La convention fait référence à un certain nombre de dispositions légales auxquelles elle n entend aucunement déroger. Ainsi, les limitations posées et l article 109 ter D et E de la loi du 21 mars 1991 (loi « Belgacom ») qui garantit le secret des communications doivent être appliquées à la lettre. De même, et bien que la référence ne soit pas indiquée au sein de la convention, il n est pas non plus dérogé à l article 314 bis du Code pénal qui interdit les écoutes de communications ou télécommunication privées.

Une distinction doit être opérée entre les données de communication et le contenu de la communication. La convention autorise, moyennant le respect des principes et procédures établis, la prise de connaissance des données de communication mais interdit la prise de connaissance du contenu des communications (par exemple, un e-mail).

Les données de communication électronique en réseau sont définies comme étant « les données relatives aux communications électroniques transitant par réseau, entendues au sens large et indépendamment du support par lequel elles sont transmises ou reçues par un travailleur dans le cadre de la relation de travail ». Compte tenu de cette définition large et technologiquement neutre, les communications électroniques en réseau tant internes qu externes sont visées et notamment la consultation de site internet, les e-mails, les forums de discussion mais aussi les messages envoyés par le biais des GSM (SMS, MMS, WAP)

On notera que la convention exclut expressément de son champ d application les modalités d accès ou d utilisation des ressources informatiques mises à la disposition des travailleurs. Ainsi, l employeur reste tout à fait libre de fixer ces conditions d accès et d utilisation. Il devra cependant respecter les principes énoncés par la convention dès lors qu il s agira de contrôler le respect de ces conditions d utilisation et d accès.

Par ailleurs, il semble que les garanties offertes par la CCT 81 ne s appliquent qu aux communication privées et non professionnelles. En effet, bien que cela ne soit pas précisé au sein du texte lui-même, le rapport précédant la convention prévoit que lorsque l objet et le contenu des données de communication électronique en réseau ont un caractère professionnel non contesté par le travailleur, l employeur pourra prendre connaissance de ces données sans autre procédure étant donné que le bon fontionnement de l entreprise doit être assuré. Un e-mail ayant un caractère professionnel non contesté pourra donc être consulté par l employeur et sans formalité.

Les principes du contrôle : finalité, proportionnalité et transparence

Finalité En vertu de ce principe, le contrôle envisagé doit viser des finalités précises et doit être nécessaire et indispensable à la réalisation de ces finalités, à savoir que la ou les finalités ne peuvent être atteintes sans le moyen de contrôle et aucun autre moyen ne permet d atteindre ces finalités. L article 5 de la CCT 81 prévoit une liste de quatre finalités : (i) la prévention de faits illicites ou diffamatoires, de faits contraires aux bonnes moeurs ou susceptibles de porter atteinte à la dignité d'autrui; (ii) la protection des intérêts économiques, commerciaux et financiers de l'entreprise auxquels est attaché un caractère de confidentialité ainsi que la lutte contre les pratiques contraires; (iii) la sécurité et/ou le bon fonctionnement technique des systèmes informatiques en réseau de l'entreprise, en ce compris le contrôle des coûts y afférents, ainsi que la protection physique des installations de l'entreprise ; (iv) le respect de bonne foi des principes et

règles d'utilisation des technologies en réseau fixés dans l'entreprise.

Cette liste est exhaustive et est censée regrouper toutes les circonstances d abus ou d anomalies que l on pourrait rencontrer dans le cadre d une relation de travail entre employeur et employé.

Selon les commentaires accompagnant la convention, sous la première finalité (faits illicites ou diffamatoires, faits contraires aux bonnes moeurs ou susceptibles de porter atteinte à la dignité d'autrui) on peut notamment rencontrer des actes de piratage informatique, dont la prise de connaissance non autorisée de données de communication électroniques en réseau relatives à la gestion du personnel ou de fichiers médicaux confidentiels, ou bien encore la consultation de sites à caractère pornographique ou pédophile, la consultation de sites incitant à la discrimination, à la ségrégation, à la haine ou à la violence à l'égard d'un groupe, d'une communauté ou de leurs membres, en raison de la race, de la couleur, de l'ascendance, de la religion ou de l'origine nationale ou ethnique de ceux-ci ou de certains d'entre eux.

Les actes visés sous la seconde finalité (pratiques contraires aux intérêts financiers, économiques et commerciaux de l'entreprise) peuvent, par exemple, prendre la forme de publicité dénigrante au sens de l'article 23, 6° de la loi du 14 juillet 1991 sur les pratiques du commerce et sur l'information et la protection du consommateur, de divulgation de fichiers ainsi que de la violation des secrets d'affaires y compris la recherche et le développement, les processus de fabrication et toutes données confidentielles.

Proportionnalité Même s il poursuit l une des finalités décrites et qu il est légitime, le contrôle envisagé doit être aussi restreint que possible. Le moyen de contrôle reste admissible tant que des moyens moins nuisibles ne peuvent pas être mis en uvre pour atteindre les finalités. En l espèce, il s agit de ne collecter en vue du contrôle que les données de communication en réseau qui sont nécessaires au contrôle. Seules les données ayant un caractère adéquat, pertinent et non excessif par rapport à la finalité poursuivie pourront être traitées. L ingérence dans la vie privée du travailleur doit être réduite au minimum.

Transparence L employeur qui souhaite mettre en place un système de contrôle des données de communication électronique en réseau doit en informer les travailleurs. Le support de cette information est laissé au choix de l employeur étant entendu que l information doit être effective, compréhensible et mise à jour. Cette information doit s effectuer à un double niveau : au plan individuel (chaque travailleur pris individuellement) et au plan collectif (au niveau des organes collectifs de l entreprise).

Qu elle soit collective ou individuelle, l information doit porter au moins sur les éléments suivants : la politique de contrôle ainsi que les prérogatives de l'employeur et du personnel de surveillance ; la ou les finalités poursuivies ; le fait que des données personnelles soient ou non conservées, le lieu et la durée de conservation ; le caractère permanent ou non du contrôle.

L information individuelle est cependant plus large. Outre les éléments à fournir lors de l information collective, l information individuelle doit également porter sur l'utilisation de l'outil mis à la disposition des travailleurs pour l'exécution de leur travail, en ce compris les limites à l'utilisation fonctionnelle; les droits, devoirs, obligations des travailleurs et les interdictions éventuelles prévues dans l'utilisation des moyens de communication électronique en réseau de l'entreprise; les sanctions prévues au règlement de travail en cas de manquement.

Dans la pratique, cet objectif sera bien souvent atteint par la rédaction d un règlement d utilisation des ressources informatiques de la société qui établira avec précision les conditions et modalités du contrôle envisagé.

L individualisation des données

Dans le respect des principes de finalité, proportionnalité et transparence, une procédure d individualisation des données peut être réalisée pour autant qu une anomalie ait été préalablement constatée dans le cadre d un contrôle de type global.

Cette procédure d individualisation consiste pour l employeur à analyser les données globales en sa possession de manière à retracer l identité de l auteur de l anomalie. En pratique, les éventuelles anomalies peuvent être constatées par la consultation périodique des données de communication électronique en réseau collectées dans l entreprise (par exemple, statistiques de durée globale de connexion à internet, sites les plus visités). L employeur analysera et décortiquera les données en sa possession, et ne pourra pousser plus avant le contrôle qu à la seule et unique condition qu une anomalie soit détectée.

Selon les cas, l individualisation des données aura lieu de manière directe ou indirecte.

Individualisation directe La procédure d individualisation pourra être directe lorsque l anomalie constatée relève de la poursuite des trois premières finalités décrites à l article 5 de la convention. Dans ce cadre, l employeur peut retracer directement l identité du ou des responsables de l anomalie, sans qu il soit requis de sa part qu il passe par une phase préalable d avertissement.

Une fois l individualisation réalisée, la suite à y réserver est laissée à l appréciation de l employeur : auditionner le travailleur, appliquer une sanction disciplinaire immédiate si elle prévue au sein du règlement de travail ou encore licencier le travailleur concerné (éventuellement pour motif grave si les conditions sont remplies).

Individualisation indirecte Lorsque l anomalie constatée relève de la poursuite de la quatrième finalité, soit le respect de bonne foi des principes et règles d'utilisation des technologies en réseau fixés dans l'entreprise, la procédure d individualisation des données doit nécessairement être indirecte et devra passer par une phase dite de sonnette d alarme. L employeur doit en effet porter à la connaissance du ou des travailleurs, de manière certaine et compréhensible, l existence de l anomalie et les avertir que les données seront individualisées si une nouvelle anomalie de même nature se produit à nouveau.

L information à fournir doit revêtir un caractère de rappel ou de mise au point des principes et règles fixées dans l'entreprise de manière à éviter la survenance d'une nouvelle anomalie de même nature. Par ailleurs, le travailleur concerné par la procédure sera invité à un entretien par l employeur et qui lui permettra de s expliquer. Cet entretien doit être préalable à toute décision ou évaluation susceptible d affecter individuellement le travailleur.

Plus d infos ?

En consultant sur notre site le texte de la CCT n° 81 sur la cybersurveillance des travailleurs .

Auteur(s) :

Thibault Verbiest
Avocat aux barreaux de Paris et de Bruxelles (Ulys)

Janice Dervaux
Avocat au Barreau de Bruxelles - Cabinet ULYS ()