



LA CYBERSURVEILLANCE AU TRAVAIL

Protection de la vie privée au travail

L'usage des technologies de l'information et de la communication (TIC) à des fins de contrôle en milieu de travail, de même que la prise en compte des enjeux liés à la protection de la vie privée, sont des problématiques déjà anciennes. Elles ont évolué de concert avec le développement, l'expansion et l'interconnexion des TIC. Durant les années 70 déjà, le souci de protection de la vie privée accompagnait la constitution des premières bases de données à caractère personnel et, au fil du temps, un cadre législatif s'est développé aux niveaux national, européen et international. Pour différents motifs, les usages des TIC à des fins de surveillance ont continué à se développer au travail et hors travail; la technologie également a continué à se perfectionner.

A

DES TECHNOLOGIES EN DÉVELOPPEMENT CONSTANT

Aujourd'hui, au rayon des nouveautés, ce sont, par exemple, les technologies de radio-identification (RFID, radio frequency identification) et les applications de la biométrie qui se révèlent problématiques pour la vie privée. Les étiquettes RFID sont des puces miniatures qui permettent, par radiodiffusion, de localiser et d'identifier un bien ou une personne. Ces étiquettes sont encore peu répandues car elles sont coûteuses et néfastes pour l'environnement. Elles sont cependant utilisées à titre expérimental par des entreprises (Gillette, Hewlett-Packard, Wal-Mart). Dans un supermarché dont tous les produits seraient équipés de telles étiquettes, le client pourrait passer à la caisse en quelques secondes sans même vider son panier, le récepteur radio pouvant détecter tous les produits en vrac et enclencher automatiquement le paiement. Ces étiquettes RFID sont aussi implantées sous la peau des animaux pour suivre

les troupeaux mais aussi parfois sous la peau des humains. En 2004 au Mexique, ces étiquettes ont été implantées dans le bras de 160 enquêteurs et avocats fédéraux pour assurer leur sécurité. Cette puce est également insérée dans des badges professionnels, des tickets d'avion, etc. Si ces étiquettes ne sont pas désactivées, elles permettent de suivre un individu ou un bien à la trace. Les caméras biométriques enregistrent quant à elle des caractéristiques faciales. Elles sont utilisées dans les systèmes de sécurité et sont déjà présentes dans certains aéroports, en Europe (Pays-Bas) et aux États-Unis.

B

LE CONTRÔLE AU TRAVAIL

Dans cet article, nous proposons un rappel des usages, des cadres législatifs et des enjeux dans le contexte professionnel. De nombreux outils dans les milieux de travail sont, ou peuvent être, utilisés à des fins de contrôle. Caméras de surveillance, ordinateurs, utilisation de courriels et d'internet, technologies de positionnement (GPS,

téléphones cellulaires), techniques biométriques fournissent de nombreuses données qui peuvent être interconnectées et analysées. Le marché des logiciels de surveillance est très important; il représente, selon la Privacy Foundation, 140 milliards de dollars par an. Des logiciels permettent de surveiller les entrées et les sorties d'un serveur, analysent les courriers électroniques, les échantillonnages de conversation, retracent l'historique des sites visités et identifient la nature de ceux-ci, etc.

Les innovations technologiques en matière de vidéosurveillance sont importantes: miniaturisation des caméras, caméras pivotant à 360 degrés, biométriques, à haute résolution, à vision nocturne, à infrarouges. La mise en réseau de caméras et d'ordinateurs permet à un seul opérateur, éventuellement à distance, de contrôler une multitude de caméras. Toutes les activités effectuées à partir d'un ordinateur génèrent également une foule de renseignements numériques: le nombre et la taille des courriels, le temps passé sur le web, la durée des pauses, etc. Les systèmes de localisation par satellite (GPS) couplés à un ordinateur peuvent devenir des outils de surveillance. Les ordinateurs de bord sont dotés de capteurs fixés aux véhicules; ils renseignent sur l'utilisation du véhicule, la vitesse, la durée des trajets, etc. Ils peuvent imposer des itinéraires et des temps pour parcourir les distances. La nouvelle génération de téléphones cellulaires incorpore la technologie GPS, leurs utilisateurs peuvent être localisés en tout temps. Des employeurs peuvent ainsi examiner les déplacements de leur personnel sur ordinateur.

C

DES DROITS ET DES DEVOIRS PARTAGÉS ET LIMITÉS

En vertu de son droit de propriété, de la propriété des outils et du lien de subordination du salarié, l'employeur a bien sûr le droit de contrôler la bonne exécution du travail et d'utiliser certains outils pour y arriver. Par ailleurs, la vie privée est un droit explicitement protégé et ce droit s'exerce aussi dans l'entreprise. La vie privée des salariés ne s'arrête pas aux portes de l'entreprise; il existe un espace de vie privée au travail.

L'usage et la banalisation des TIC en milieu professionnel a donné une impulsion incontestable au brouillage des frontières entre vie professionnelle et vie privée. Cette interpénétration est maintenant rendue « traçable » par les outils technologiques.

Le repérage d'actes malveillants ou négligents ne prête pas à controverse mais il existe de nombreuses zones troubles dans l'usage des TIC à des fins de surveillance: les caméras dans les espaces de repos; les micros et caméras cachés; l'accès aux données stockées sur les ordinateurs des collaborateurs; la cartographie des réseaux et des méthodes des agents commerciaux; l'enregistrement du personnel par les caméras de surveillance dans les grands magasins; le relevé des parcours et des temps d'intervention des infirmières ou aides soignantes à domicile, via le GPS; l'enregistrement des communications téléphoniques, parfois à l'insu du client qui appelle; etc. La controverse apparaît quand cette traçabilité des activités justifie des mesures disciplinaires ou des sanctions graves allant jusqu'au licenciement, ou encore quand elle comporte des intrusions vexatoires dans la vie privée.

D

LE CADRE NORMATIF EN BELGIQUE

Il n'existe pas de législation spécifique encadrant l'usage des TIC à des fins de surveillance au sein des entreprises. Un ensemble de textes épars vient encadrer ces usages. Le cadre normatif général comprend les textes relatifs à la protection de la vie privée et à l'intrusion dans les communications d'autrui: l'article 8 de la Convention européenne des droits de l'homme, l'article 22 de la Constitution, l'article 109 ter D et E de la loi du 21 mars 1991 (loi Belgacom), l'article 314 bis du code pénal, la loi du 8 décembre 1982 (loi vie privée). Un seul instrument normatif s'adresse spécifiquement au monde professionnel: la convention collective de travail n° 81 du 26 avril 2002 rendue obligatoire par Arrêté royal du 12 juin 2002. L'objectif de ce texte est de rappeler les normes juridiques existantes afin de garantir le droit fondamental des travailleurs à la vie privée dans la relation de

travail, tout en tenant compte des nécessités inhérentes au bon fonctionnement de l'entreprise.

E

LA CONVENTION COLLECTIVE N° 81

La CCT n° 81 encadre le contrôle des « données de communication électronique en réseau », c'est-à-dire les courriels, les usages d'internet, intranet, extranet, les SMS, le chat, les forums de discussion, le wap... Le contrôle est permis mais il ne peut porter atteinte à la vie privée et aux libertés individuelles ou collectives.

Les conditions de ce contrôle doivent rencontrer trois principes: le principe de finalité, le principe de proportionnalité, le principe de transparence.

Le principe de *finalité* stipule les situations dans lesquelles le contrôle est permis, elles sont au nombre de quatre:

- La prévention de faits illicites ou diffamatoires, contraire aux bonnes moeurs ou susceptibles de porter atteinte à la dignité d'autrui (par exemple, la prévention des actes de piratage, la consultation de sites illicites).
- La protection des intérêts économiques et financiers de l'entreprise auxquels est attaché un caractère de confidentialité ainsi que la lutte contre les pratiques contraires (par exemple, prévenir la divulgation de fichiers, la publicité dénigrante, les secrets d'affaires).
- La sécurité et/ou le bon fonctionnement techniques des systèmes informatiques en réseau de l'entreprise, ainsi que la protection des installations physiques de l'entreprise (par exemple, le téléchargement de fichiers volumineux qui ralentissent le réseau ou présentent des risques de virus).
- Le respect de bonne foi des principes et règles d'utilisation des technologies en réseau fixés dans l'entreprise (contrôle pour vérifier le respect des règles fixées en matière d'accès et d'utilisation des ressources informatiques).

Le principe de *proportionnalité* stipule que le contrôle ne peut entraîner une ingérence dans la vie privée du travailleur et que s'il y a une ingérence, elle doit être réduite au minimum. Le contrôle doit être adéquat, pertinent, non excessif et nécessaire au regard des finalités poursuivies. Il ne porte dans un premier temps que sur des données globales, c'est-à-dire qu'on ne peut procéder d'emblée à un contrôle visant à identifier l'usage particulier qu'un travailleur déterminé fait du réseau.

Le principe de *transparence* prévoit une information des travailleurs à la fois collective, via les organes de représentation (conseil d'entreprise, délégués syndicaux...) et individuelle, via par exemple le règlement de travail.

Lorsqu'un employeur constate une anomalie, il peut retracer l'identité du travailleur à l'origine de cette anomalie. La CCT prévoit également les procédures de cette *individualisation* du contrôle, c'est-à-dire l'analyse de données globales en vue de retrouver l'identité d'un auteur d'anomalie. Selon les cas, cette individualisation pourra être directe, sans formalités, ou indirecte, après une phase préalable d'information collective.

Cette CCT couvre une partie des usages des TIC, ceux liés aux communications électroniques et aux usages d'internet et autres réseaux. Elle a un effet régulateur et pédagogique mais elle n'épuise pas la question des usages des TIC à des fins de contrôle et les risques d'ingérence dans la vie privée dans le cadre professionnel. Elle fait suite à une autre convention, la CCT n° 68 appelée « CCT caméra ». Les discussions actuelles concernent une autre forme de contrôle, éminemment personnel, la « fouille » par des vigiles.

F

BANALISATION DES TIC ET OBSESSION SÉCURITAIRE

L'usage démesuré des TIC à des fins de contrôle du travail est la résultante d'une banalisation des technologies en milieu professionnel et d'une obsession sécuritaire en croissance ces dernières années. En même temps, les organisations

actuelles encouragent, de manière informelle, une interpénétration des temps privé et professionnel qui apporte une flexibilité réciproque aux salariés et aux employeurs, mais qui peut poser problème dans certaines circonstances.

Patricia Vendramin
Gérard Valenduc

Article paru dans La Lettre EMERIT n°43

Sources

- Fédération des Travailleurs du Québec, *Les TIC à quel prix ?*, Actes du colloque sur les technologies de l'information et de la communication, mai 2005 (www.ftq.qc.ca).
- Convention collective de travail n° 81 du 26 avril 2002 relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communication électroniques en réseau.



AVEC LE SOUTIEN DU MINISTÈRE DE LA COMMUNAUTÉ FRANÇAISE,
SERVICE DE L'ÉDUCATION PERMANENTE