THIBAULT MEIERS
Clifford Chance Europe LLP

Surveiller les connexions Internet, oui, mais avec circonspection !

Les salariés reconnaissent que 20 % à 50 % du temps passé sur Internet au bureau est consacré aux loisirs. En moyenne, au moins une heure par jour serait dédiée à surfer sur la toile à des fins personnelles… soit un mois par an !
Perte de temps de travail et donc de productivité, coût associé aux connexions, risque pour le réseau et la sécurité en cas de consultation de sites "malveillants" (contenant un cheval de Troie par exemple), déficit d'image si l'on venait à retracer la consultation de sites illicites grâce à l'adresse IP ou – pire – engagement de la responsabilité de l'employeur en cas de dommage causé par l'usage d'Internet au temps et au lieu du travail avec le matériel de l'entreprise : autant d'arguments qui légitiment une surveillance par l'employeur des connexions de ses salariés.

Surveillance seulement car, selon la Cnil, un usage raisonnable d'Internet à des fins personnelles doit être toléré. L'interdiction de certaines connexions est néanmoins admise par l'autorité administrative, lorsqu'il s'agit de sites au contenu illicite (pornographie, incitation au racisme, etc.) ou encore du téléchargement de logiciels, de la connexion à des forums ou de l'accès aux boîtes de réception personnelles, en raison du risque de propagation de virus.
L'employeur peut opter pour un contrôle global et indifférencié des connexions des salariés ou pour une surveillance individualisée des sites visités par chaque utilisateur. Cette seconde voie est privilégiée par les entreprises, la responsabilité collective ne comptant que peu d'émules.
Dans ce cas, l'employeur doit, préalablement à l'introduction des moyens techniques permettant la surveillance des connexions : recueillir l'avis du comité d'hygiène, de sécurité et des conditions de travail sur leur impact sur les salariés (sentiment de "flicage" générateur de stress, etc.) ; consulter le comité d'entreprise sur ce moyen de contrôle de l'activité des salariés ; les déclarer à la Cnil en tant que traitement automatisé d'informations nominatives ; et, enfin, les porter à la connaissance des collaborateurs par écrit. Cette dernière information n'est pas nécessairement individuelle – bien que ce soit préférable – et peut n'être que collective, du moment qu'elle est accessible, précise et exhaustive quant aux modalités concrètes du contrôle.
Faute de respecter ces formalités, toute décision prise à l'encontre d'un salarié à l'aide d'informations collectées par le dispositif de surveillance est infondée. La seule solution pour l'employeur est alors le constat de l'historique des connexions par un huissier.

Une fois l'outil en place, il reste à distinguer ce qui relève des connexions professionnelles de la navigation à des fins personnelles afin que le procédé ne soit pas attentatoire à la vie privée.
De façon surprenante, la Cour de cassation considère, à cet égard, que les connexions établies pendant le temps de travail grâce à l'ordinateur de l'entreprise sont présumées avoir un caractère professionnel, de sorte que l'employeur peut librement y avoir accès, même hors la présence du salarié.
Cependant, à la différence des fichiers et emails, on voit mal comment le salarié peut concrètement identifier ses connexions Internet comme personnelles afin de s'opposer au contrôle de l'employeur. La Cour vient de le préciser, le simple tri dans un groupe de favoris intitulé "personnel" est insuffisant. Le critère de l'heure de la connexion n'est pas non plus pertinent avec le développement des forfaits et le caractère de plus en plus poreux de la frontière temps de travail/temps personnel.

Et que dire du lieu d'établissement de la connexion, avec le développement des BlackBerry et Iphone. Certes, la nature personnelle de la connexion peut se déduire de l'adresse du site ou de son contenu, mais ce n'est pas toujours évident (recrutement.com pour un RH) et suppose, en tout état de cause, une prise de connaissance des sites consultés par l'employeur, laquelle peut caractériser une immixtion dans la vie privée du salarié (consultation du compte bancaire, etc.).

Enfin, même avec un accès codé et nominatif à l'ordinateur, l'imputabilité de la connexion fautive peut se poser, car si l'ordinateur est une vraie "boîte noire", il ne peut pas encore témoigner de quel salarié était effectivement connecté.
Surveillance des connexions doit donc rimer avec prudence.

Thibault Meiers, avocat au cabinet Clifford Chance Europe LLP, membre d'Avosial, le syndicat des avocats d'entreprise en droit social.