Andrea Mondini
avocat, Etude Schellenberg Wittmer, Zurich,
www.swlegal.ch

Internet et courriel au travail

Quelles sont les mesures que les entreprises doivent adopter pour lutter contre d'abus et quelles sont les limites légales qu'elles doivent respecter?

1. Situation actuelle

L'utilisation optimale d'Internet et du courriel, tant du point de vue technique qu'organisationnel, permet aux entreprises de réaliser d'importants gains de productivité et d'économiser des frais. Mais ces effets positifs risquent d'être contre-balancés par les risques inhérents à un usage privé abusif d'Internet et du courriel au travail.
L'utilisation abusive des moyens de communication d'une entreprise à des fins privées a non seulement une portée financière mais influence également la sécurité informatique. En effet, le trafic de données privées peut engendrer des risques accrus pour la sécurité au niveau technique (par exemple les virus informatiques), de même qu'un recours excessif aux capacités de mémoire ou le blocage du poste de travail électronique. Au vu de ce constat, il faut se demander comment et dans quelle mesure, en vertu du droit suisse, les employeurs doivent tolérer l'utilisation au ravail d'Internet et du courriel à des fins privées et quelles sont les limites légales qu'il convient de respecter par rapport aux mesures de protection envisageables, en particulier les limites définies par le droit du travail, la législation sur la protection des données et le droit pénal.

2. Aperçu: mesures techniques préventives et répressives

En matière de limitations des risques, il convient de séparer clairement les questions techniques des questions juridiques, qui traitent de l'admissibilité de l'usage privé. En ce qui concerne les questions techniques, on distinguera les mesures de protection techniques préventives et les mesures de surveillance répressives.
Les mesures de protection techniques préventives ont pour but de minimiser les risques et de garantir le bon fonctionnement et la sécurité d'une infrastructure informatique. Parmi les principales mesures techniques préventives figurent la protection par mot de passe, la protection de l'accès, le cryptage des données particulièrement sensibles, les programmes anti-virus, le blocage de certains sites web, les programmes de gestion des quotas de disque, les mesures de sauvegarde et les «firewalls». Du point de vue juridique, les mesures de protection de ce type sont non seulement autorisées mais même souhaitées puisqu'elles permettent de prévenir des activités illégales (par exemple la diffusion de virus informatiques, le sabotage d'ordinateurs, la violation de secrets d'affaires, l'abus de données personnelles).
Les mesures techniques répressives de surveillance permettent de constater et de sanctionner après coup d'éventuels abus. Dans ce domaine, on mentionnera la surveillance du réseau et du trafic de courriels, la surveillance des écrans, voire la surveillance des claviers et des souris. D'un point de vue juridique, de telles mesures de surveillance répressives ne sont admissibles que de manière très restreinte. En cette matière toutefois, il convient de tenir compte de l'effet dissuasif déterminant découlant des moyens prévus par le droit du travail.

3. Limites juridiques générales de la surveillance

Les limites juridiques mises à la surveillance des employés découlent principalement du droit du travail, de la législation relative à la protection des données et du droit pénal. Le domaine privé est en outre également couvert par le secret des télécommunications. Un règlement d'utilisation devrait déterminer dans chaque cas particulier si et dans quelle mesure l'utilisation privée des moyens de communication de l'entreprise est autorisée ou si une telle utilisation est partiellement ou totalement interdite (cf. ch. 4 ci-après).
Du point de vue technique, les outils informatiques sont en mesure d'établir des procès-verbaux des activités menées par leur intermédiaire. Juridiquement, la surveillance anonyme et permanente du fonctionnement et de la sécurité d'un système informatique est sans autre admissible. La surveillance anonyme du comportement de navigation sur Internet à des fins statistiques est également autorisée. La surveillance est dite «anonyme» si elle ne permet pas de déterminer au comportement de navigation la manière de naviguer sur Internet de chaque collaborateur pris individuellement. Par contre, la surveillance cachée, permanente et personnalisée des employés est interdite en Suisse (art. 26 OLT3). Le but et le sens de cette interdiction est de protéger l'employé contre une surveillance permanente et ciblée de son comportement. La surveillance de l'écran, du clavier et des mouvements de la souris ainsi que les programmes dits «espions» violent la sphère intime et la personnalité des

employés concernés et ne sont dès lors pas admissibles. Par ailleurs, la protection de la personnalité d'un des employés est également garantie par la loi sur la protection des données et par les dispositions du Code des obligations sur le droit du contrat de travail. Fait également partie des surveillances non autorisées l'analyse personnalisée des procès-verbaux sans information préalable des employés en aient été informés au préalable est également interdit. La surveillance du Surveiller la manière de naviguer comportement de navigation visant dans le but d'à identifier une personne n'est par ailleurs admise qu'exceptionnellement, en cas de soupçon ou de constatation d'abus, et ceci seulement dans les cas où un abus ne peut être empêché par des moyens de protection techniques préventifs. S'il peut l'être: dans ce cas également, les mesures de protection préventives techniques, ces moyens préventifs ont la priorité sont prioritaires. Une telle surveillance devrait se faire de manièreau moyen de pseudonymes attribués, c'est-à-dire par l'attribution aux employés de pseudonymes (par exemple une série de chiffres), ces pseudonymes étant qui seront tout d'abord enregistrés sous cette une forme anonyme. En cas de constatation d'abus, la liste établissant quel pseudonyme a été attribué à quel employé permet d'analyser les procès-verbaux, cette liste ne pouvant par ailleurs être connue que des responsables du personnel. ces procès-verbaux peuvent être analysés au moyen d'une liste de correspondances qui fait apparaître l'attribution et n'est connue que des responsables du personnel. Dans ce cas, il est déterminant de pouvoir commencer par la possibilité d'établir des procès-verbaux des données des utilisateurs sous forme de pseudonymes, sans avoir recours aux responsables du personnel. dans un premier temps est déterminant

Dès lors, la constatation d'un abus, respectivement l'existence d'un soupçon, correspondant et ainsi que l'information préalable des employés constituent les deux conditions pour qu'd'une surveillance personnalisée soit admissible. Dans la pratique, cette information dles employés sont informés est assurée par au moyen d'une réserve correspondantead hoc précisée figurant en toutes lettres dans un règlement de surveillance rédigé par écrit.

4. Moyens recommandés au regard du droit du travail: règlement d'utilisation et de surveillance

En vertu des dispositions sur le contrat de travail, tout employeur a le droit d'édicter des directives générales (art. 321d CO). Il peut ainsi décider librement dans quelle mesure Internet et le courriel sont à disposition des employés à leur place de travail et la manière dont ceux-ci doivent utiliser ces instruments électroniques. La marge de manœuvre laissée par la loi à l'employeur découle de ce principe: l'employeur peut interdire entièrement l'utilisation, la limiter, voire la prescrire pour certaines tâches. Les employés n'ont par conséquent aucun droit à l'utilisation privée des outils Internet sur leur lieu de travail.

4.1 Règlement d'utilisation: usage selon les volontés de l'employeur décide

S'il n'est pas obligatoire d'adopter un *règlement d'utilisation,* cette possibilité permet néanmoins à l'employeur de mettre les choses au point tout en profitant de la marge de manœuvre que lui laisse la loi en matière de limitation de l'usage privé des instruments informatiques. Savoir si les employés ont le droit d'utiliser Internet et le courriel à des fins privées sur leur place de travail dépend dès lors principalement de l'employeur, l'autorisation pouvant être différente selon la catégorie des employés concernés et les besoins professionnels. Il faut en outre souligner que la violation d'un tel règlement constitue un motif suffisant pour identifier la personne fautive (cf. ch. 3 ci-dessus). Un tel règlement peut donc interdire de télécharger des films et de la musique sur la place de travail ou limiter l'utilisation privée des services de courriel à des communications brèves et urgentes.

Même si l'employé, en vertu de son l'obligation générale de fidélité et de diligence (art. 321a CO), doit user de manière de l'employé (art. 321a CO) exige un usage appropriée des instruments de travail de l'employeur, un flou il subsiste pour les employés qui ne pouvantsont pas au bénéfice d' se référer à aucun un règlement d'utilisation un flou quant à l'admissibilité de l'usage d'Internet et des services dedu courriel à des fins privées. Par ailleurs, le règlement d'utilisation devrait être rédigé sous une formede manière concrète et claire de manière à ceafin que les limites de à l'usage privé toléré au sur le lieu de travail en découlent sans doute possible. Si tel n'était pas le casA défaut, il n'est guère possible en pratique de déclarer déterminer si un usage à des fins privées comme est admissible ou pas ou interdit et il est donc s'il est constitutif d'un abus, condition préalable impossible de constater un abus qui constitue pourtant une condition nécessaire à l'application d'éventuelles sanctions.

4.2 Règlement de surveillance: possibilité de l'analyse personnifiée en cas d'abus

Contrairement au règlement d'utilisation, l'employeur doit impérativement édicter 'établissement d'un règlement de surveillance constitue une exigence absolue pour autant que l'employeurs'il désire veut se ménager la possibilité d'analyser d'éventuels procès-verbaux de manière personnalisée d'éventuels procès-verbaux. La surveillance qui en découle peut constituer une atteinte à la sphère privée de l'employé. Par uUne simple remarque réserve dans le règlement suffit cependant pour que, l'employeur satisfait toutefois àsoit considéré comme ayant l'exigence d'suffisamment informéer l'employé ses employés de la possibilité de cette atteinte en cas d'abus ou en cas d'existence d'unde soupçon d'abus. Il faut souligner ici que l'établissement l'adoption d'un tel règlement peut constituer une sensibilisationpermet de sensibiliser les bienvenue des employés. Ainsi, – le seul fait qu'une surveillance personnalisée est soit possible en cas d'abus peut avoir un effet préventif sur le comportement des employés.

5. Courriels professionnels et privés

Si l'utilisation des services de courriel à des fins privées dans une entreprise est en principe autorisée et si les courriels privés sont également reconnaissables en tant que tels, par exemple grâce à une indication correspondante dans la ligne «objet», ils sont assimilables à du courrier privé à sur la place de travail et jouissent de la même protection globale que du le courrier normalordinaire. Si des tiers ouvrent un tel courrier personnel, respectivement lisent des courriels clairement marqués comme étant «privés», l'on est en présence d'ils commettent une violation illégale de la personnalité : compte tenu de la protection de la personnalité et de l'interdiction de la surveillance du comportement, l'employeur n'est pas autorisé à prendre connaissance du contenu des courriels privés de l'employé; le contenu des courriels désignés comme privés ne peut donc pas être utilisé. Par ailleurs, le trafic des courriels est couvert par le secret des télécommunications. Le contenu des courriels désignés comme privés ne peut donc a fortiori en aucun cas être utilisé.

La situation est tout à fait différente pour les courriels professionnels: dans ce cas, l'employeur est en droit d'établir de manière systématique un procès-verbal de ces courriels de manière systématique, de les enregistrer et de les sauvegarder. Les courriels professionnels représentent sont de manière générale de la correspondance d'affaires et l'employeur est donc tenu de les conserver pendant une durée de 10 ans (art. 962 CO). Dans le cadre de la sauvegarde, respectivement de l'archivage, des problèmes pratiques de différenciation

pratiques se posent toutefois qui ne peuvent être résolus au niveausur le plan juridique que si l'employeur informe de manière générale ses employés, dans le cadre d'un règlement, que tous les courriels échangés à sur la place de travail, y compris les courriels privés, seront archivés. On comprend dès lors aisément que des courriels privés puissent également faire l'objet d'une telle mesure d'archivage. Les employés ont quant à eux la possibilité d'éviter l'archivage de leurs courriels privés en les détruisant ou en renonçant complètement à communiquer au moyen de courriels privés.
D'un point de vue pratique,, il est recommander d'établir et d'appliquer l'établissement et l'application d'une véritable politique en matière de courriel, «E-Mail Policy» se recommandent sous la forme d'une concept global relatif quant à la réception, l'archivage, la destruction et les droits d'accès.

6. Violations et sanctions

6.1 Abus de la part de l'employé

Un abus de la part de l'employé peut constituer une violation du contrat de travailvioler des conventions résultant du droit du travail, ou respectivement d'un règlement d'utilisation édicté par l'employeur. Dans ce dernier cas, l'employé répond des dommages qu'il cause à l'employeur intentionnellement ou par négligence (art. 321e CO). Pour pouvoir prendre des sanctions, l'employeur étant doit tenu de prouver à la fois que l'employé son employé a violé son devoir de diligence et le dommage qui en résulte afin de pouvoir sanctionner l'employé en raison de la violation du règlement d'utilisation. Les poursuites pénales par les autorités compétentes demeurent réservées pour autant qu'un délit ait été commis (par exemple diffamation, espionnage industriel, harcèlement sexuel ou diffusion de matériel raciste ou pornographique). Même s'il n'existe aucune obligation de porter plainte, il est recommandé que l'employeur porte plainte dans un tel cas afin d'éviter toute accusation de complicité.
L'employeur est responsable d'informer les employés de leurs devoirsobligations (de ne pas faire) et de mettre en place ldes conditions de mise en œuvred'application optimales des règlements adoptés, tant d'un point de vue tant technique qu'organisationnel pour les règlements établis, par exemple par le biais de cours de formation.

6.2 Surveillance indue par l'employeur

Si l'employeur ne respecte pas les conditions nécessaires mises à la surveillance de l'utilisation d'Internet et des services dedu courriel, l'employé peut contester devant un tribunalen justice les atteintes dont il est l'objet ainsi que les sanctions du droit du travail qui en découlent (par exemple le un licenciement abusif) en faisant valoir une violation illégale de sa personnalité et son droit à la constatation de l'illégalité de ces mesures, voire en réclamant des dommages-intérêts contre à sonl' employeur. S'il y a violation de la sphère privée ou intime ou accès non autorisé à des données personnelles, cela peut également avoir des suites pénales sont également envisageables.
Afin d'éviter toute surveillance inadéquate par l'employeur, il est important de définir clairement l'utilitéle but, le contenu et la durée de conservation des procès-verbaux ainsi que l'utilisation de ces derniers, tout en s'assurant que les données personnelles soient toujours traitées dans le respect des principes de proportionnalité et d'affectation à un usage déterminé. Il faut encore mentionner à ce sujet que l'employé peut en tout temps demander à être informé du traitement si des données le concernant sont traitées (art. 8 al.1 LPD).

7. Signature électronique

La signature électronique est un sceau numérique lié à un message généré créé par une clé de individuelle signature et contrôlé par une clé de contrôle (public key). La clé de contrôle est authentifiée par une autorité de certification. En Suisse, la Lloi fédérale sur la signature électronique (SCSE) établit un cadre juridique sûr pour la correspondance d'affaires électronique. La reconnaissance juridique est déterminante dans ce domaine: depuis le 1er janvier 2005, les signatures numériques qualifiées ont la même valeur que les signatures olographes manuscrites, pour autant qu'elles e celles-ci se basent sur un certificat qualifié qui ne peut être obtenu qu'auprès d'une fournisseurs de services de certification (suisses ou étrangers) reconnus.
Même si les signatures électroniques sont relativement fréquentes en pratique, il n'existe encore aucune signature électronique juridiquement valable au sens de la loi susmentionnée, étant donné que la Suisse ne compte encore aucun fournisseur de services de certification reconnu. Par conséquent, la signature électronique légalement valable légalement n'obtiendra n'acquerra desa validité juridique que lorsque la Confédération aura reconnu' un premier fournisseur de services de certification aura été reconnu par la Confédération. Les qualités déterminantes essentielles de la signature électronique au sens de la nouvelle loi se réfèrent àsont l'intégrité d'un du message (impossibilité de modifier le mode de transmission), l'authenticité son authenticité (le partenaire de communication étant identifiéauthentifié) et le caractère incontestable (l'envoi étant irrévocable).

8. Conclusion

Afin de clarifier la situation et de pouvoir agir contre les abus, il est indispensable que les entreprises adoptent un règlement écrit d'utilisation sur l'utilisation et de la surveillance comprenantortant des règles obligatoires en matière d'utilisation de du courriels et d'Internet à sur la place de travail et définissant dans quelle mesure l'utilisation à des fins privées est tolérée. L'adoption d'un règlement de sur la surveillance et la réservel'information relative à certaines mesures constituent en outre des conditions indispensables pour la prise de décisions tellesprocéder à que l'analyse personnalisée de données de procès-verbaux. Concrètement, il est possible de résumer comme suit les conditions d'une surveillance personnalisée, qui reste très délicate du point de vue juridique: d'une part, il faut que des mesures de protection préventives techniques et organisationnelles aient été prises (mots de passe, cryptage etc.). Ces mesures doivent dans tous les cas être prioritaires face par rapport aux mesures de surveillance. D'autre part, il convient de prendre des mesures juridiques, à savoir l'adoptionpplication de règlements d'utilisation et de surveillance. Dans tous les cas, une surveillance personnalisée n'est admissible qu'en cas d'abus ou de soupçon d'abus. La surveillance permanente de l'écran, de la souris ou du clavier ainsi que le recours à des logiciels «espions» ne sont de manière générale pas admissibles. En ce qui concerne les courriels privés, un telle règlement devrait préciser que tous les courriels privés n'étant qui ne sont pas clairement marqués en tant quecomme tels seront considérés comme de la correspondance d'affaires, susceptible d'être archivée. et que l'archivage de tels courriels privés est donc possible.
Globalement, l'employeur doit surtout concentrer ses efforts sur le domaine de la prévention technique afin d'empêcher un usage non souhaité, voire illégal, et afin d'empêcher que l'entreprise ne subisse des dommages techniques. L'effet préventif de ces mesures lorsqu'elles sont appliquées systématiquement permet le plus souvent d'éviter le recours aux moyens répressifs tels que la surveillance personnalisée. ■

(Traduction de l'article original paru en allemand)
Tiré de: CH-D-Wirtschaft no. 4.2005