

1 Correspondance privée et entreprise

Le courrier électronique s'est développé à une vitesse remarquable, si bien que ce moyen de communication, nouveau il y a à peine quelques années, est, aujourd'hui, devenu un moyen de communication indispensable aux entreprises, au même titre que le téléphone.

Cette intrusion de « nouveaux » moyens de communication dans l'entreprise soulève certaines questions :

Personnes ne contestera la légitimité de l'employeur à vouloir s'intéresser à l'activité du salariés, qui utilise les moyens mis à sa disposition par l'entreprise pour accomplir son travail. Néanmoins, cet intérêt doit se concilier avec une nécessaire confidentialité des échanges, que ce soit vis à vis de l'extérieur, des autres salariés, ou même, vis à vis de l'employeur lorsque ces messages sont personnels.

Au regard du droit, cette confidentialité est assurée en ce que ces communications ne sont pas publiques et sont, en l'espèce, des correspondances, dites privées, protégées par le secret en vertu de la loi.

Il est alors nécessaire de concilier cette confidentialité avec le nécessaire contrôle que l'employeur pourrait vouloir exercer. Or, le secret de la correspondance privée ne souffre que deux exceptions, à savoir, les interceptions en cas d'enquête criminelle, ou celles pour raison d'Etat, sur autorisation écrite du premier ministre.

Pour résoudre cette problématique, l'Angleterre a, en octobre 2001, fait le choix d'une intervention législative, avec la « law business practice regulation », autorisant à l'employeur un contrôle quasi-intégral des correspondances de ses salariés. Un peu plus de trois ans plus tard, cette loi est toujours dénoncée par les syndicats...

La France a préféré s'orienter vers une solution de type contractuelle, comme ce fut le cas en matière de téléphonie.

Afin de bien cerner la problématique et ses solutions, nous nous proposons de voir la définition de la correspondance privée émise par voie de communication électronique, puis les conséquences de cette définition au sein de l'entreprise.

1.1 La correspondance privée émise par voie de communications électroniques

La loi du 10 juillet 1991 relative au secret des correspondances émises par voie des communications électroniques protège les correspondances émises par la voie des communications électroniques (nous noterons que la loi du 10 juillet 1991, de même que la LCEN ont été modifié par la loi du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle qui à notamment remplacée le terme « télécommunications » par le terme « communications électronique »). Il faut alors définir la correspondance émise par voie de communications électronique, puis caractériser son caractère privé avant de voir son régime.

1.1.1 La correspondance émise par voie de communications électroniques

La correspondance peut être définie comme étant toute relation, écrite ou non, entre deux ou plusieurs personnes, qu'il s'agisse, par exemple, de lettres, de messages, de plis fermés ou ouverts, ou encore, de communication téléphonique.

La communication électronique quant à elle est définie par l'article 32 du code des postes et des communications électroniques comme étant toute « émissions, transmissions ou réceptions de signes, de signaux, d'écrits, d'images ou de sons, par voie électromagnétique ».

A l'évidence, le message électronique répond à ces définition et doit, par là, être qualifié de correspondance émise par voie de communications électroniques.

Cela étant, la protection de la loi est subordonnée au caractère privée de la correspondance.

1.1.2 La correspondance privée

Pour être protégée, la correspondance doit être privée. Deux critères permettent de caractériser ce caractère privé ; le premier, relatif au destinataire, exige que le ou les destinataires soient « déterminés et individualisés ». Le second, relatif au contenu, veut que le contenu du message soit « fonction de considérations fondées sur la personne du destinataire ».

Le message électronique pourra alors être qualifié de correspondance privée et, à ce titre, être protégé par le secret des correspondances

1.1.2.1 L'atteinte au secret

L'atteinte au secret résulte de l'interception, le détournement, l'utilisation ou la destruction de correspondance émises par voie de communications électroniques, ou encore, l'installation d'appareils conçus à ces fins, dès lors que cette violation est faite de mauvaise foi. La mauvaise foi est ici constituée par la seule connaissance, par la personne qui commet le délit, que la correspondance ne lui est pas destinée. La sanction de cette interdiction est une peine d'une année d'emprisonnement et une amende de 45 000 euros.

Lorsque cette atteinte est le fait d'une personne chargée d'une mission de service public, la peine d'emprisonnement est portée à 3 années et l'exigence de mauvaise foi est supprimée, l'infraction étant caractérisée par le seul détournement, la destruction, l'interception ou l'utilisation d'une correspondance privée destinée à un tiers. Cette règle a été appliquée à un administrateur réseau par la cour d'appel de Paris, dans un arrêt du 12 décembre 1997

1.2 Les implications de la qualification de correspondance privé dans la gestion du réseau

Le régime de protection des correspondances privées est relativement rigide et, lors de la gestion d'un réseau, il convient de s'interroger sur la qualification des contenus susceptibles de transiter sur ce dernier

1.2.1.1 Les correspondances privées professionnelles

La correspondance professionnelle est une correspondance, transmise par un salarié dans l'exercice de ses fonctions, par le matériel mis à sa disposition par l'employeur dans le but d'un usage professionnel.

La jurisprudence a eut à se prononcer à plusieurs reprises sur ce sujet. Dans un arrêt du 16 janvier 1992, la chambre criminelle de la cour de cassation déclare non réunis les éléments constitutifs du délit de violation de correspondance privée, un chef de bureau ayant ouvert trois lettres adressées à un chercheur et contenant des convocations destinées à ce dernier en tant que membre du CNRS. La cour jugea que le courrier ne portant pas mention de son caractère personnel devait être considéré comme étant professionnel et que le CNRS, son contenu étant « envoyé au plaignant en tant que membre du CNRS », était le véritable destinataire.

Cette solution doit être transposé au courrier électronique. Il faut alors distinguer les messages professionnels qui, s'ils demeurent des correspondances privées, sont destinés à l'employeur qui ne peut dès lors pas se voir opposer le secret des correspondances, et les messages personnelles qui sont destinés à l'employé et dont le secret est opposable à l'employeur.

La jurisprudence aborde cette distinction, au sujet d'autres moyens de correspondances, de manière très pragmatique. Ainsi, les communications téléphoniques seront toujours présumés personnelles puisque, de l'avis de la cour d'appel de Paris (dans un arrêt du 7 mai 1997) il est « impossible de distinguer, sauf précisément en les captant, les communications relevant de la sphère privée ». A l'inverse, en matière de courrier postal, elle considère qu'il y a une présomption de professionnalité dès lors que l'enveloppe ne porte pas de mention contraire.

Dès lors, une solution proche devrait être dégagée pour les messages électroniques. Ceux-ci seraient présumés personnels lorsque leur sujet laisserait apparaître ce caractère de manière explicite (mention « personnel ») ou de manière implicite (« liste des courses pour la maison »). En revanche, les messages dont le sujet feraient apparaître un caractère professionnel devraient être considéré comme professionnel et, dès lors, la protection ne sera pas opposable à l'employeur.

1.2.2 La confidentialité du message électronique

Le secret des correspondance protège ainsi le message professionnel des atteintes extérieures à l'entreprise, mais la question peut se poser de la confidentialité au sein même de l'entreprise, et, plus particulièrement, vis à vis des autres salariés.

En effet, dès lors que l'on considère que les messages professionnels ne sont pas des messages personnels à son destinataire, la question se pose de savoir qui peut en prendre connaissance, et, surtout, lorsqu'une telle prise de connaissance pourrait entraîner une « concurrence déloyale » entre salariés ou chercheurs, comment assurer la confidentialité de tels messages.

A notre sens, le message étant destiné à un salarié en particulier, il faut considérer que celui-ci bénéficie d'un mandat pour le recevoir au nom et pour le compte de l'entreprise, mandat dont il est le seul à bénéficier, à l'exclusion de ses collègues ou concurrent. Ainsi, l'atteinte au secret de cette correspondance relèverait bien, à notre sens, d'une atteinte au secret des correspondances privées en ce que la personne tierce qui en prendrait connaissance ne serait ni destinataire du message, ni mandatée pour le faire. Reste que le problème peut se poser vis à vis de la hiérarchie. La seule solution en cas reste le recours à l'accord contractuel.

En ce qui concerne le CNRS, la charte utilisateur pour l'usage de ressources informatiques et de services Internet, intégrée aux règlements intérieurs des « entités du CNRS » et applicable « à l'ensemble des agents du CNRS tous statuts confondus, et plus généralement à l'ensemble des personnes, permanentes ou temporaires, utilisant les moyens

informatiques de l'entité ainsi que ceux auxquels il est possible d'accéder à distance directement ou en cascade à partir du réseau administré par l'entité » prévoit qu'il « est interdit de prendre connaissance d'informations détenues par d'autres utilisateurs, quand bien même ceux-ci ne les auraient pas explicitement protégées. Cette règle s'applique également aux conversations privées de type courrier électronique dont l'utilisateur n'est destinataire ni directement, ni en copie ».

En présence de messages personnels, il sera interdit de procéder à l'interception de ce message et encore moins à un contrôle de son contenu. Le problème se pose alors en matière de « spam » ou de virus informatiques.

1.2.2.1 Le « spam »

Le « spam », en français, « pourriel » peut être défini comme étant « l'encombrement délibéré d'un forum de discussion ou un compte e-mail par l'envoi de messages non sollicités, telles les annonces à caractère publicitaire ». La question se pose de savoir si les « pourriels » peuvent être qualifiés de correspondances privées. En effet, en premier lieu, il s'agit de correspondances puisque tout message électronique répond à cette définition. En second lieu, le destinataire est bien identifié, puisque cette identification procède de la définition même du message transmis par courrier électronique.

Il reste à étudier le critère relatif au contenu. Dans certains cas, les messages semblent être individualisés puisque les entreprises de « cybermarketing » établissent des profils d'utilisateur très ciblés et individualisent le contenu des messages en fonction de ces profils. Néanmoins, ce critère ne peut pas être considéré comme rempli, l'envoi de message publicitaire étant par définition une communication au public.

Dès lors, il faut considérer que les « pourriels » ne peuvent pas être considéré comme des correspondances privées, et que, dès lors, leur suppression ne sera pas constitutive d'une suppression de correspondances privées. Il convient tout de même d'être très prudent, car, si par erreur, le système de filtrage supprimait une correspondance privée, reconnue, à torts, comme étant un « pourriel », c'est-à-dire en cas de « faux positif », cela serait constitutif du

délit de correspondance privée.

Remarques suite à la conférence :

- *Les listes grises : Les listes grises permettent de filter les pourriels en testant le serveur émetteur. Le serveur de réception refuse une première fois les messages entrant. Si le serveur expéditeur du message renvoi une seconde fois le message, c'est qu'il ne s'agit a priori pas d'un pourriel, dans le cas contraire, il s'agit d'un pourriel et le destinataire ne le reçoit pas. A notre sens, il s'agit nécessairement d'une atteinte aux correspondances privées, puisque la conséquence de ce test est de retarder l'arrivée du message et que le délit est constitué par ce retardement... Dans l'entreprise, cela ne posera pas vraiment de problèmes, à condition que ce soit prévu dans le règlement intérieur ou le règlement d'utilisation des ressources informatiques, puisque cette atteinte aux libertés du salarié semble parfaitement proportionnée aux buts recherchés (lutter contre le spam) et que le retard sera insignifiant.*
- *Les listes noires: Le système des listes noires permet également de lutter contre les porriels. Le système repose sur le principe que l'on peut identifier les serveurs expéditeurs de pourriels et qu'il suffit donc de systématiquement refuser les messages émanants de ceux-ci. Dès lors que ces serveurs sont susceptibles d'adresser des messages autres que des pourriels, la suppression (ou le refus) de ces messages, qui sont des correspondances privées, est interdite. Ainsi, le système des listes noires risquerait d'entraîner la suppression de correspondances privées et, ainsi, la comission d'un délit. Cela doit donc être prévu conventionnellement.*

1.2.2.2 La lutte contre les virus

Le courrier électronique est l'un des principaux vecteurs de propagation des virus. Il semble alors nécessaire, afin d'assurer la protection du réseau, d'analyser les messages entrant sur le réseau afin de détruire les virus avant qu'ils ne soient susceptible de nuire. A cet fin, la technique habituelle consiste en l'utilisation d'un robot qui va analyser tous les messages entrant et, le cas échéant, détruire les virus.

Le problème posé par cette technique est que l'analyse du message constitue une violation de correspondance privée et sa destruction ou celle du virus, le délit de destruction ou d'altération de correspondance privée.

Dans le cas du « spamming », comme dans celui de la gestion des virus, la légitime défense trouvera, dans certains cas, à s'appliquer : la légitime défense dégage de sa responsabilité l'auteur d'une infraction qui la commet « pour interrompre l'exécution d'un crime ou d'un délit contre un bien ». Le spamming ou l'envoi de virus étant constitutifs de délit en portant atteinte à un système de traitement automatisé, la légitime défense pourrait être invoquée dans certains cas.

Toutefois, la légitime défense ne pourra en aucun cas permettre le contrôle systématique des virus ou la suppression répété de faux positif.

Dès lors, la seule solution envisageable est le recours à l'accord contractuel –au sens large – c'est-à-dire, prévoir ce contrôle dans les règles d'utilisation de la messagerie et s'assurer que l'utilisateur accepte ce contrôle.

Pour conclure, il convient de remarquer que la « charte déontologique RENATER » prévoit, dans son 4^{ème} point, que « l'utilisateur accepte que le GIP RENATER prenne des mesures d'urgences [...] pour préserver la sécurité en cas d'incident dont le GIP RENATER aurait connaissance ». Cette disposition pourrait permettre le filtrage en matière de « spamming », dès lors que celui-ci porte atteinte à la sécurité du réseau, notamment par la saturation des serveurs, mais surtout, trouve à s'appliquer aux virus. Toutefois, la formulation, notamment le terme « mesure d'urgence » se prête à l'interprétation (peut-on prendre quotidiennement des mesures d'urgences ?) et des termes plus explicites – l'utilisateur accepte le filtrage du « spam » et accepte le risque de perte de message...– seraient préférables.

1.2.3 D'autres « nouvelles » correspondances privées ?

Il convient de remarquer que la qualification de correspondance émises par voie des

communications électroniques n'a pas vocation à s'appliquer aux seuls messages électroniques. Ainsi, toute communication qui répondrait à aux critères que nous avons vu précédemment doit être considérée comme une correspondance privée et est protégée en tant que telle.

Ce sera le cas des communications par messageries instantanées, telle que MSN messenger ou AIM. Dans ce cas, à notre avis, il faudra considérer, à l'instar du téléphone, qu'il est impossible de savoir si la communication est privée ou professionnelle sans en prendre connaissance et ainsi, considérer qu'il y a une présomption de privauté.

Ce sera également le cas en matière de peer to peer. La plupart des logiciels de peer to peer, comme Kaza ou Emule, permettent de discuter avec d'autres utilisateurs. Il s'agit ici de messageries instantanées et la solution sera la même que précédemment. En outre, si la mise à disposition de fichier et l'accès aux bases de données des fichiers en partages doit être qualifiée de communication au public, la communication qui s'établie entre les machines une fois que l'utilisateur à choisi les fichiers qu'il souhaitait télécharger devrait probablement être qualifié de correspondance privée, ce qui interdit d'interrompre de tels flux ou de prendre connaissance de leur contenu.

Dans tous les cas, le moyen le plus efficace consiste en l'accord contractuel, que ce soit par l'intermédiaire du règlement intérieur ou par celui de chartes acceptés par les salariés.

