Selon une étude réalisée en 2010 par la société OLFEO, 63 % du temps passé par les salariés sur Internet au travail l'est pour un usage non professionnel... Quelle limite l'employeur peut-il apporter à l'utilisation des moyens informatiques mis à la disposition du salarié ? Peut-il sanctionner un usage personnel de ces moyens ?

Le salarié et les moyens informatiques à sa disposition

par
Ronan Kervadec
Avocat

par
Laura Bertrand
Juriste

DROIT AU RESPECT DE LA VIE PRIVÉE DU SALARIÉ

Si l'employeur peut utiliser des outils technologiques intrusifs permettant la surveillance de ses salariés sur leur lieu de travail, le salarié ne renonce pas pour autant à toute vie privée en franchissant le seuil de l'entreprise. Il est en effet protégé par les articles 9 du Code civil et 8 de la Convention européenne des droits de l'Homme et des libertés fondamentales qui consacrent pour chacun le droit au respect de sa vie privée.

Dans un célèbre arrêt « Nikon » d'octobre 2001, la Chambre sociale de la Cour de cassation a affirmé que le salarié a droit, **même au temps et au lieu du travail**, au respect de l'intimité de sa vie privée, en particulier au **secret de ses correspondances** (*Cass. soc., 2 oct. 2001, n° 99-42.942 ; confirmé par Cass. soc., 17 juin 2009, n° 08-40.274*). L'employeur ne peut violer sans condition cette liberté fondamentale, même s'il a préalablement interdit une utilisation non professionnelle des moyens informatiques mis à la disposition du salarié.

Est-ce à dire que vous pouvez désormais librement consulter des sites de charme ou vous consacrer depuis votre •••

●●● bureau à l'organisation de vos prochaines grandes vacances… ? Pas vraiment !

LA PRÉSOMPTION DU TOUT PROFESSIONNEL

La jurisprudence a déduit une **présomption de professionnalité** de la correspondance électronique du salarié, des fichiers présents sur son disque dur (*Cass. soc., 17 mai 2005, n° 03-40.017*) et de l'historique de ses connexions Internet réalisées pendant son temps de travail (*Cass. soc., 9 juill. 2008, n° 06-45.800 ; Cass. soc., 9 févr. 2010, n° 08-45.253*). Sont par conséquent exclus du champ de protection de la vie privée les messages et fichiers à caractère professionnel, c'est-à-dire tout ce qui n'est pas qualifié et identifié par le salarié comme « personnel » (*CA Chambéry, 6 nov. 2003, n° 2002/358*). Notons au passage que l'inscription d'un site Internet sur la liste des « favoris » de l'ordinateur ne lui confère aucun caractère personnel.
Par application de ce principe de professionnalité, et sous réserve de respecter les dispositions du droit du travail et celles de la loi « Informatique et Libertés », l'employeur peut donc accéder aux fichiers et correspondances du salarié **non identifiés comme « personnels »**, hors de la présence de ce dernier (*L. n° 78-17, 6 janv. 1978, JO 7 janv.*).
Sous certaines conditions supplémentaires, il peut même accéder aux fichiers et mails personnels pour démontrer les fautes ou abus du salarié et justifier son licenciement.

LES MOYENS INFORMATIQUES TRAITANT DES DONNÉES PERSONNELLES

Reprenons depuis le début : l'article 2 de la loi « Informatique et Libertés » définit un « *traitement de données à caractère personnel* » comme toute opération ou tout ensemble d'opérations portant sur une information relative à une personne physique identifiée ou identifiable, et ce quel que soit le procédé utilisé.
Dès lors, les moyens informatiques mis en place au sein de l'entreprise, qu'ils aient pour objectif ou non d'opérer un contrôle de l'activité du salarié, tombent sous le coup de la loi « Informatique et Libertés » puisqu'ils requièrent, pour fonctionner, la collecte des nom, prénom, adresse mail, etc. du salarié.
L'employeur doit donc, préalablement à la mise en œuvre de ces moyens, respecter un certain nombre de règles (déclaration à la Cnil et information du salarié) pour que le traitement de ces données personnelles soit légal.
À défaut, il est non seulement passible de sanctions, tant au titre de la violation de la loi « Informatique et Libertés » que des dispositions du droit du travail (*C. trav., art. L. 1221-9*), mais il ne pourra en outre pas utiliser ces informations pour justifier le licenciement d'un salarié. La Cour de cassation considérant en effet que les informations ont été collectées de manière illicite (*Cass. soc., 29 janv. 2008, n° 06-45.814*).

La déclaration obligatoire

La loi « Informatique et Libertés » impose une **déclaration préalable auprès de la Commission nationale de l'informatique et des libertés** (Cnil) de tout traitement automatisé d'informations nominatives permettant l'identification directe ou indirecte d'une personne. Le format de déclaration varie selon la nature des données collectées, leur destination, le niveau d'intrusion dans la vie privée, etc.
Procéder à un traitement de données à caractère personnel sans respecter les prescriptions de la loi est puni de cinq ans d'emprisonnement et de 300 000 € d'amende (*C. pén., art. 226-17*). À bon entendeur…
À l'heure actuelle, les outils de gestion du personnel, notamment l'accès à des moyens informatiques, requièrent donc bien une déclaration à la Cnil. Cette dernière a d'ailleurs mis en place un dispositif de déclaration simplifiée qui permet aux employeurs de vérifier leur conformité avec les exigences de la loi, notamment l'obligation d'information préalable des personnes concernées.

Information individuelle

Cette obligation générale d'information porte notamment sur l'**identité des destinataires** des données et le lieu où s'exerce le **droit d'accès et de rectification** des personnes concernées.
S'agissant plus précisément des salariés, le Code du travail prévoit également qu'*« aucune information concernant personnellement un salarié […] ne peut être collectée par un dispositif qui n'a pas été porté préalablement à la connaissance du salarié […] »* (*C. trav., art. L. 1221-9*).
L'employeur peut satisfaire à cette obligation (et en apporter la preuve) par l'insertion d'une clause dans le contrat de travail, ou d'une mention dans le règlement intérieur (qui fait l'objet d'un affichage et d'une remise en mains propres aux nouveaux salariés), ou par la diffusion d'une note de service. Qu'elle résulte des dispositions du Code du travail ou de la loi du 6 janvier 1978, l'information préalable, condition de la loyauté de la collecte des données, est nécessaire à la licéité d'un traitement de données mais pas suffisante selon la taille de l'entreprise.

Information du CE

L'article L. 2323-32 du Code du travail prévoit également l'**information du comité d'entreprise** sur les traitements automatisés de gestion du personnel préalablement à leur introduction dans l'entreprise et leur modification ultérieure. Plus avant, information et consultation sont même requises quand les moyens mis en œuvre permettent un contrôle de l'activité des salariés.
À titre d'exemple, la mise en place de caméras de vidéosurveillance dans les locaux ou d'un procédé de géo-localisation dans les véhicules de fonction des salariés nécessitera l'information et la consultation préalable du comité d'entreprise, notamment si l'employeur souhaite utiliser ces procédés « *pour vérifier, contrôler et établir les manquements ou les*

fautes des salariés » (*CA Pau, 14 avr. 2008, n° 07/00352 : « Dès lors qu'il n'est pas démontré que le comité d'entreprise a été informé et consulté, préalablement à la décision de l'employeur de mettre en œuvre dans l'entreprise un système de vidéosurveillance, celui-ci ne saurait être considéré comme la mise en place de moyens ou de techniques permettant un contrôle de l'activité des salariés, de sorte qu'il est interdit à l'employeur d'utiliser des moyens de preuve obtenus à l'aide de ce procédé pour vérifier, contrôler et établir les manquements ou les fautes des salariés »*).

LA SANCTION DE L'USAGE PERSONNEL D'INTERNET AU TRAVAIL

Il n'existe pas de principe d'interdiction générale et absolue d'utilisation d'Internet à des fins personnelles. Une telle interdiction, pour être opposable au salarié (*CA Douai, 28 févr. 2005, n° 01/01258*), supposerait par conséquent une décision de l'employeur (*CA Douai, 17 déc. 2004, n° 04/00517*) insérée dans le règlement intérieur par exemple.
Gardons à l'esprit qu'il est communément admis par l'ensemble des juridictions que l'employeur doit faire preuve d'une certaine tolérance à l'égard d'une utilisation personnelle modérée d'Internet par le salarié. C'est d'ailleurs l'objet de la charte informatique.
Pour autant, même si l'usage personnel n'est pas prohibé par l'employeur, **l'abus** peut bien entendu être sanctionné, le salarié étant rémunéré pour travailler et non pour surfer.
Aussi, l'utilisation par le salarié des outils informatiques mis à sa disposition pendant son temps de travail, à des fins étrangères à l'activité de l'entreprise et d'une certaine gravité, pourra justifier son licenciement.
Quelques illustrations permettent d'éclairer les critères retenus par les juges pour apprécier la gravité de la faute.

La cause réelle et sérieuse de licenciement

La jurisprudence considère qu'une utilisation personnelle d'Internet, **sans intention de nuire et sans abus manifeste**, sera au mieux qualifiée de cause réelle et sérieuse.
La consultation d'un site web personnel à caractère sado-masochiste créé par un collègue au mépris du règlement intérieur (*CA Grenoble, 10 nov. 2003, n° 00/04741*), l'envoi d'un courriel humoristique à partir de l'adresse professionnelle transmis en boule de neige et causant un encombrement de la messagerie de l'entreprise (*CA Toulouse, 4 nov. 2004, n° 04/00859*) ou encore l'envoi de 156 mails personnels en 2 mois (*CPH Angers, 30 janv. 2009, n° 09-00286.* Cette décision a été sanctionnée en appel faute « *d'éléments sérieux* ») ont été qualifiés de cause réelle et sérieuse justifiant un licenciement.
À l'inverse, la cause réelle et sérieuse ne sera pas retenue si le licenciement est uniquement fondé sur un usage raisonnable d'Internet par le salarié (à titre d'exemple, ne dépassant pas 10 heures sur un an : *CA Douai, 17 déc. 2004, n° 04/00517*), ou sur la connexion à une dizaine de sites Internet, ne dépassant pas chacune une minute, pour assurer la défense d'un collègue licencié (*CA Paris, 22e ch., 24 mai 2005, n° 04/36576*).

La faute grave

Seront, en revanche, qualifiés de faute grave les agissements faisant courir un **risque de sécurité** pour l'entreprise, pouvant **nuire à la réputation de l'employeur** ou constituant un **abus manifeste**.
Il en est ainsi de la consultation de sites pornographiques et pédophiles plus de 8 heures par mois par un salarié travaillant à mi-temps dans l'entreprise (*CA Douai, 28 févr. 2005, n° 01/01258*) et du stockage de nombreux films et images pornographiques sur le disque dur du poste de travail (1430 fichiers représentant plus de 509 MO : *CA Paris, 21e ch., 12 mai 2005, n° 04/36746*).
Plus récemment et pour illustrer un abus rendant impossible le maintien du salarié dans l'entreprise, la Cour de cassation a qualifié de faute grave le fait pour un salarié d'avoir surfé environ 41 heures sur un mois via la connexion Internet de son entreprise (*Cass. soc., 18 mars 2009, n° 07-44.247*).

LA PREUVE DE LA FAUTE

Les preuves collectées par l'employeur pourront être déclarées irrecevables non seulement si les moyens informatiques ou de surveillance n'ont pas été mis en œuvre dans les conditions requises par la loi « Informatique et Libertés », mais aussi en cas de doute sur l'identité de l'auteur des faits reprochés.
En effet, en matière sociale, la preuve doit être licite, loyale et proportionnelle. L'employeur doit prouver que la faute est imputable au salarié, que les faits se sont déroulés pendant le temps de travail et que la preuve a été licitement collectée et conservée.

Imputabilité

Les preuves établies contre un salarié alors qu'il partage son poste informatique et que les comptes utilisateurs ne sont pas séparés (*CA Douai, 17 déc. 2004, n° 04/00517)* ou qu'il partage son bureau avec d'autres salariés dans une ambiance conflictuelle (*CA Metz, 14 déc. 2004, n° 02/03269*) ou encore si les accès ne sont pas protégés par mot de passe (*CA Paris, 7 déc. 2004, n° 03/33571*) ne seront pas recevables.

Le temps de travail

La preuve de l'heure et de la date de l'activité du salarié peut être fournie par **le contrôle des fichiers de journalisation des connexions**. Les fichiers de journalisation des connexions, destinés à identifier et enregistrer toutes les connexions ou tentatives de connexion à un système automatisé d'informations, constituent une mesure de sécurité, généralement préconisée par la Cnil dans le souci que soient assurées la sécurité et la confidentialité des données à caractère personnel, lesquelles ne doivent pas être accessibles à des tiers non autorisés ni utilisées à des fins étrangères ●●●

●●● à celles qui justifient leur traitement. Ils n'ont pas pour vocation première le contrôle des utilisateurs.
Pour autant, l'heure d'ouverture d'un fichier ne démontrant pas nécessairement la durée de connexion, l'employeur devra tenter de connaître la durée et la fréquence de consultation du fichier concerné (*CA Paris, 22e ch., 24 mai 2005, n° 04/36576* : la seule indication des heures de sauvegarde d'un document rédigé par le salarié pendant les heures de travail ne démontre pas l'amplitude du temps consacré à ce travail).
À l'inverse, en ce qui concerne l'utilisation d'Internet et de la messagerie électronique, le **relevé des dates et heures de téléchargement** sur l'ordinateur du salarié suffisent à établir que ces téléchargements ont été réalisés pendant les heures de travail (*CA Besançon, 9 sept. 2003, n° 02/1454*).
De manière générale, plus la fréquence des utilisations sera importante, moins il existera de doutes au profit du salarié.

Licéité

Compte tenu de la présomption de professionnalité présentée ci-dessus, la preuve ne pose véritablement problème que pour relever le caractère abusivement « personnel » de l'activité du salarié.
Pour respecter le principe du droit au secret des correspondances et à l'intimité de la vie privée, les jugent imposent que la consultation de fichiers personnels du salarié « soupçonné » s'opère **en sa présence** ou lorsque celui-ci a été **dûment appelé**, sauf risque ou événement particulier permettant de passer outre cette exigence, comme par exemple l'intrusion d'un virus menaçant le système informatique de l'entreprise (*Cass. soc., 17 mai 2005, n° 03-40.017*).
A ainsi été jugé irrecevable un placement sous scellés opéré par huissier, sans respect du contradictoire, pendant les vacances du salarié et dont le procès-verbal comportait de nombreuses imprécisions (*CA Douai, 17 déc. 2004, n° 04/00517).*

En revanche, la simple vérification par l'administrateur du système informatique de l'entreprise de la nature des sites où s'est connecté le salarié durant son temps de travail, l'identification des sites visités et la transmission des informations obtenues au dirigeant de la société, constituent une procédure licite si la vérification a été opérée à l'occasion de contrôles de routine effectués par le département des ressources humaines sans qu'un système quelconque de surveillance du salarié n'ait été mis en place (*CA Amiens, 7 avr. 2009, n° 08/02085*).

Le recours à l'huissier et au juge

Si l'employeur doute fortement de la loyauté du salarié (au point que ce dernier pourrait effacer toutes les preuves compromettantes avant l'établissement de preuves permettant de justifier son licenciement), il peut recourir aux dispositions de l'article 145 du Code procédure civile qui dispose que « *s'il existe un motif légitime de conserver ou d'établir avant tout procès la preuve de faits dont pourrait dépendre la solution d'un litige, les mesures d'instruction légalement admissibles peuvent être ordonnées à la demande de tout intéressé, sur requête ou en référé* ».
Cette procédure n'étant pas contradictoire, **le salarié n'est pas informé** de l'ordonnance du juge autorisant l'employeur et un huissier à s'introduire sur son ordinateur ou dans sa correspondance privée ou professionnelle (*C. proc. civ., art. 493*).
Concrètement, l'huissier ou l'expert désigné se présente dans l'entreprise muni de l'ordonnance qu'il présente au salarié concerné, et exécute la mission pour laquelle il a été mandaté par le juge sans que le salarié puisse s'y opposer. Il laisse ensuite copie de l'ordonnance au salarié.
Bien entendu, la demande doit être particulièrement motivée, imposant à l'employeur d'étayer précisément ses soupçons et de justifier d'un risque pour l'entreprise.
Un conseil donc… restez concentré sur votre travail ! ■