

Le régime juridique applicable à la surveillance par l'employeur de l'utilisation faite des outils informatiques et de l'Internet mis dans l'entreprise à la disposition du salarié

Depuis le célèbre arrêt NIKON¹ rendu en 2001, la Haute juridiction a eu l'occasion non seulement de confirmer le droit du salarié au respect de l'intimité de sa vie privée même au temps et au lieu de travail, mais également de le délimiter en précisant **son exacte étendue, l'étendue des pouvoirs de l'employeur et dernièrement, ceux de l'administrateur réseau**².

Afin d'y voir plus clair, nous reprendrons les apports essentiels de l'évolution jurisprudentielle en la matière en distinguant d'une part l'utilisation à des fins personnelles, pendant le temps de travail, des outils informatiques mis à la disposition du salarié par l'employeur (I) et d'autre part, l'utilisation de l'Internet pendant le temps de travail depuis l'ordinateur mis à disposition par l'employeur (II).

I. L'utilisation à des fins personnelles des outils informatiques mis à la disposition du salarié par l'employeur

Les outils informatiques ici traités sont **les courriers électroniques, les dossiers et les fichiers**.

Le principe applicable à ces outils informatiques a été dégagé par l'arrêt Nikon suscitée. Dans cette affaire, il était question de courriers électroniques envoyés et reçus depuis l'ordinateur professionnel du salarié. La Haute juridiction a reconnu à ce dernier, **sur le fondement du principe du secret des correspondances**³, **un espace protégé au sein même de l'entreprise et quasiment inviolable au nom du nécessaire respect à la vie privée**, en considérant que « *le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée* » ; « *En conséquence (...) l'employeur ne peut (...) prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail* ».

En toute logique, cette jurisprudence fut étendue, en 2005, aux fichiers contenus dans les répertoires informatiques d'un disque dur d'un ordinateur mis à disposition du salarié⁴ ; puis, en 2006, aux documents détenus par le salarié dans le bureau mis à sa disposition par l'entreprise⁵.

Au fil du temps, la position de la Cour de cassation exprimée par l'arrêt Nikon, position excessive, a subi des tempéraments avec les arrêts rendus postérieurs. Ils constituent la jurisprudence applicable à ce jour, exposée ci-après.

Le principe. Il est interdit à l'employeur de prendre connaissance des messages électroniques, fichiers et dossiers considérés par le salarié comme personnels.

Les exceptions à ce principe. La jurisprudence considère que le principe suscitée souffre de deux exceptions⁶ :

- **la présence ou convocation du salarié**;
- hors présence du salarié, s'il y a un **risque ou évènement particulier**. Ce qui n'est pas le cas, par exemple, de la découverte de photos érotiques dans un tiroir du bureau d'un salarié.

¹ Cass.soc. Nikon, 2 octobre 2001

² Cass.soc., Sanofi Chilie c/M.Guzzi et a., 17 juin 2009

³ Principe issu de la Liberté Fondamentale consacrée par l'article 8 de la Convention Européenne de Sauvegarde des Droits de l'Homme et des Libertés Fondamentales

⁴ Cass.soc., Cathnet-Science, 17 mai 2005

⁵ Cass.Soc., 18 octobre 2006

⁶ arrêt Cathnet-Science suscitée

Dans ces hypothèses⁷, l'employeur pourra alors prendre connaissance, à titre exceptionnel, de la correspondance privée ou des fichiers ou dossiers personnels du salarié, de préférence en présence d'un tiers.

Il a aussi été admis que l'employeur ait communication de messages, fichiers ou documents personnels du salarié, hors de la présence de ce dernier et sans le convoquer, s'il parvient à obtenir du juge, sur le fondement de l'article 145 du NCPC, l'aide d'**un huissier de justice**. Ainsi, par exemple, pour obtenir communication de la teneur de courriels stockés par ce dernier sur le disque dur de l'ordinateur mis à sa disposition par son employeur⁸ ou encore, pour enregistrer une copie des données contenues dans l'ordinateur mis à la disposition du salarié⁹. Dans ces deux espèces, l'employeur disposait, en raison de faits propres à chaque espèce, d'**un motif légitime** indispensable pour obtenir du juge une telle mesure d'instruction ; à savoir la suspicion d'actes de **concurrence déloyale**.

L'application de ce principe et de ses exceptions est devenue simple : lorsque les messages, fichiers ou documents ne sont clairement identifiés comme personnel de **par leur objet** ou, depuis 2009, de **par leur classement**¹⁰, ils **sont présumés professionnels**¹¹ et par conséquent, l'employeur peut librement y accéder sans que le salarié concerné soit présent ou ait été convoqué ou encore, sans qu'il y ait un risque ou événement particulier le justifiant. Cette présomption, combinée aux exceptions suscitées, a considérablement élargi le pouvoir de contrôle de l'employeur par rapport à la solution initiale posée cinq ans auparavant. L'équilibre entre les droits du salarié et le pouvoir de direction de l'employeur face aux TIC est ainsi rétabli.

S'est posée la question de savoir si l'employeur pouvait obtenir la communication de messages, dossiers ou fichiers personnels par le biais de son administrateur réseau. En effet, eu égard à sa fonction dans l'entreprise aux termes de laquelle il doit veiller à assurer le fonctionnement normal et la sécurité des réseaux et systèmes informatiques, il peut légitimement accéder à l'une quelconque des données contenues dans les outils mis à la disposition des salariés par l'entreprise. En tel cas, peut-il porter à la connaissance de l'employeur les messages, fichiers ou dossiers personnels du salarié ?

La Cour de cassation a eu l'occasion de répondre à cette question en juin dernier dans l'arrêt Sanofi suscitée. Elle distingue nettement les pouvoirs de l'employeur et ceux de l'administrateur réseau, considérant que **suite à un incident de sécurité du système informatique, l'administrateur réseau peut légitimement procéder à un contrôle a posteriori de la messagerie des salariés**¹². Cette solution est conforme avec la position de la CNIL en la matière. En revanche, s'agissant de l'employeur, c'est purement et simplement l'arrêt Cathnet-Science qui s'applique: sauf présence ou convocation du salarié, d'un risque particulier ou d'un huissier, l'employeur ne peut pas effectuer un tel contrôle et ouvrir les messages personnels des salariés. Il ne peut non plus obtenir communication de leur teneur via son administrateur réseau. Effectivement, l'administrateur ne peut lui faire une telle communication sans violer le secret des correspondances et **son obligation de confidentialité**. On imagine dans quelle situation délicate se trouve ainsi placé l'administrateur réseau : il n'a pas le droit à l'erreur dans son appréciation de l'incident de sécurité et doit s'empêcher de communiquer ce qu'il découvrira à l'employeur.

Pour conclure cette partie, j'indiquerai que pour que les choses soient simples et transparentes, la rédaction d'**une charte informatique** fixant les règles du jeu (mise en évidence de l'intérêt, pour le salarié, de distinguer clairement les messages, fichiers et documents personnels; description du

⁷ Ces exceptions ne sont pas sans rappeler celles retenue en matière de fouille des casiers par l'employeur (Cass.soc., 15 avril 2008) ou encore de contrôle des sacs (Cass.soc., 11 février 2009)

⁸ Cass.soc., DATACEP, 23 mai 2007

⁹ Cass.soc., arrêt du 10 juin 2008

¹⁰ Cass.soc., Sanofi Chilie c/M.Guzzi et a., 17 juin 2009

¹¹ Cass., soc., 18 octobre 2006

¹² En l'espèce, le contrôle de la messagerie concernait 17 salariés et faisait suite à la réception par la société de plusieurs lettres anonymes dont le contenu laissait penser que leur auteur avait eu accès à des données confidentielles et verrouillées de l'entreprise

pouvoir de l'employeur sur les messages, fichiers et documents présumés professionnels ; description du pouvoir de l'administrateur réseau, etc) est vivement recommandée.

Une telle charte pourra également édicter les règles en matière d'utilisation de l'Internet à des fins personnelles.

II. L'utilisation à des fins personnelles de l'Internet mis à disposition du salarié par l'employeur

Alors qu'en 2001¹³, la Cour de cassation avait invalidé toute interdiction par l'employeur d'une utilisation personnelle de l'ordinateur mis à disposition, incluant ainsi la connexion à l'Internet et donc une navigation privée du salarié, elle a très nettement assoupli sa position, en 2004 puis dernièrement en 2008.

Ainsi, en 2004¹⁴, tout en maintenant cette solution, elle a cependant précisé que **toute navigation** au temps et au lieu de travail **ne sera pas protégée** par le droit au respect à la vie privée du salarié ; ainsi **des navigations à titre personnel jugées déraisonnables**. Se faisant, elle a reconnu à l'employeur un certain pouvoir de contrôle et de surveillance de l'activité du salarié l'amenant à rechercher et apprécier le type d'usage fait par le salarié de l'Internet (types de sites consultés, temps consacré, etc...) et par conséquent, la possibilité d'exercer son pouvoir de sanction. A cet égard, le respect des obligations CNIL est indispensable : déclaration du traitement (logs, fichiers de journalisation) et information des salariés. Cette information se fera le plus souvent par le biais de la charte informatique.

Puis, en 2008, la Haute juridiction est allée encore plus loin, délaissant la solution retenue sept ans auparavant. En effet, elle a institué une **présomption de caractère professionnel** des « *connexions effectuées pendant le temps de travail grâce à l'outil informatique mis à la disposition du salarié pour l'exécution de son travail* ». Ainsi se trouve consacré le **pouvoir de contrôle général (avec ou hors présence du salarié) de l'employeur sur l'historique de navigation** pour juger du caractère raisonnable ou non de l'usage par le salarié de l'Internet à titre personnel. Dans la mesure où un usage jugé déraisonnable pourra donner lieu à l'application d'une sanction, il y a lieu là encore de respecter scrupuleusement les obligations CNIL et, par souci de transparence, de détailler la teneur de ce pouvoir général de contrôle et de sanction dans la charte informatique.

Pour conclure, on notera qu'au fil du temps, la Cour de cassation a délaissé une position excessive et déraisonnable pour tenter de parvenir à davantage d'équilibre entre le pouvoir de contrôle de l'employeur sur l'activité des salariés dans le cadre de son pouvoir disciplinaire et de direction avec les droits et libertés fondamentales des salariés, tels que la protection de la vie privée.



Rédactrice : Claire – Avis-droit-social.net

¹³ arrêt Nikon suscité

¹⁴ Cass.crim., Nortel, 19 mai 2004