FEDIL

Publication

BRÈVES DE JURISPRUDENCE 2/2017: LA SURVEILLANCE DU SALARIÉ

SUMMARY / CONTENT

INTRODUCTION

Que ce soit à travers des systèmes de vidéosurveillance, de géolocalisation, de cybersurveillance, ou bien d'autres encore, l'employeur dispose de plus en plus de moyens technologiques pour contrôler si les salariés exécutent leur travail. Plus délicat que les aspects technologiques, est la question de savoir quels systèmes peuvent effectivement être appliqués en vertu de la loi.

Le but de ce numéro des brèves de jurisprudences est de fournir un aperçu des différents systèmes de surveillance qui sont ou ne sont pas acceptés et des règles encadrant leur mise en œuvre. Quel que soit le système envisagé, il convient de rappeler que les magistrats sont tenus d'analyser la légalité de tout

traitement de données à des fins de surveillance à la lumière des dispositions légales applicables. En matière de surveillance du personnel, plus précisément, il s'agit essentiellement de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel ainsi que l'article L. 261-1. du Code du travail.

Ce dernier énonce en effet cinq scénarios dans lesquels la surveillance opérée par l'employeur peut être admise, à savoir si elle est nécessaire :

- pour les besoins de sécurité et de santé des salariés, ou
- pour les besoins de protection des biens de l'entreprise, ou
- pour le contrôle du processus de production portant uniquement sur les machines, ou
- pour le contrôle temporaire de production ou des prestations du salarié, lorsqu'une telle mesure est le seul moyen pour déterminer le salaire exact, ou
- dans le cadre d'une organisation de travail selon l'horaire mobile.

Notons encore que, peu importe la finalité recherchée par la surveillance, l'employeur doit toujours informer préalablement les salariés visés par la mesure, le comité mixte (qui reste compétent jusqu'aux prochaines élections sociales en février/mars 2019) ou, à défaut, la délégation du personnel (si l'entreprise ne dispose pas de comité mixte) ou, à défaut, l'Inspection du Travail et des Mines (ITM). Par ailleurs, tout traitement de données à des fins de surveillance doit être autorisé au préalable par la Commission nationale pour la protection des données (CNPD), du moins encore jusqu'à l'entrée en vigueur du nouveau projet de loi n° 7049 qui remplacera la procédure d'autorisation par une simple notification de la part de l'employeur.

Avant de mettre en place un système de surveillance, il convient donc toujours d'analyser au cas par cas si la surveillance envisagée l'est bien pour satisfaire l'une des cinq finalités décrites à l'article L.261-1. du Code du travail et puis de respecter les procédures d'information et d'autorisation préalables.

Le non-respect de ces dispositions peut donner lieu à des sanctions pénales telles que prévues à l'article L. 261-2. du Code du travail et surtout au rejet des résultats de la surveillance à titre de preuve en justice, tel que le démontrent notamment les affaires qui suivent.

SURVEILLANCE DES E-MAILS DU SALARIÉ

PREMIÈRE AFFAIRE : VIOLATION DE L'ARTICLE 8 CEDH

Résumé : M. B rbulescu, ressortissant roumain, ouvre, sur invitation de son employeur, un compte Yahoo Messenger afin de répondre aux demandes des clients. Après avoir informé M. B rbulescu que ses communications sur ledit compte avaient été surveillées, son employeur procède à son licenciement pour avoir échangé via ce compte des messages privés avec son frère et sa fiancée (45 pages de messages en une semaine !), malgré l'interdiction générale au sein de l'entreprise d'utiliser Internet à des fins personnelles. Dans son premier arrêt du 12 janvier 2016, la Cour européenne des droits de l'homme (CEDH) considère que la surveillance de l'employeur avait été raisonnable dans le contexte d'une procédure disciplinaire. Partant, elle conclut à la non-violation du droit de M. B rbulescu au respect de sa vie privée et de sa correspondance en vertu de l'article 8 de la Convention. L'affaire est cependant renvoyée à la demande de M. B rbulescu devant la Grande Chambre de la CEDH qui, au contraire, décide

ce qui suit :

« Tout au long de la procédure, le requérant s'est plaint notamment, tant devant les juridictions internes que devant la Cour, de la surveillance faite par son employeur de ses communications sur les comptes Yahoo Messenger en question et de l'utilisation du contenu de ces communications dans le cadre de la procédure disciplinaire dont il a fait l'objet.

(...) Il ressort des éléments produits devant la Cour que le requérant avait été informé du règlement intérieur de son employeur, qui prohibait l'usage des ressources de l'entreprise à des fins personnelles. Il avait pris connaissance du contenu de ce document et l'avait signé, le 20 décembre 2006. De plus, l'employeur avait fait circuler parmi tous les employés une note d'information, datée du 26 juin 2007, qui rappelait l'interdiction d'utiliser les ressources de l'entreprise à des fins personnelles et précisait qu'une employée avait été licenciée pour avoir enfreint cette interdiction.

(...) En ce qui concerne la question de savoir si le requérant avait reçu un avertissement préalable de la part de son employeur, la Cour rappelle qu'elle a déjà conclu qu'il n'apparaissait pas que l'intéressé eût été informé à l'avance de l'étendue et de la nature de la surveillance opérée par l'entreprise ni de la possibilité que celle-ci ait accès au contenu même de ses communications. (...)

La Cour estime que pour pouvoir être considéré comme préalable, l'avertissement de l'employeur doit être donné avant que celui-ci ne commence son activité de surveillance, a fortiori lorsque la surveillance implique également l'accès au contenu des communications des employés. (...)

Quant à l'étendue de la surveillance opérée et du degré d'intrusion dans la vie privée du requérant, la Cour relève que cette question n'a été examinée ni par le tribunal départemental ni par la cour d'appel, alors qu'il apparaît que l'employeur a enregistré en temps réel l'intégralité des communications passées par le requérant pendant la période de surveillance, qu'il y a eu accès et qu'il en a imprimé le contenu. (...)

Dans ces conditions, il apparaît que les juridictions nationales ont manqué, d'une part, à vérifier, en particulier, si le requérant avait été préalablement averti par son employeur de la possibilité que ses communications sur Yahoo Messenger soient surveillées et, d'autre part, à tenir compte du fait qu'il n'avait été informé ni de la nature ni de l'étendue de la surveillance dont il avait fait l'objet, ainsi que du degré d'intrusion dans sa vie privée et sa correspondance. De surcroît, elles ont failli à déterminer, premièrement, quelles raisons concrètes avaient justifié la mise en place des mesures de surveillance, deuxièmement, si l'employeur avait pu faire usage de mesures moins intrusives pour la vie privée et la correspondance du requérant et, troisièmement, si l'accès au contenu des communications aurait été possible à son insu. Eu égard à l'ensemble des considérations qui précèdent et nonobstant la marge d'appréciation de l'État défendeur, la Cour estime que les autorités internes n'ont pas protégé de manière adéquate le droit du requérant au respect de sa vie privée et de sa correspondance et que, dès lors, elles n'ont pas ménagé un juste équilibre entre les intérêts en jeu. Partant, il y a eu violation de l'article 8 de la Convention ».

CJUE, B rbulescu c. Roumanie (requête no 61496/08) du 05/09/2017

Commentaire : L'arrêt rendu a vocation à s'appliquer dans tous les 47 Etats membres du Conseil de l'Europe, y compris au Luxembourg. Les juridictions nationales devront ainsi s'en tenir aux critères établis par la CEDH, chaque fois qu'elles auront à apprécier si une mesure de surveillance mise en œuvre par l'employeur s'est déroulée dans le respect de la vie privée et de la

*correspondance du salarié sur le lieu de travail. Cela pourrait les obliger à exercer à l'avenir un contrôle beaucoup plus strict que jusqu'à présent sur (i) les raisons qui ont motivé la surveillance, (ii) l'existence éventuelle de mesures moins intrusives et (iii) l'étendue de l'information préalable du s*alarié surveillé.

DEUXIÈEME AFFAIRE : CONDAMNATION AU PÉNAL DE L'EMPLOYEUR

Résumé : La salariée est dispensée de travailler à partir de la date de son licenciement. Pendant la durée de son préavis, on lui refuse tout accès à son lieu de travail, et partant à ses e-mails professionnels. Plus tard, elle est informée par certains de ses contacts que des courriels qu'ils lui ont envoyés pendant cette période, leur ont été retournés avec la mention que l'employeur les avait ouverts. Sur cette base, elle décide de saisir la justice d'une procédure pénale à l'encontre tant de la société qui l'employait que du dirigeant physique de cette dernière.

« XX estime que c'est à tort que les juges de première instance ont acquitté ses anciens employeurs des infractions mises à leur charge, dans la mesure où ils auraient ouvert des courriels qui étaient d'évidence à caractère privé dans son adresse professionnelle et ce après son licenciement. Ainsi, les dirigeants de la société VISTRA auraient consulté un email provenant d'une personne travaillant auprès de la banque ING malgré le fait qu'ils avaient connaissance du fait que XX n'avait, en sa qualité d'auditeur interne, aucun contact professionnel avec cette banque. Ils auraient encore ouvert un courriel intitulé « Privé-Drink Nouvel An », malgré l'indication expresse que ledit message était à caractère privé. Ils auraient finalement ouvert un message lui adressé sur son adresse professionnelle par un employé de la banque RBC DEXIA qui portait l'indication expresse de son caractère privé, à savoir la mention « PRIVATE CONFIDENTIAL ». (...)

Les employeurs contestent encore n'avoir eu aucun droit de regard sur les emails de XX litigieux, alors qu'ils lui seraient parvenus non seulement sur la messagerie professionnelle qui a été mise à disposition de l'employée par la société VISTRA à des fins professionnelles et ce pendant la période de préavis de licenciement de XX qui avait été dispensée de travailler. Il aurait partant été légitime que les courriels de XX aient été dirigés vers ses supérieurs hiérarchiques dans la mesure où l'entreprise pour laquelle elle aurait travaillé, devait être en mesure de traiter les informations en relation avec l'activité de l'employée. (...)

Le traitement des données à caractère personnel est protégé à titre général par les dispositions de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, qui prévoit en son article 11 que « le traitement à des fins de surveillance sur le lieu de travail ne peut être mis en œuvre par l'employeur, s'il est le responsable du traitement, que dans les conditions visées à l'article L. 261-1. du Code du travail ».

La même loi définit en son article 2 (e) la notion de « donnée à caractère personnel » comme étant « toute information de quelque nature qu'elle soit et indépendamment de son support, y compris le son et l'image, concernant une personne identifiée ou identifiable (...) ».

Le traitement de ces données à caractère personnel à des fins de surveillance sur le lieu de travail est soumis à une autorisation préalable de la Commission nationale pour la protection des données conformément à l'article 14 de la loi de 2002 précitée et ne peut être mis en œuvre aux termes de l'article L. 261-1. du

Code du travail que « s'il est nécessaire, 1. pour les besoins de sécurité et de santé des employés, ou, 2. pour des besoins de protection des biens de l'entreprise, ou, 3. pour le contrôle du processus de production portant uniquement sur les machines, ou, 4. pour le contrôle temporaire de production ou des prestations du salarié, lorsqu'une telle mesure est le seul moyen pour déterminer le salaire exact, ou, 5. dans le cadre d'une organisation de travail selon l'horaire mobile conformément au présent code (...) ».

L'article L. 261-1. du Code du travail précise encore que « le consentement de la personne concernée ne rend pas légitime le traitement mis en œuvre par l'employeur ». (...)

L'utilisation de la messagerie professionnelle à des fins privées n'est partant, contrairement aux assertions des cités directs, pas interdite par la société VISTRA à ses employés. Il ne ressort également pas du règlement interne de la société appelée « VISTRA GROUP SECURITY POLICY », versé en cause, que les employés de la société VISTRA se seraient engagés à ne pas utiliser la messagerie professionnelle à des fins privées. (...)

Il ressort de ce qui précède que l'utilisation par XX de sa messagerie professionnelle auprès de la société VISTRA a des fins privées ne lui était pas interdite. Les messages transitant par ce biais sont cependant à considérer, sauf preuve du contraire, comme des messages à caractère professionnel.

La Cour considère, tout comme les juges de première instance, que le premier courriel en cause datant du 1ier décembre 2011 adressé par CC de la banque ING à XX, ne comportant aucun intitulé ne peut pas être considéré comme faisant preuve du caractère privé de l'envoi, alors qu'il ne permet, faute d'intitulé, pas d'entrevoir sa nature. Le fait que XX n'ait le cas échéant pas eu de rapports directs avec d'autres personnes que l'auditeur externe et la CSSF et que le message provienne d'une société qui, le cas échéant, n'a pas de relations directes avec la société VISTRA ne permet pas de conclure à son caractère ostentatoirement privé. (...)

Il en va de même du second message visé par la citation directe, à savoir le courriel du 15 décembre 2011 intitulé « Privé-Drink Nouvel An » provenant de BB qui travaille auprès de la société LORANG. Le caractère privé de ce message laisse d'être établi, alors que ni l'intitulé « Privé-Drink Nouvel An », ni son contenu ne permettent de conclure au caractère privé de ce message, mais font suggérer des relations professionnelles. La présomption du caractère professionnel du message n'a partant pas été renversée, de sorte qu'en consultant ledit message les intimés en cause n'ont pas enfreint les dispositions légales précitées.

Quant au dernier courriel litigieux, à savoir, le courriel du 19 décembre 2011, provenant de l'adresse professionnelle de AA, auprès de la RBC DEXIA IS, le caractère privé résulte des termes mêmes de l'intitulé du message. En indiquant non seulement « PRIVATE » mais surtout « CONFIDENTIAL » l'expéditrice a visé clairement XX comme étant le seul destinataire de son envoi, de sorte que le caractère privé du courriel est établi. Les dispositions légales assurant la protection des données à caractère personnel et la confidentialité des communications effectuées au moyen d'un réseau de communications public et de services de communications électroniques accessibles au public n'exigeant pas de dol spécial pour la constitution de l'élément moral des infractions visées, la simple transgression de la loi par ceux qui ont consulté le message en cause implique leur intention coupable. (...)

Le message du 19 décembre 2011 adressé par BB à XX et portant la mention « PRIVATE CONFIDENTIAL » a seul donné lieu à condamnation au pénal de ZZ et de la société VISTRA. XX reste cependant à défaut de justifier d'un quelconque

préjudice moral du simple fait que l'un de ses anciens employeurs a consulté ledit courriel qui ne contient qu'une simple demande générale de réponse. Le jugement entrepris est partant à confirmer au civil bien que pour d'autres motifs ».

CSJ du 28/04/2015 n° 159/15 du rôle

Commentaire : Bien que les amendes ne s'élevaient qu'à 500 euros, l'une pour la société, l'autre pour son dirigeant, cette affaire montre clairement que la consultation des courriels privés des salariés peut conduire à de sérieuses condamnations au pénal et doit se dérouler dans le strict respect des dispositions légales assurant la protection des données à caractère personnel et la confidentialité des communications effectuées au moyen d'un réseau ou service de communications. Par ailleurs, cet arrêt fournit des informations précieuses sur ce qu'on doit entendre exactement par « message privé ». Ainsi, les messages transitant par la messagerie professionnelle sont présumés être des messages à caractère professionnel. En l'espèce, le salarié a cependant réussi à renverser cette présomption et à prouver le caractère privé du message litigieux puisque ce dernier indiquait clairement dans son objet qu'il était « PRIVATE CONFIDENTIAL».

SURVEILLANCE À TRAVERS UN SYSTÈME DE GÉOLOCALISATION (GPS)

Résumé : Grâce à un système de géolocalisation installé dans la voiture de fonction, l'employeur a pu découvrir que son salarié utilisait ladite voiture qui, en vertu de son contrat de travail lui avait été mis à disposition exclusivement pour ses déplacements professionnels, également à titre privé, à une heure tardive du jour et sans rendez-vous indiqué dans son horaire. Dans le cadre du procès qui suit la résiliation du contrat de travail, le salarié proteste contre la licéité des listings obtenus à l'aide de ce système de géolocalisation. Il prétend, entre autres, que le système n'aurait jamais été ni autorisé par le CNPD, ni porté à son attention.

« (...) En vertu de l'article L. 261-1. du Code du travail le traitement des données à caractère personnel à des fins de surveillance sur le lieu du travail n'est possible que dans certaines hypothèses spécifiques, notamment dans le cadre d'une organisation de travail selon l'horaire mobile et à condition que la personne concernée soit informée préalablement. Si, au vu des explications circonstanciées fournies par la société (...), il n'est pas à exclure que A ait pris connaissance, lors de la remise du véhicule, de la note de service du 26 novembre 2013 relative au système de géolocalisation dans les véhicules de service, (...), il n'en demeure pas moins qu'une preuve formelle qu'il a été « informé préalablement » par l'employeur n'est pas rapportée en l'espèce.

A ne conteste cependant pas avoir travaillé, selon un système d'horaire mobile, de sorte qu'il devait être conscient et accepter que son employeur procède périodiquement à un contrôle de son temps de travail afin de parer à d'éventuels abus et que la mise à disposition d'un véhicule de service pour l'exercice de son activité professionnelle avait comme corollaire l'obligation pour lui de ne pas utiliser le véhicule à des fins privées.

Dès lors, une éventuelle irrégularité commise par la société (...) au niveau du respect de la disposition légale n'a, en l'espèce, ni compromis le droit à un procès équitable, ni entaché la fiabilité du moyen de preuve contradictoirement débattu entre parties, A n'ayant à aucun moment mis en

cause la fiabilité du système de géolocalisation installé par son employeur. Une éventuelle irrégularité ne saurait ainsi faire échec à la prise en compte des données recueillies par le système de géolocalisation dans le cadre de l'administration de la preuve en justice.

Il n'y a dès lors pas lieu d'écarter les listings obtenus à l'aide du système de géolocalisation installé dans le véhicule de service de A.

En ordre subsidiaire, A demande à voir écarter tous les listings antérieurs de plus de deux mois à la date du licenciement.

Il résulte de l'autorisation précitée de la Commission nationale pour la protection des données que les données ne pourront être conservées au-delà de deux mois, mais que les données « relatives au temps de travail » peuvent être conservées pendant une durée maximale de trois ans.

Comme en l'espèce les données recueillies par le système de géolocalisation du véhicule de service permettent de contrôler le respect par le salarié de son temps de travail, il en suit que le moyen laisse d'être fondé.

Il résulte de l'autorisation précitée de la Commission nationale pour la protection des données qu'il y a lieu de distinguer suivant l'hypothèse où le salarié est autorisé à utiliser le véhicule professionnel à des fins privées, c'est-à-dire en dehors des heures de travail, auquel cas le salarié a droit au respect de sa vie privée et son employeur n'est pas autorisé, en vertu du respect du principe de proportionnalité, à mettre en œuvre la géolocalisation et l'hypothèse où l'employeur s'oppose à l'utilisation du véhicule en dehors des horaires de travail, auquel cas le système de géolocalisation peut rester activé.

Il a été retenu ci-avant que A n'avait droit à un véhicule de service que pour l'exercice de son activité professionnelle.

Il en suit que le système de géolocalisation pouvait rester activé. »

CSJ 26.10.2017 n° 44278 du rôle

Commentaire : Un système de géolocalisation installé dans le véhicule de service est un mécanisme qui permet, entre autres, à l'employeur de faire un suivi du temps de travail dans le cadre d'une organisation de travail selon l'horaire mobile. Si l'objectif est effectivement d'effectuer un tel contrôle périodique du temps de travail et que l'usage du véhicule est clairement limité au cadre professionnel, la Cour d'appel semble, nonobstant le jugement de la CEDH ci-avant, appliquer une approche plutôt tolérante quant à la question de savoir si l'employeur s'est conformé aux exigences légales, notamment en matière d'information préalable du salarié.

SURVEILLANCE À TRAVERS DE CAPTURES D'ÉCRAN

Résumé : Un salarié est licencié pour avoir utilisé Internet à des fins privées de manière répétée et régulière, ceci malgré interdiction formelle de la part de l'employeur et en contournant le blocage d'accès. L'employeur entend prouver les faits allégués par des attestations testimoniales ainsi que par des captures d'écran (« screenshots ») réalisées sur l'ordinateur professionnel du salarié.

« (...) L'employeur déclare avoir fait vérifier par des captures d'écran si le salarié

« avait accès à Internet, s'il faisait usage de cet accès et (…) dans quelle mesure ».

Le contrôle régulier et à distance via TT.) a été effectué à la demande de l'employeur par une entreprise informatique à l'aide d'un dispositif installé sur le serveur de l'entreprise, visant le poste de M. A.), et, suivant l'employeur, par environ six captures d'écran par après-midi pendant une période de dix jours du 14 au 26 septembre 2011.

La capture d'écran constitue une copie de l'image affichée sur un ordinateur. L'ordinateur visé est identifié par l'employeur et, les contrôles étant effectués durant les après-midi où M. A.) occupe seul le bureau, l'usage peut être relié au salarié individualisé. La méthode utilisée permet à l'employeur de connaître le contenu de l'affichage sur l'écran et de suivre l'activité du salarié sur l'ordinateur. La capture d'écran fournit à l'employeur des informations sur un salarié identifié ou identifiable, permet de collecter et d'enregistrer des données à caractère personnel et constitue un traitement de données à caractère personnel au sens de l'article 2 de la loi modifiée du 2 août 2002 relative à la protection des données.

Ce traitement n'était ni nécessaire ni utile pour mettre fin à l'activité du salarié sur Internet.

Cette activité déployée par l'employeur sur le lieu de travail, avec l'usage de moyens techniques, en vue de détecter des mouvements, des images, des paroles ou des écrits ou l'état d'une personne, constitue un traitement de données à caractère personnel à des fins de surveillance, qui n'est possible que s'il est nécessaire pour l'une des finalités définies à l'article L. 261-1. du Code du travail.

Or, même si l'employeur avait constaté ou soupçonné l'usage non-autorisé d'Internet, la surveillance par capture d'écran n'était nécessaire :

- ni pour les besoins de sécurité et de santé des salariés,
- ni pour les besoins de protection des biens de l'entreprise,
- ni pour le contrôle du processus de production portant uniquement sur les machines,
- ni pour le contrôle temporaire de production ou des prestations du salarié, lorsqu'une telle mesure est le seul moyen pour déterminer le salaire exact,
- ni dans le cadre d'une organisation de travail selon l'horaire mobile.

Le traitement de données effectué par l'employeur à des fins de surveillance sur le lieu de travail est intervenu en violation de l'interdiction expresse de l'article L. 261-1. du Code du travail. Dès lors, c'est à juste titre que le Tribunal du travail a écarté des débats les captures d'écran ainsi que les attestations testimoniales, dans la mesure où elles se rapportent au résultat du traitement illicite de données, éléments de preuve résultant d'une voie illégale ».

CSJ 04.07.2016 n° 41114 du rôle

Commentaire : en l'espèce, le licenciement du salarié avec effet immédiat prononcé par l'employeur a été déclaré abusif, parce que les captures d'écran proposées par l'employeur pour prouver que le salarié faisait un usage fréquent d'Internet à des fins privées, notamment par la pratique de jeux et la consultation de sites de vente de voiture, furent rejetées. Selon la Cour d'appel, la surveillance du poste de travail du salarié n'était justifiée par aucune des conditions de l'article L. 261.-1. du Code du travail et les captures d'écran ne pouvaient dès lors pas été prises en considération.

SURVEILLANCE À TRAVERS UNE CAMÉRA DE VIDÉOSURVEILLANCE

Résumé : un salarié est licencié avec effet immédiat en raison notamment d'une consommation excessive d'alcool sur le lieu du travail, mais en dehors des heures normales de travail. En justice, l'employeur entend prouver ce reproche à travers un enregistrement réalisé par caméra de vidéosurveillance. Or, le salarié se base sur les termes de l'autorisation de la CNPD, qui interdit le visionnage des enregistrements dans l'unique but de contrôler le comportement du salarié, pour voir rejeter l'enregistrement en tant que mode de preuve de son état d'ébriété.

« (...) Dans la mesure où la demande de l'employeur de visionner l'enregistrement fait par la caméra de vidéosurveillance n'entre pas dans une des cinq hypothèses limitativement prévues par l'article L. 261-1. du Code du travail ci-avant détaillées, mais tend au contraire à vérifier le comportement de B.) dans la nuit du 14 au 15 juin 2013, plus précisément son prétendu état d'ébriété, elle est à rejeter.

En effet, à l'instar du Tribunal du travail, qui a fait une analyse et application correctes et justes tant de l'article 11 de la loi modifiée du 2 août 2002, relative à la protection des personnes à l'égard du traitement des données à caractère personnel, lequel renvoie à l'article L. 261-1. du Code du travail, que de l'autorisation préalable de la Commission nationale pour la protection des données, qui précise expressément dans son point 4.4., que « la surveillance ne doit pas servir à observer le comportement, les déplacements et les performances des membres du personnel de la société A.) », il y a lieu de confirmer le jugement déféré en ce qu'il a, à bon escient décidé « que la société employeuse ne saurait être admise à prouver les faits reprochés au salarié par les enregistrements qu'elle a effectués au moyen des caméras de vidéosurveillance installées dans son restaurant » pour en conclure à bon droit que « la société employeuse est partant restée en défaut de prouver que le salarié a consommé des boissons alcooliques de son employeur sur son lieu de travail et qu'il y a été ivre ».

CSJ 14.07.2015 n° 41176 du rôle

Commentaire : Cet arrêt est une autre illustration de l'application rigoureuse des conditions de l'article L. 261-1. du Code du travail et de l'autorisation préalable de la CNPD par les juridictions luxembourgeoises. Encore une fois, l'employeur n'a pas réussi à apporter la preuve du comportement qu'il reprochait au salarié puisque son moyen de preuve, à savoir l'enregistrement réalisé par la caméra de surveillance, a été considéré illicite. Par conséquent, le licenciement a été déclaré abusif, malgré le comportement répréhensible et même potentiellement dangereux du salarié, à savoir sa présence sur le lieu de travail en état d'ébriété.

SURVEILLANCE DE JEUX JOUÉS SUR INTERNET

Résumé : Une salariée se fait licencier pour utilisation massive d'un site Internet de jeux communautaires pendant les heures de travail.

« Le règlement intérieur de la société A Luxembourg précise clairement que « l'utilisation / accès Internet est limité exclusivement aux sites revêtant un caractère professionnel en relation directe avec la fonction de l'utilisateur » et

encore « une liste des sites visités les plus utilisés par les utilisateurs est tenue à jour en interne et pourra être consultée et diffusée à tout moment en interne en cas de besoin ». (...)

La Cour entend relever que, même à supposer qu'elle n'ait pas été informée de l'interdiction de jouer sur Internet sur son lieu de travail par un règlement d'ordre interne, quod non, force est cependant de constater que par sa nature, sa définition et sa finalité même, le contrat de travail entraîne l'obligation pour le salarié, qui est payé par son employeur pour ce faire, de travailler et non pas de surfer sur Internet, respectivement de jouer à des jeux communautaires sur Internet sur son lieu de travail, de sorte qu'en tentant de justifier son attitude par l'ignorance d'une interdiction patronale, la salariée est en l'espèce d'une mauvaise foi caractérisée.

Pour établir la réalité du susdit motif, l'employeur produit une série de pièces dont la salariée, qui se prévaut de l'article L- 261-1. du Code du travail précité, demande le rejet pour être illégales. (...)

Si en vertu de son pouvoir de gestion et de direction, l'employeur peut surveiller l'activité de ses salariés, tous les modes de preuve ne sont pas admissibles et notamment l'intimité de la vie privée limite les marges de manœuvre du chef d'entreprise.

Il est en effet de principe que le salarié a droit, même au temps et lieu de travail, au respect de sa vie privée qui implique en particulier le secret de la correspondance dont font partie les courriers électroniques reçus et envoyés par lui grâce à un outil informatique mis à sa disposition pour son travail et ce même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur.

Cependant, il est apparu que la formulation trop absolutiste du susdit principe pourrait ne pas laisser de place à l'atteinte licite.

Il a dès lors été décidé d'écarter de la sphère d'ingérence de l'employeur uniquement les fichiers personnels des salariés.

Partant, si les intérêts de l'entreprise l'exigent et que certaines conditions sont remplies, il doit être permis à l'employeur de porter atteinte à la vie privée de son salarié, ce d'autant plus que l'inviolabilité absolue des correspondances risque d'inciter des salariés indélicats à y loger des dossiers plus ou moins illégaux.

Il en suit, d'une part, que pour constituer une preuve illicite, le document versé aux juridictions du travail pour preuve des agissements fautifs du salarié doit porter sur des données à caractère personnel et privé du salarié, dans lequel cas l'ingérence commise par l'employeur dans la sphère privée du salarié est illégitime et disproportionnée, d'autre part, qu'il n'est pas permis à un employeur de mettre le poste de travail du salarié, à savoir toutes les applications de son ordinateur, y compris sa messagerie, sous un contrôle exclusif et régulier.

En effet, le fait d'enregistrer ces données de manière non occasionnelle et d'en déterminer le comportement du salarié est à qualifier de surveillance au sens de l'article 2 de la loi modifiée du 1er août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

Or, en l'espèce, dans la mesure où l'employeur n'a pas procédé à un contrôle des données à caractère personnel de B, il n'a en effet à aucun moment contrôlé le courrier électronique personnel et privé de sa salariée effectué sur son site de travail et plus particulièrement contrôlé sa correspondance, ses emails

personnels, ni enregistré toutes ses données de façon régulière et non occasionnelle, mais il s'est contenté d'effectuer un contrôle ponctuel en conformité avec le règlement intérieur de la société, des sites les plus visités par sa salariée, que l'article L. 261-1. du Code du travail ne trouve pas à s'appliquer.

C'est en effectuant cette vérification ponctuelle qu'il a constaté que B consultait massivement le site « Kapilhospital.com » qui est un site de jeux communautaires.

Il en suit que l'employeur ne s'est pas procuré des preuves de façon illégale, de sorte qu'il n'y a pas lieu de faire abstraction des pièces versées par l'employeur. (...)

Les pièces versées prouvent à suffisance que B a utilisé au mois de mars 2012 le site « kapilhospital.com » à raison de 51,4% de son temps de travail, soit en a fait un usage massif, plus précisément entre 9 heures et 15 heures 59, avec la considération que le site litigieux précité est un site internet de jeux communautaires.

Dès lors que la salariée, en jouant sur son ordinateur professionnel pendant les heures de travail dans une mesure qui ne peut être tolérée, a violé les obligations découlant du contrat de travail, elle a compromis, par cette attitude fautive, la confiance qui doit exister entre les parties au contrat de travail, de sorte que l'employeur était autorisé pour ce seul motif à la licencier avec préavis. »

CSJ III 12.11.2015 n° 41245 du rôle

Commentaire : Cet arrêt fournit de précieuses orientations quant aux démarches à suivre par l'employeur face à des problèmes liés à une utilisation excessive d'Internet de la part des membres du personnel. Les salariés étant payés pour travailler et non pas pour surfer sur Internet, un tel comportement peut justifier un licenciement avec préavis. L'employeur peut contrôler ponctuellement quels sites ont été visités. Il convient cependant de souligner que cet arrêt a fait l'objet de critiques par la CNPD. En effet, contrairement à la Cour d'appel qui considérait que la surveillance n'était qu'occasionnelle puisque la liste des sites Internet n'était pas consultée tous les jours, selon M. Thierry Lallemang (CNPD) « il s'agit là d'une surveillance permanente et systématique » (cf. article paru dans le Paperjam).