n° 547 | novembre 2018 32 € - Mensuel - ISSN 0014-6269

face au RISQUE

EXPLOSION À STRASBOURG

60 ANS DE REX

MARCHÉ DE LA DÉTECTION INCENDIE

10 TECHNOLOGIES QUI CHANGENT VOTRE MÉTIER

Pouvoirs d'investigation et sûreté des entreprises (2e partie)

La lutte contre les fraudes internes peut amener les employeurs à porter atteinte à la vie privée des salariés. Le cabinet Vigo fait le point sur les droits et devoirs des entreprises. Après avoir abordé, dans notre n° 546 d'octobre 2018, la gestion du personnel et le contrôle biométrique, il évoque ici l'écoute et l'enregistrement des appels téléphoniques et le contrôle des outils informatiques mis à disposition des salariés. D'autres thématiques suivront dans notre prochain numéro.

71 % des entreprises françaises interrogées indiquent avoir été victimes d'une fraude au cours des deux dernières années, contre 68 % en 2016 et 55 % en 2014, selon une étude PWC réalisée en 2018[1]. Un chiffre qui, s'il est significativement plus élevé que la moyenne mondiale (49 %), souligne la capacité des entreprises françaises à détecter les fraudes.

La lutte contre la fraude est ainsi un enjeu de plus en plus important pour les entreprises, celle-ci occasionnant des risques à la fois en termes financiers, d'activité, de gestion des données et de réputation. Ces risques, non négligeables, appellent de la part des entreprises, la mise en place de différentes mesures visant à prévenir et contrôler la fraude, et à garantir la sûreté de l'entreprise.

En 2018, selon la même étude, la cybercriminalité devient le type de fraude le plus signalé, devant le détournement d'actifs, 60 % des entreprises indiquant avoir été touchées par la cybercriminalité au cours des 24 derniers mois.

Cependant, l'employeur ne peut librement porter atteinte à la vie privée de ses salariés. Doivent alors s'équilibrer besoin de sécurité de l'entreprise et vie privée des employés dans chacune des sphères de l'entreprise.

L'employeur ne peut pas consulter librement des courriels portant la mention « Personnel » ou « Privé ».

Écoute et enregistrement des appels téléphoniques. L'entreprise peut mettre en place des dispositifs visant à procéder à l'écoute en temps réel et l'enregistrement sonore des appels téléphoniques des salariés sur leur lieu de travail, sous certaines conditions. Ces écoutes et enregistrements doivent être réalisés en cas de nécessité reconnue et doivent être proportionnés aux objectifs poursuivis, lesquels incluent la formation, l'évaluation des salariés ou l'amélioration de la qualité du service.

En revanche, la lutte contre les incivilités par exemple ne peut justifier l'enregistrement de tous les appels ; l'entreprise peut cependant opter par exemple pour un système, moins intrusif, permettant au salarié de déclencher l'enregistrement en cas de problème. En aucun cas ainsi, les écoutes et enregistrements ne peuvent être permanents ou systématiques ; ils ne peuvent pas non plus être couplés à un système de capture d'écran des postes informatiques des salariés, une telle pratique étant, elle aussi, trop intrusive.

En outre, toujours en vue d'assurer un équilibre avec le respect de la vie privée des salariés, ceux-ci et les instances représentatives du personnel doivent être informés avant toute installation d'un dispositif d'écoute ou d'enregistrement, et des périodes pendant lesquelles ils sont susceptibles d'être écoutés[2]. Les enregistrements peuvent être conservés jusqu'à six mois, et les documents d'analyses rédigés à partir de ceux-ci, jusqu'à un an.

L'entreprise peut aussi solliciter la consultation des relevés de communications téléphoniques auprès de l'opérateur, sans avertissement préalable des salariés[3]. De même, la simple vérification des relevés de la durée, du coût et des numéros des appels téléphoniques passés à partir de chaque poste, édités au moyen de l'autocommutateur téléphonique de l'entreprise, ne constitue pas en soi un procédé de surveillance illicite même si elle n'a pas été préalablement portée à la connaissance des salariés[4].

Contrôle des outils informatiques mis à disposition des salariés. Il est communément admis que les outils informatiques mis à disposition des salariés par les entreprises sont présumés avoir une utilisation uniquement professionnelle. Cependant, la question se pose de savoir dans quelle mesure, lorsque le salarié utilise les outils informatiques à des fins autres que professionnelles, l'employeur peut avoir accès à ces données.

Pour les courriels, le salarié a le droit au secret de ses correspondances personnelles. L'employeur ne pourra ainsi pas consulter librement des courriels portant la mention « Personnel » ou « Privé ». Cette

1) *PWC, « Pulling fraud out of the shadows »*, Global Economic Crime and Fraud Survey 2018

2) Cass. soc., 16 déc. 2008, n° 07-43.993

3) Cass. soc., 15 mai 2001, n° 99-42.937

4) Cass. soc., 29 janv. 2008, n° 06-45.279

protection ne vaut plus lors d'une enquête judiciaire, lorsque le juge rend une décision autorisant l'accès ou lorsque les courriels ne sont pas identifiés comme personnels. La même règle s'applique pour les fichiers sur l'ordinateur professionnel qui ont, par défaut, un caractère professionnel. S'ils sont identifiés comme étant personnels, l'employeur pourra y avoir accès soit en présence de l'employé ou après l'avoir dûment appelé, soit sans le consulter lorsqu'un risque ou un événement particulier le commande. Il appartiendra alors aux juges d'apprécier le bien-fondé de cette démarche en cas de litige. Il convient toutefois de noter que si l'employeur ne peut avoir accès à des courriels identifiés comme personnel, l'administrateur réseau, tenu d'une obligation de confidentialité, peut y avoir accès dans le cadre de sa mission de sécurité du réseau informatique[5].

Le régime des SMS *(Short Message Service)* envoyés et reçus depuis un téléphone professionnel est plus délicat. L'usage du téléphone est présumé être professionnel et l'employeur peut, à ce titre, consulter les SMS hors la présence du salarié[6] ou produire le relevé des communications devant une cour sans l'accord préalable du salarié[7]. Contrairement aux courriels, les SMS ne comportent pas d'objet, pour les identifier comme personnel. Il est donc conseillé de faire apparaître la mention « Personnel » ou « Privé » en début de texte. S'il ne peut raisonnablement être attendu des tiers qu'ils identifient de la sorte les messages adressés à un salarié (les messages reçus pourraient en effet, selon la logique, être consultés), il pourrait être imaginé, de manière plus générale, de personnaliser les contacts pour que les échanges avec les personnes désignées comme relevant de la sphère privée restent bel et bien privés[8]. Sur le même principe, la CEDH (Cour européenne des droits de l'Homme) a jugé qu'un employeur ne peut accéder au contenu de messages envoyés via une messagerie instantanée au moyen d'un logiciel espion sans avoir au préalable clairement averti le salarié de la mise en place de cette surveillance, de sa nature et de son ampleur[9].

La Cour de cassation ne s'est pas encore prononcée sur la question de savoir si l'employeur peut consulter une clé USB personnelle se trouvant sur le lieu de travail mais non connectée à un outil informatique fourni par l'entreprise.

Les mots de passe et identifiants du salarié sont eux strictement confidentiels et n'ont donc pas à être communiqués à l'employeur. Néanmoins, si l'employé possède, sur son poste, des informations indispensables à la poursuite de l'activité, l'employeur peut exiger que les codes lui soient communiqués, dans le cas où l'administrateur réseau ne peut fournir l'accès au poste.

Enfin, la Chambre sociale de la Cour de cassation a eu en 2013[10] à s'intéresser aux cas des clés USB personnelles utilisées dans le cadre professionnel. La Cour a considéré que, dès lors que la clé est connectée à un outil informatique mis à la disposition par l'entreprise pour l'exécution du contrat de travail, elle est présumée être utilisée à des fins professionnelles. L'employeur peut donc avoir accès aux fichiers non identifiés comme personnels sur cette clé, hors la présence du salarié. Une fois encore, si des fichiers sont identifiés comme personnels, l'employeur ne peut les consulter sans avoir préalablement prévenu le salarié. La Cour ne s'est en revanche pas encore prononcée sur la question de savoir si l'employeur peut consulter une clé USB personnelle qui se trouve sur le lieu de travail mais qui n'est pas connectée à un outil informatique fourni par l'entreprise. Eu égard à la jurisprudence de la Cour relative au régime de la fouille sur les lieux de l'entreprise, on peut raisonnablement penser que l'employeur ne devrait pas être autorisé à la consulter sans avoir en amont l'accord du salarié, une solution manifestement plus respectueuse des libertés du salarié.

Emmanuel Daoud, Avocat, Cabinet Vigo
Membre du réseau Gesica
Membre du Conseil de l'Ordre
Inscrit sur la liste des Conseils de la Cour pénale internationale
Marine Doisy, Élève-avocate
Philippine Viaud, Étudiante en droit

5) Cass. soc., 17 juin 2009, n° 08-40.274

6) Cass. com., 10 février 2015, n° 13-14.779

7) CA Colmar, 6 avril 2017, RG n° 15/03644

8) Ce sont toutefois des précisions sur lesquelles la Cour de cassation n'a pas eu l'occasion de se prononcer.

9) CEDH, 5 sept. 2017, Bărbulescu c. Roumanie, req. n° 61496/08

10) Cass. soc., 12 février 2013, FS-P+B, n° 11-28.649

À noter

- Notre prochain numéro abordera la charte informatique, la géolocalisation et la vidéosurveillance.
- Cet article a été rédigé en août 2018 et tient compte de la jurisprudence jusqu'à cette date.

Face au Risque évolue, découvrez nos nouvelles formules !

SITE WEB — En continu
NEWSLETTER — Chaque semaine
MAGAZINE — Chaque mois

www.faceaurisque.com

face au RISQUE

+ d'actus riches et pertinentes
+ de retours d'expérience illustrés
+ de suivi de textes réglementaires
+ de contenus adaptés à vos besoins