n° 548 | décembre 2018 – janvier 2019 32 € – Mensuel – ISSN 0014-6269

face au RISQUE

INCENDIE MONSTRE DE PNEUS

RGPD, 6 MOIS DÉJÀ

TOUT SUR LE RESPONSABLE SÉCURITÉ

PROTÉGER LA DONNÉE

Pouvoirs d'investigation et sûreté des entreprises (3e partie)

Lutter contre les fraudes internes peut parfois amener les employeurs à porter atteinte à la vie privée des salariés. Le cabinet Vigo fait à ce sujet le point sur les droits et les devoirs des entreprises. Après avoir abordé, dans notre n° 546 d'octobre 2018, la gestion du personnel et le contrôle biométrique, puis dans notre n° 547, l'écoute et l'enregistrement des appels téléphoniques et le contrôle des outils informatiques mis à disposition des salariés, voyons ici la charte informatique, la géolocalisation et la vidéosurveillance.

L'investissement dans la lutte contre la fraude est un enjeu de plus en plus important pour les entreprises, celle-ci occasionnant des risques à la fois en termes financier, 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 une étude PWC[1], la cybercriminalité devient le type de fraude le plus signalé, devant le détournement d'actifs : 60 % des entreprises indiquent avoir été touchées par la cybercriminalité au cours des 24 derniers mois.

Si l'entreprise possède une grande liberté pour lutter contre ces fraudes, l'employeur ne peut pour autant 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.

Charte informatique. La réalisation d'une charte informatique ne constitue pas pour l'entreprise une obligation légale. En revanche, elle est conseillée par la Cnil dès lors qu'elle apporte un éclairage aux salariés s'agissant de leurs droits et obligations dans l'utilisation des outils que l'entreprise met à leur disposition. Elle constitue un instrument de sécurisation pour l'entreprise dès lors que les modalités d'utilisation des outils informatiques qui y sont précisées sont opposables au salarié. Toutefois, elle n'est opposable que si elle est annexée au règlement intérieur – ou au contrat de travail du salarié – et qu'il est démontré qu'elle a été portée à la connaissance du salarié[2].

Dans les entreprises, les caméras ne peuvent être installées que dans des endroits particuliers (couloirs, entrées et sorties) et dans un objectif précis (sécurité, dissuasion, identification des auteurs d'infractions).

71 %

des entreprises françaises indiquent avoir été victimes d'une fraude au cours des deux dernières années, contre 68 % en 2016 et 55 % en 2014, selon PWC.

La vidéosurveillance. L'utilisation de dispositifs de vidéosurveillance est de plus en plus fréquente au sein des entreprises. De tels dispositifs sont eux aussi strictement encadrés. Des caméras ne peuvent être installées que dans des endroits particuliers (couloirs, entrées et sorties) et dans un objectif précis (sécurité, dissuasion, identification des auteurs d'infractions, etc.). Elles ne peuvent en revanche filmer les salariés sur leurs lieux de pause, les toilettes, ou les locaux syndicaux. Elles ne peuvent pas non plus, sauf circonstances particulières[3], les filmer sur leur poste de travail.

En outre, seules les personnes qui y sont habilitées peuvent consulter les images de vidéosurveillance, dans le cadre de leurs fonctions, et les images ne peuvent être enregistrées que pour une durée liée à l'objectif de l'enregistrement (quelques jours peuvent suffire).

Le dispositif de vidéosurveillance doit être inscrit dans le registre des

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

2) CA Douai, 30 novembre 2011, RG n° 10/02459.

3) Le cas par exemple des employés manipulant de l'argent, qu'une caméra peut filmer mais celle-ci doit davantage filmer la caisse que le caissier ; ou le cas d'entrepôts où sont stockées des marchandises de valeur et au sein duquel travaillent des manutentionnaires.

traitements de données tenu par l'employeur, lequel doit pouvoir être transmis sur demande à la Cnil[4]. Et, si les caméras filment un lieu ouvert au public, le dispositif doit être autorisé par le préfet du département.
Les instances représentatives du personnel doivent être consultées et informées avant toute décision d'installation ; les salariés doivent eux aussi être informés de tout moyen de contrôle de leur activité[5], et ce y compris lorsque le système de surveillance en cause est installé au sein d'une société cliente[6].
Ce n'est que lorsque la surveillance a lieu dans un endroit où les salariés ne travaillent pas qu'il a pu être jugé que leur information préalable n'était pas nécessaire[7].

Géolocalisation. L'entreprise peut installer des dispositifs de géolocalisation dans les véhicules utilisés par des employés, dans des buts très précis, incluant notamment les actions suivantes :
– suivre, justifier et facturer une prestation de transport ;
– assurer la sécurité de l'employé et des marchandises dont il a la charge ;
– contrôler le respect des règles d'utilisation du véhicule fixées par l'employeur ;
– ou à titre accessoire, suivre le temps de travail, lorsque cela ne peut être réalisé par un autre moyen.
En revanche, la géolocalisation ne peut servir à contrôler en permanence ou en dehors du temps de travail un salarié. Ces derniers doivent dans tous les cas être tenus informés de l'installation d'un tel dispositif, doivent avoir accès aux données les concernant qui sont enregistrées[8], et doivent pouvoir désactiver la collecte ou transmission de la localisation en dehors de leur temps de travail. La géolocalisation ne peut ainsi être utilisée que pour les finalités qui ont été portées à la connaissance du salarié[9].
Seules les personnes habilitées doivent pouvoir accéder aux données collectées dans le cadre de la géolocalisation. Ces données ne peuvent être conservées plus de deux mois, à moins que leur collecte soit réalisée à des fins d'optimisation des tournées (1 an) ou pour le suivi du temps de travail (5 ans).
Comme tout traitement de données, le dispositif de géolocalisation doit être inscrit dans le registre des activités de traitement tenu par l'employeur, dans le cadre des dispositions du RGDP.

Les dispositifs d'investigation à disposition des entreprises (et donc, des employeurs) sont ainsi nombreux. Ils sont strictement encadrés en vue de garantir un équilibre avec le droit à la vie privée des salariés.
Il est ainsi recommandé aux entreprises pour lesquelles cette désignation n'est pas obligatoire[10], de nommer malgré tout un délégué à la protection des données (DPO), qui sera associé à la mise en œuvre de ces diverses mesures d'investigation. Chargé d'informer et de conseiller le responsable de traitement ou le sous-traitant et leurs employés, de contrôler le respect du droit en matière de protection des données et de coopérer avec l'autorité de contrôle, il permettra à l'entreprise de garantir au mieux la conformité de ses investigations aux règles qui les encadrent.

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

4) Antérieurement à l'entrée en vigueur du RGPD, une déclaration à la Cnil de toute installation d'un dispositif de surveillance des salariés était indispensable, sous peine d'illicéité des preuves issues de ce système de traitement automatisé de données personnelles (Cass. soc., 8 octobre 2014, n° 13-14.991) ou de condamnation pour omission de déclaration (Cass. soc., 9 juillet 2016, n° 14-87.753).

5) Cass. soc., 20 novembre 1991, n° 88-43.120.

6) Cass. soc., 12 janvier 2012, n° 10-23.482.

7) Cass. soc., 31 janvier 2001, n° 98-44.290 ; Cass. soc., 19 avril 2005, n° 02-46.295.

8) La Cnil a pu imposer une sanction de 10 000 € à l'employeur qui refusait de fournir à un salarié qui la sollicitait, la copie de ses données.

9) Cass. soc., 3 nov. 2011, n° 10-18.036.

10) La désignation d'un DPO est obligatoire, sur le fondement du RGPD, pour les autorités ou les organismes publics, les organismes dont les activités de base les amènent à réaliser un suivi régulier et systématique des personnes à grande échelle, et les organismes dont les activités de base les amènent à traiter à grande échelle des données dites « sensibles » ou relatives à des condamnations pénales et infractions.

À noter

• Cet article a été rédigé en août 2018 et tient compte de la jurisprudence jusqu'à cette date.

La clause de dédit-formation

En contrepartie d'une formation assurée par l'employeur, la clause de dédit-formation oblige le salarié à rester à son service pendant une certaine durée et à lui verser, en cas de démission anticipée, une indemnité correspondant aux frais de formation engagés.

Un salarié avait mis fin à son contrat de travail en cours de période d'essai. L'employeur lui avait remis un reçu pour solde de tout compte faisant état d'un solde négatif car il avait retenu des sommes correspondant à l'indemnité de dédit prévue par son contrat de travail. Contestant ce solde, le salarié a alors saisi jusqu'à la cour d'appel qui a retenu que la clause de dédit-formation :
– ne précisait pas la date, la nature et la durée des formations concernées ;
– a été conclue sur la base d'une évaluation forfaitaire et non du coût réel de la formation pour l'employeur, coût dont il n'était pas justifié, et dont les modalités de paiement n'avait pas été prévues.
La clause a été jugée non valable et déclarée nulle.

Les critères de validité d'une clause de dédit-formation ont été fixés par la Cour de cassation.
La clause doit en effet :
– viser des frais de formation supérieurs à ceux prévus par la loi ou la convention collective ;
– ne pas rendre impossible toute démission du salarié (en ne prévoyant pas des coûts de formation excessifs ou une durée d'application trop longue) ;
– prévoir une indemnité de dédit proportionnée aux frais de formation (l'indemnité doit correspondre aux frais réels de formation engagés par l'employeur, et non à une évaluation forfaitaire) ;
– donner lieu à la conclusion d'une convention écrite conclue avant le début de la formation et précisant la date, la nature, la durée de la formation et son coût réel pour l'employeur, ainsi que le montant et les modalités du remboursement à la charge du salarié.
La clause qui ne remplit pas ces critères est nulle, et donc inopposable au salarié.

Cour d'appel d'Aix-en-Provence, 18 mai 2018, n° 17/01153

Émilie Meridjen
Associée du cabinet Sekri Valentin Zerrouk