n° 546 | octobre 2018 | 32 € Mensuel – ISSN 0014-6269

face au RISQUE

INCENDIE À EUROPA-PARK

LES POUVOIRS DU RESPONSABLE DE SÉCURITÉ

LE MARCHÉ DE LA TÉLÉSURVEILLANCE

ÉVITER LE RADICALISME

Pouvoirs d'investigation et sûreté des entreprises (1re partie)

La lutte contre les fraudes internes peut parfois amener les employeurs à porter atteinte à la vie privée des salariés, comme le montre l'abondante jurisprudence en la matière. Le cabinet Vigo fait le point sur les droits et devoirs des entreprises concernant la gestion du personnel et le contrôle d'accès biométrique. D'autres thématiques seront abordées dans nos prochains numéros.

Une étude réalisée en 2018 révèle que 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. Un chiffre qui, s'il est significativement plus élevé que la moyenne mondiale (49 %), souligne la capacité des entreprises françaises à détecter les fraudes[1].

L'investissement dans 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 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.

Et si diverses mesures de sûreté ont déjà pu être mises en place dans l'entreprise, elles auront vocation à évoluer et s'adapter au développement de nouveaux types de fraude. 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.

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.

Recrutement et gestion du personnel. Lors du recrutement, l'employeur est amené à collecter un certain nombre de données personnelles sur le candidat. Se pose alors la question de leur gestion. Ces données ne doivent servir qu'à évaluer la capacité du candidat pour le poste proposé. L'employeur ne peut donc valablement pas demander le numéro de sécurité sociale du candidat ni même des informations sur ses proches, ses opinions politiques ou syndicales. Il est en revanche en mesure de collecter des données qui peuvent se révéler utiles à la gestion administrative du personnel, à l'organisation du travail ou encore à l'action sociale. Les données collectées ne sont accessibles qu'aux personnes intervenant dans le processus de recrutement.

Dans tous les cas, le candidat et l'employé doivent être préalablement informés de l'utilisation de techniques d'aide au recrutement ou de fichiers de gestion du personnel. Ils possèdent également tous deux un droit d'accès sur les données qui les concernent.

60 % des entreprises françaises déclarent avoir été touchées par la cybercrininalité au cours des 24 derniers mois[1].

Dans le cas d'une issue négative du processus de recrutement, l'employeur ne peut garder les informations relatives aux candidats que pendant deux ans maximum. Au-delà de cette durée en effet, même en l'absence de demande de destruction, il doit en informer la personne intéressée.

En outre, s'agissant de la gestion du personnel, seules les personnes chargées de cette gestion ont un accès aux informations concernant les salariés. Les employés peuvent en outre avoir accès aux commentaires faits par l'employeur à leur égard, ces commentaires devant toujours être pertinents et non excessifs. Il convient de noter toutefois que les valeurs de classement annuel ou de potentiel de carrière n'ont pas à être communiquées lorsqu'elles sont encore prévisionnelles et ne peuvent donc l'être que lorsqu'elles ont été utilisées pour prendre une décision.

Contrôle d'accès biométrique. Bien des entreprises ont aujourd'hui recours aux technologies biométriques pour contrôler l'accès aux locaux, qu'ils fassent l'objet d'une restriction de circulation ou non. De par leur nature personnelle et unique, la collecte et l'utilisation des données biométriques d'une personne, c'est-à-dire les *« caractéristiques physiques, physiologiques ou comportementales d'une personne physique »*[2], doivent être rigoureusement encadrées. L'article 9 du RGPD interdit en effet le traitement de *« données biométriques aux fins d'identifier une personne physique de manière unique »*, sauf lorsque l'une des situations précisées par le second paragraphe dudit article est caractérisée.

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

2) *Article 4 du Règlement général sur la protection des données (RGPD)*

En ce sens, l'entreprise doit assurer le respect de la vie privée de ses employés. À ce titre, l'employeur se doit de réaliser une analyse d'impact sur la protection des données (PIA) du contrôle d'accès biométrique afin d'identifier les risques posés et, le cas échéant, les réduire. Par ailleurs, l'accès aux données biométriques est strictement réservé aux membres qui y sont habilités par leurs fonctions et l'employeur doit mettre en place des mesures empêchant les personnes non habilitées d'avoir accès auxdites données. Les données relatives aux accès doivent en outre être supprimées trois mois après leur enregistrement et celles qui sont utilisées pour le suivi du temps de travail ne peuvent être conservées au-delà de cinq ans.

Les règles concernant l'information de la collecte sont, elles, plus souples. En effet, la Cour de cassation a récemment considéré qu'une information globale, via un intranet auquel tous les salariés ont accès, annonçant la collecte de leurs données personnelles était légale et conforme à l'obligation de loyauté, l'information individuelle de chacun des employés concernés n'étant donc pas nécessaire[3]. Cette information est conforme, à la condition cependant que les personnes concernées aient un accès effectif à l'information et possèdent un droit de rectification sur les informations en question – une solution déjà introduite par la CJUE (Cour de justice de l'Union européenne) en 2011[4].

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

3) Cass. soc., 13 juin 2018, n° 16-25.301
4) CJUE, 5 mai 2011, aff. C-543/09

À noter

- Nos prochains numéros aborderont les sujets suivants : écoute et enregistrement des appels téléphoniques, contrôle des outils informatiques mis à disposition des salariés, charte informatique, vidéosurveillance et géolocalisation.
- Cet article a été rédigé en août 2018 et tient compte de la jurisprudence jusqu'à cette date.

Grève sur un site Seveso et respect des impératifs de sécurité

Deux récents cas de jurisprudence illustrent les difficultés à concilier l'exercice du droit de grève sur un site Seveso et le maintien de l'activité de l'entreprise dans des conditions de sécurité suffisantes pour les travailleurs.

En pareilles circonstances, la tentation est grande pour l'employeur, au regard de son obligation de sécurité, de prévenir tout risque en procédant tout bonnement au « lock-out » de l'entreprise, c'est-à-dire à la fermeture temporaire du site, entraînant la suspension de l'exécution des contrats de travail de l'ensemble du personnel, gréviste comme non-gréviste. Mais à quelles conditions le peut-il selon la jurisprudence ?

Fermeture temporaire d'une usine.

Dans un premier arrêt *(Soc., 18 janvier 2017, n° 15-23986 à 15-23995)*, à la suite de l'échec de négociations salariales, une grève avait débuté sur un site de production de substances chimiques Seveso « seuil haut » de la société Rhodia.

En raison des contraintes et des risques générés par les débrayages successifs des grévistes, l'employeur avait pris la décision, à l'issue d'une réunion extraordinaire du comité d'établissement, de procéder à la fermeture temporaire de l'intégralité des installations de l'usine.

Les grévistes avaient demandé en référé l'allocation de dommages-intérêts pour compenser les pertes de salaires et pour atteinte au droit de grève.

Confirmant les ordonnances du Conseil de Prud'hommes, la Cour de cassation a rejeté les demandes des salariés et reconnu la situation contraignante en termes de sécurité obligeant l'employeur à arrêter la production. Elle relève en particulier que *« la succession d'arrêts et de redémarrages des installations avait pour effet, pour le premier atelier HQPC de ne plus permettre de maîtriser la composition des goudrons et la température nécessaire à la fluidité des produits générant des bouchages et des opérations à haut risque, pour le deuxième atelier Vanilline d'encrasser des installations et de créer un risque de bouchages de la tuyauterie imposant des opérations exposant à un risque de brûlure et pour le dernier atelier DPHE d'entraîner une consommation de plus de 20 tonnes d'éther en deux jours au lieu de 3 tonnes/semaine en temps normal ainsi qu'une importante fuite de ce produit se répandant jusqu'à l'extérieur de l'entreprise et que ces dysfonctionnements qui ne relevaient pas de phénomènes habituels dans le cadre du fonctionnement normal des ateliers étaient d'une particulière dangerosité amplifiant de manière conséquente les risques pour les salariés et les installations »*.

> Le tribunal a considéré que la grève ne constitue ni un trouble manifestement excessif, ni un risque de dommage imminent.

Le juge refuse la fermeture d'un établissement.

Dans un récent jugement *(TGI Grenoble, 5 juillet 2018, n° RG 18/00696)*, le juge des référés a au contraire refusé d'autoriser la fermeture d'un établissement Seveso seuil haut de traitement thermique de déchets spéciaux liquides dans lequel certains salariés, contestant le nouvel accord d'intéressement, s'étaient mis en grève à raison de débrayages ponctuel devenus, au fil du temps, quotidiens.

Pour décider que la grève pouvait se poursuivre au regard des conditions de sécurité, le juge relève en premier lieu que *« les modalités d'exercice de la grève avec une permanence de personnels pour assurer le fonctionnement des incinérateurs et éviter des baisses de températures des fours, selon les directives de la direction, permet d'assurer la sécurité du site et des personnels »*.

Il rappelle également que la maintenance des installations est assurée en continu. Enfin, la société Suez Iws Chemicals France est en mesure, depuis trois mois que dure la grève, de prendre les dispositions pour limiter les arrivées de produits à incinérer à hauteur des capacités actuelles de brûlage et l'établissement et ses clients ont la possibilité de se tourner vers d'autres sites d'incinération sur le sol français et en Europe.

Ces constats conduisent le tribunal à considérer que la grève, telle qu'elle s'exerce dans l'usine, ne constitue ni un trouble manifestement excessif, ni un risque de dommage imminent.

Morgane Darmon
CNPP, service Assistance réglementaire