Les pouvoirs d'investigation du responsable sûreté

À l'instar des personnes physiques, les entreprises peuvent être victimes d'agissements délictueux voire criminels de la part de personnes extérieures, comme de leurs salariés. Selon une étude PwC, 55 % des entreprises françaises ont déjà fait l'objet de tentatives de fraude.

Maksim/Fotolia.com

▲ Les données biométriques ne doivent être accessibles qu'à des personnes habilitées.

Victime désormais privilégiée, l'entreprise doit se prémunir contre les risques identifiables et ceux non encore identifiés en adoptant des règles de sécurité strictes et en prévoyant des mesures dites d'investigations.
À cette fin, de nombreuses entreprises décident d'investir dans le recrutement d'un directeur sûreté dont le travail consiste à évaluer les risques propres à l'entreprise et à mettre en place un système de prévention et, éventuellement, un processus d'investigations face à une attaque.
Toutefois, l'entreprise n'a pas carte blanche en matière d'investigation. L'équilibre doit être trouvé entre le besoin de sécurité de l'entreprise et le respect de la vie privée des salariés. Le cas échéant, elle pourrait s'exposer à des poursuites civiles (article 9 du code civil) et pénales (article 226-1 du code pénal).
À titre d'illustration, en 2013 la société Euro Disney a fait l'objet d'une condamnation pénale pour avoir, avec l'aide de sociétés de renseignements privés, récolté illégalement des informations puisées dans les fichiers de police sur des candidats à l'embauche et des salariés en

Mikhaylenzhan/Fotolia.com

PEUT-ON PLACER DES CAMÉRAS DE VIDÉOSURVEILLANCE DANS UNE ENTREPRISE ?

À des fins de dissuasion de vols, de dégradations, d'agressions et, de manière générale, de sécurisation, les entreprises ont recours de façon croissante à la vidéosurveillance. Ce dispositif est néanmoins très encadré car potentiellement attentatoire à la vie privée des salariés.
Ainsi, le choix de l'emplacement des caméras de vidéosurveillances est restreint : les entrées et sorties du bâtiment, les issues de secours, les couloirs et les zones de marchandises peuvent être filmés. Toutefois, il est interdit car disproportionné, de filmer les salariés à leur poste de travail, dans les toilettes ou dans les endroits dédiés à la détente tels que la cafétéria.
Quant à la conservation des images recueillies, elle ne peut excéder un mois, sauf en cas d'incident déclenchant une procédure disciplinaire ou pénale. Dans ce cas, les images pourront être conservées le temps de la procédure.

Les formalités

Le système de vidéosurveillance implique également l'accomplissement de plusieurs formalités par l'entreprise.
Tout d'abord, l'installation d'un dispositif de vidéosurveillance doit être soumise à l'information et à la consultation des instances représentatives du personnel de l'entreprise.
Ensuite, l'existence du dispositif de vidéosurveillance doit faire l'objet d'un affichage visible dans les locaux et doit être porté à la connaissance de chaque salarié (via une note de service par exemple).
Enfin, l'entreprise doit déclarer le système de vidéosurveillance envisagé auprès de la Cnil, sous peine de ne pas pouvoir opposer les images collectées aux salariés en cas de procédure disciplinaire ou pénale.

période d'essai. La société avait justifié à l'époque avoir eu recours à ce type de consultation dans le souci d'assurer la sécurité du parc mais aussi et surtout des enfants.
Les possibilités d'investigations pouvant être mises en œuvre par l'entreprise sont donc très encadrées. Des mesures dites de « sûreté » existent telles que le contrôle biométrique de l'accès aux locaux, l'écoute et l'enregistrement des appels téléphoniques et le contrôle des outils informatiques mis à disposition des salariés.
Il convient de préciser dès maintenant que toutes les mesures d'investigations ci-après décrites, doivent préalablement à leur mise en place, faire l'objet d'une information et d'une consultation de la part des instances représentatives du personnel ainsi que d'une déclaration, voire d'une demande d'autorisation, auprès des services de la Commission nationale de l'informatique et des libertés (Cnil).

Le contrôle d'accès biométrique

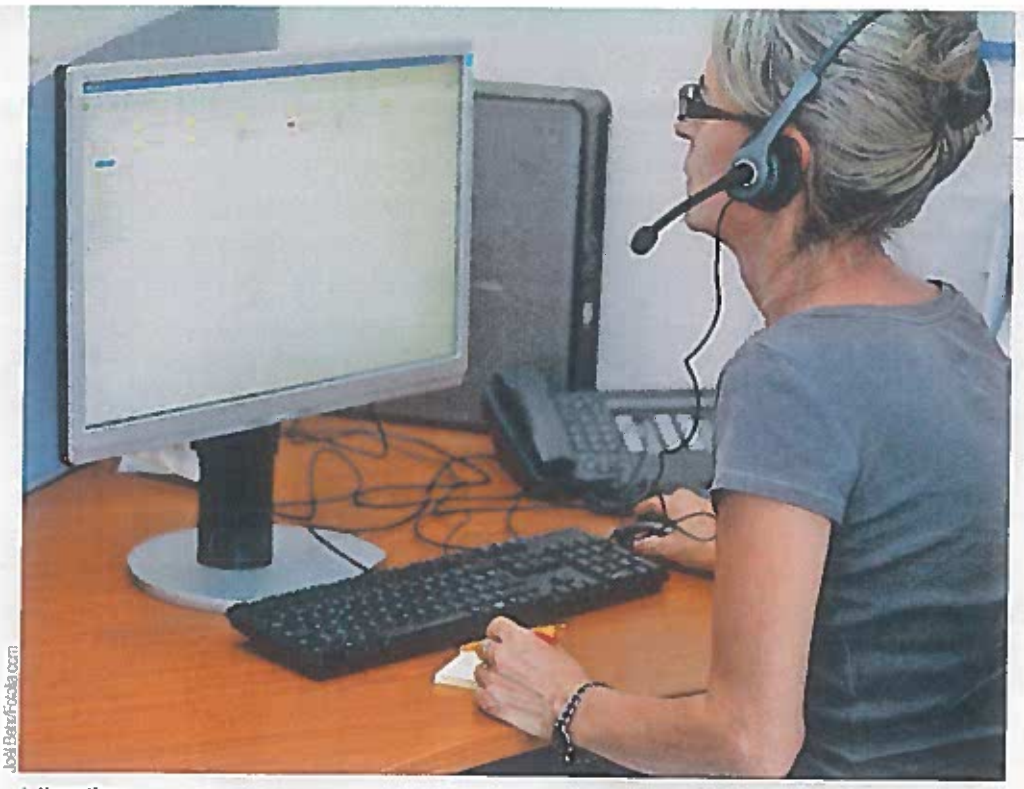
Les contrôles d'accès aux locaux de l'entreprise existent depuis longtemps. Cependant avec l'essor des technologies biométriques, les entreprises ont aujourd'hui les moyens de mettre en place un contrôle bien plus précis et personnalisé, sans que cela ne nécessite d'importantes ressources financières.
Ainsi, il est désormais possible de contrôler l'accès aux locaux grâce à la reconnaissance du contour de la main, de l'empreinte digitale ou encore par reconnaissance du réseau veineux des doigts de la main.
Toutefois, la récolte de données biométriques (informations liées aux caractéristiques comportementales et physiologiques d'une personne) est encadrée en raison de l'impact potentiellement important sur la vie privée des personnes concernées. Par conséquent, les informations récoltées ne doivent être accessibles qu'à des personnes habilitées, gérant la sécurité de l'entreprise, et doivent être supprimées trois mois après leur enregistrement.

L'écoute et l'enregistrement des appels téléphoniques

L'entreprise peut, sous certaines conditions, mettre en place un dispositif d'écoute et d'enregistrement des conversations téléphoniques de ses salariés sur leur lieu de travail.
Seulement, la durée de conservation des enregistrements téléphoniques ne peut excéder six mois.
Il convient de préciser que ce système de surveillance est cantonné à des fins de formation et d'évaluation des employés, ainsi que d'amélioration de la qualité du service. En effet, il est pour l'instant interdit d'installer un dispositif d'écoute et d'enregistrement permanent des salariés. Autrement dit, le salarié ne peut pas faire l'objet de surveillance systématique, y compris à des fins probatoires.
Néanmoins, si à l'occasion d'écoutes « surprise », des griefs ressortent des comptes rendus d'écoutes téléphoniques à l'encontre d'un salarié, ils peuvent être utilisés comme moyen de preuve lors d'une procédure disciplinaire ou judiciaire le visant.
Par ailleurs, l'entreprise a la faculté de vérifier le relevé des communications téléphoniques fourni par l'opérateur, sans que cela ne constitue un procédé de surveillance illicite. De même, sous réserve d'une déclaration à la Cnil, l'entreprise peut vérifier les relevés des appels passés à partir du poste de chaque salarié, édité au moyen d'un autocommutateur.

Le contrôle des outils informatiques mis à disposition des salariés

La plupart des risques ou menaces proviennent ou passent de manière croissante, par le biais du système informatique de l'entreprise : cyberattaques, fraude au président, vol de données informatiques.
Il est donc indispensable que l'entreprise contrôle l'utilisation par ses salariés des outils mis à leur disposition pour l'exécution de leur travail, sans préjudice des actions de formation à leur attention.
À titre d'illustration, l'entreprise peut surveiller l'utilisation



Joël Barraclough.com

▲ Un système d'écoute et d'enregistrement des conversations téléphoniques peut être mis en place pour une période de 6 mois maximum à des fins de formation et d'évaluation des employés.

d'Internet par son salarié du fait que « *les connexions établies par un salarié sur des sites Internet pendant son temps de travail [...] sont présumées avoir un caractère professionnel de sorte que l'employeur peut les rechercher aux fins de les identifier, hors de sa présence* » (Cour de cassation, chambre sociale, arrêt du 9 juillet 2008 n° 06-45800). L'entreprise a également la possibilité de limiter l'utilisation d'Internet à l'aide de dispositifs de filtrage de sites ou de détection de virus.

Quant à la messagerie professionnelle du salarié, il convient de préciser que les courriels ont par défaut un caractère professionnel. De ce fait, l'entreprise peut en prendre connaissance librement y compris en dehors de la présence du salarié.

En revanche, un courriel identifié comme étant personnel par le salarié est protégé, de sorte que l'entreprise ne peut pas le consulter de façon discrétionnaire. Toutefois cette protection au bénéfice de celui-ci disparaît si l'entreprise obtient une ordonnance du juge en vue de la désignation d'un huissier de justice, qui prendra alors connaissance des messages personnels du salarié.

Le contrôle par l'entreprise de l'utilisation des moyens informatiques peut être opportunément décrit dans une charte informatique.

L'élaboration d'une telle charte ne constitue pas une obligation légale mais est très fortement recommandée car elle représente un instrument de sécurisation, de sensibilisation et de responsabilisation des utilisateurs. Elle permet d'encadrer l'utilisation par les salariés du matériel informatique mis à leur disposition (ordinateur, messagerie électronique, Internet, intranet etc.), en établissant des règles d'utilisation, en définissant les modalités de contrôle par l'employeur et en informant les salariés sur leurs droits et obligations.

Surtout, la seule annonce de la mise en place d'un système réglementé et contrôlé permet, dans une certaine mesure, de réduire sensiblement les risques existants.

Si la charte figure dans le règlement intérieur de l'entreprise, elle sera opposable aux salariés et le non-respect des dispositions prévues au sein de la charte informatique pourra être, par conséquent, sanctionné disciplinairement.

En somme, de nombreuses mesures d'investigations « sûreté » peuvent être mises en place par l'entreprise mais celle-ci doit faire usage de prudence et de proportion, tout en ne perdant pas de vue les formalités obligatoires dont l'entreprise doit s'acquitter pour se protéger et protéger ses salariés. ■

Rebecca Nahon
Emmanuel Daoud
Avocats – Cabinet Vigo