

Option DROIT & AFFAIRES

L'ÉVÉNEMENT

DLA Piper accueille une spécialiste en données personnelles

L'entrée en vigueur en 2018 du nouveau règlement européen sur la protection des données pousse les cabinets à étoffer leurs équipes IP/IT. Avant l'été, McDermott Will & Emery avait ainsi annoncé la création d'un département Protection des données (ODA 360).

Cette fois, c'est DLA Piper qui renforce ses équipes avec l'arrivée d'une nouvelle associée en la personne de Denise Lebeau-Marianna. Aux côtés de Jonathan Rofé, responsable du département Propriété intellectuelle et Technologie du bureau parisien, cette ancienne de Baker Mckenzie, où elle a exercé pendant plus de vingt ans, apporte son expertise en matière de protection des données personnelles. Intervenant sur de nombreux secteurs, dont la grande distribution, le luxe, l'aéronautique, la défense ou encore la santé, elle accompagne les entreprises dans leurs démarches de mise en conformité, tant en matière de traitement des données que de lutte contre la corruption, le blanchiment et le financement du terrorisme.

Exerçant à la fois en conseil, en précontentieux et contentieux,

elle intervient également dans le cadre de projets big data, d'intelligence artificielle ainsi que sur les sujets liés à l'Internet des objets. «Je suis ravie de rejoindre DLA Piper qui bénéficie d'équipes très

intégrées tant au niveau national, qu'international avec de fortes interactions entre les départements et les différents bureaux. Cette organisation permet de fournir à nos clients la meilleure expertise d'un véritable cabinet international et contribue ainsi à mieux développer la clientèle», souligne la nouvelle associée.

Titulaire d'un master international en droit privé et droit des affaires (université Panthéon-Assas, 1989), Denise Lebeau-Marianna est également diplômée de l'Essec (1991) et d'un master en droit des technologies de l'information et de la communication (université Paris XI, 1993). Arrivée chez Baker Mckenzie en 1994, elle s'est progressivement spécialisée en protection des données personnelles

et a ainsi été à l'origine de la création de la pratique au sein du bureau parisien. Nommée associée en 2016, elle est par ailleurs expert agréé EuroPriSe en données personnelles. ■ Coralie Bach



Photo : Studio Falour

Denise Lebeau-Marianna

AU SOMMAIRE

Communauté

Carnet

Avocats et legaltech : de la méfiance à la collaboration

p.2

p.3

Affaires

IPO : Près de 1,8 milliard d'euros levés sur la Place de Paris Deals

p.4

p.5-7

Analyses

Simplification de la procédure d'appel pour une meilleure efficacité

p.8-9

La radicalisation en entreprise

p.10-11

RESPONSABILITÉ DE L'ENTREPRISE

La radicalisation en entreprise

Prosélytisme et revendications communautaristes, comportements ambigus de salariés qui ont accès à des installations ou des informations stratégiques... A l'Uclat (Unité de coordination de la lutte antiterroriste), le constat est édifiant. L'islamisme radical impacte aujourd'hui de plus en plus d'entreprises, toutes tailles confondues, dans tous les secteurs d'activité.



Par Thibault de Montbrial, associé,

Et toujours, les mêmes questions se posent : quelle est la marge de manœuvre de l'entreprise ? quelle frontière entre une pratique religieuse ostensible et une radicalisation nuisible ou dangereuse ?

En apparence, le vide est abyssal : les entreprises se sentent démunies, entre inaction fautive et réaction excessive, et craignent de se mettre en infraction avec la loi. Les fédérations patronales croulent sous les demandes, sans trop savoir comment conseiller. Les pouvoirs publics n'ont pas de réponses adaptées aux opérateurs privés. Ils renvoient au numéro vert dédié (0800 005 696) et/ou au formulaire de signalement du site du ministère de l'Intérieur et incitent en «off» à la plus grande vigilance.

En réalité, la situation n'est juridiquement pas si complexe et les réponses opérationnelles, variées. Si, malgré les décisions rendues en 2017 par la CJUE (Cour de justice de l'Union européenne), le droit ne donne pas de réponse magique, force est de constater que, bien maniée, la boîte à outils recèle de trésors cachés...

Le principe de précaution commande aux entreprises d'intégrer une obligation de vigilance et un principe de neutralité religieuse pour anticiper ces risques d'un nouveau genre.

Les risques pour l'entreprise

D'abord, le risque psychosocial. Le vivre ensemble professionnel est impacté, avec son lot de tensions accumulées, de prosélytisme et de risque de contamination. L'ambiance au travail s'en trouve dégradée, le travail désorganisé et les managers dépassés.

Ensuite, le risque sécuritaire. La sécurité des personnes est dans tous les esprits, à défaut d'être verbalisée. La sécurité des installations technologiques aussi. La sécurité économique, enfin, avec la crainte de voir des informations stratégiques (savoir-faire, fichier clients) passer entre de mauvaises mains et utilisées à des fins détournées voire dangereuses. S'y ajoutent les risques juridiques en droit du travail et droit civil : quelles réponses apporter aux reven-

dications communautaristes ? Comment protéger les femmes de l'entreprise, victimes de misogynie ? D'un côté, le risque de mesures disciplinaires infondées ou abusives avec les sanctions prud'homales ; de l'autre, la responsabilité civile de l'employeur du fait de ses préposés et/ou pour manquement à son obligation de santé et sécurité.

Le risque pénal complète cet état des lieux : entre la possibilité d'être victime, la crainte de passer pour le bourreau et le risque de complicité passive, les entreprises ignorent comment réagir. Le panel de qualifications pénales est large : harcèlement moral, discrimination, délit non intentionnel, etc.

Pire, le risque commercial et réputationnel : mécontentement des clients, des partenaires, médiatisation des dérives, syndicalisme toxique, etc.

Les hypothèses ne sont plus d'école et les risques pesant sur l'entreprise sont, eux, bien réels.

Vers une obligation de vigilance

Au-delà du principe élémentaire de précaution, les signaux juridiques convergent dans le sens d'une obligation de vigilance de l'entreprise.

L'ordonnance du 7 avril 2016 étend la pénalisation du manquement à l'obligation de santé et de sécurité de l'employeur.

La loi Sapin 2 impose aux entreprises de mettre en place un dispositif de traitement des signalements des lanceurs d'alerte, susceptibles de porter sur toute menace et/ou comportement pénalement répréhensible.

La loi Vigilance contraint les très grandes entreprises à un devoir général de vigilance en matière de santé et de sécurité des personnes.

Enfin, les juges ont une interprétation de plus en plus extensive des délits non intentionnels (atteinte involontaire et risque causé à autrui) pour négligence, c'est-à-dire défaut de vigilance.

Notre conviction est que la question n'est plus de savoir si le juge sanctionnera, mais quand et comment les entreprises seront sanctionnées pour manquement à leur devoir de vigilance.

La boîte à outils : une adaptation pragmatique du logiciel et des outils existants

Le point névralgique du raisonnement tient dans l'évaluation et l'anticipation globale des risques de l'entreprise : juridique, financier, psychosocial, structurel, dangerosité, intérêts stratégiques à protéger, etc.

Les entreprises sont loin d'être démunies. Il leur suffit simplement d'adapter leur logiciel avec pragmatisme et de croiser les compétences et outils existants.

Comment ? En sensibilisant les managers au repérage des comportements à risque et leur hiérarchisation. L'Uclat a réalisé une grille d'indices et hiérarchisé les comportements à risque.

Changer le logiciel, c'est d'abord intégrer le risque à la veille quotidienne.

C'est aussi utiliser autrement les outils à disposition. Ainsi les méthodes de veille stratégique développées par l'intelligence économique et les dispositifs de contrôle contraignants des lois Sapin 2 et Vigilance peuvent-ils s'avérer pertinents, pour peu qu'ils soient bien combinés et transposés à l'objectif poursuivi.

Une fois la cartographie des risques établie, l'entreprise peut arbitrer et décider. En toute logique, son choix se portera sur le meilleur rapport risque au regard de la protection de ses intérêts stratégiques et sa valorisation financière (juridique, économique, social, réputation).

Au professionnel du droit de trouver ensuite les moyens juridiques permettant de mettre en œuvre et de sécuriser la/les opérations envisagées. Au besoin, en contact avec les administrations concernées.

Une boîte à outils complétée en 2017 par la CJUE et la loi sécurité publique

Une norme préventive entérinée par la CJUE : le principe de neutralité en entreprise

Fréquemment invoqué par les employeurs à l'appui

de certaines contraintes vestimentaires, le souci de préserver l'image et l'intérêt commercial de l'entreprise ne justifie pas une décision de licenciement pour refus d'ôter un signe religieux.

Ce principe a été rappelé le 14 mars 2017 par la CJUE avec un bémol de poids : le licenciement est injustifié sous réserve que le principe de neutralité en entreprise ne soit pas édicté dans le règlement intérieur.

Dans un deuxième avis du même jour, la CJUE consacre et explicite ce principe : le règlement intérieur peut prévoir une interdiction de porter tout signe religieux sur le lieu de travail si cela est justifié par un objectif légitime (tel qu'une politique de neutralité vis-à-vis des clients), des moyens proportionnés au but recherché et justifiés par le fonctionnement de l'entreprise ou le respect de droits fondamentaux.

De nouvelles normes répressives à l'appui de l'éviction des salariés dangereusement radicalisés

Le Code de la sécurité intérieure prévoit que les salariés des entreprises de transport de personnes et/ou de marchandises dangereuses peuvent faire l'objet d'enquêtes administratives, à l'occasion de leurs fonctions, pour examiner le risque d'atteinte à la sécurité.

La loi sécurité publique du 28 février 2017 complète ce dispositif en autorisant le licenciement à l'issue de cette enquête, sous réserve du défaut de reclassement. Elle réintroduit aussi le délit de consultation habituelle de site djihadistes, étant rappelé que l'employeur peut surveiller, sous certaines conditions, les sites consultés par ses salariés.

L'entreprise, tout comme votre société, n'est pas épargnée par la radicalisation islamiste. Pour le management souvent désorienté face aux implications multiples, nous avons une bonne nouvelle : des réponses opérationnelles sont possibles ! ■



et Marie-Laure Ingouf, associé, MIZ Avocats

L'exemple des revendications d'horaires adaptés

Pour le ramadan	Caractère exceptionnel et sans conséquence	Pas signe d'un processus radical	Acceptable Négociable
Horaires de pause pour les prières quotidiennes	Aménagement matériel envisageable sous réserve de sa compatibilité fonctionnelle et du défaut d'hostilité envers les collègues	Signe d'une pratique scrupuleuse	Acceptable Négociable VIGILANCE
Horaires de travail en fonction des prières quotidiennes	Pratique modifiant l'organisation du travail de l'entreprise	Signe de radicalisation	Non acceptable ni négociable ALERTE