Les minutes de
LALLEMAND & LEGROS
Newsletter numéro 4 - Septembre 2017

## EDITO

Humanisme, intégrité et professionnalisme sont les valeurs qui unissent les membres de notre cabinet.
Si tous les avocats composant Lallemand & Legros vivent leurs propres engagements, à leurs mesures, selon leurs sensibilités, notre association a toujours souhaité s'investir dans la cité.
Afin d'inscrire cet investissement dans le concret, notre cabinet a décidé d'apporter son soutien à l'action de l'association Solidarité Grands-Froids.
Cette association dont l'objectif est d' « aider à mieux vivre dans la rue » par l'aide concrète aux personnes en difficulté morale, physique ou sociale organise des actions de récolte de fonds, de vêtements et d'autres biens matériels.
Elle est aussi constamment à la recherche de bénévoles pour assurer les distributions des vêtements récoltés aux sans-abri lors de « vestiaires » qu'elle organise dans les différents centres d'hébergement du centre de Bruxelles.

Un long couloir rempli d'hommes, de femmes et d'enfants, d'ici ou d'ailleurs, qui n'ont pour la plupart pas d'autres vêtements que ceux qu'ils portent sur le dos.
Les portes de cette salle qui s'ouvrent sur des bénévoles qui ont trié les vêtements récoltés par âge et par taille et qui vont, tour à tour, les accueillir afin de les aider à tenter de trouver des vêtements adaptés pour remplacer les leurs.
Des vêtements neufs ? non, mais en parfait état et propres.
De simples regards et des sourires permettent de se comprendre.

Même si elle paraît dérisoire face à la détresse rencontrée, cette aide est essentielle. Afin de ne pas s'arrêter à des mots, nos avocats se sont engagés à assurer des « vestiaires » à un rythme régulier, tout au long de l'année.

Sachant qu'il n'y a jamais assez de mains pour aider, n'hésitez pas à découvrir cette association :
*http://www.solidaritegrandfroid.be*

# Dossier Spécial: RGPD

## La nouvelle règlementation européenne en matière de protection des données personnelles : soyez prêts pour mai 2018 !

*Par Stéphane Rodrigues*

Le cadre juridique européen en matière de protection des données personnelles, reposant actuellement sur la directive 95/46/CE[1], sera entièrement renouvelé le 25 mai 2018 avec l'entrée en vigueur du nouveau règlement (UE) 2016/679 du 27 avril 2016 portant règlement général sur la protection des données (« RGPD »)[2]. S'agissant d'un règlement d'application directe, il n'a pas à faire l'objet, en tant que tel, d'une transposition en droit national. Cela étant, une modification de la Loi sur la vie privée de 1992 est programmée pour aménager certains dispositifs, notamment en ce qui concerne l'autorité de contrôle ou le régime des sanctions.

Administration ou entreprise, la première question à laquelle il convient de répondre est de savoir si le RGPD est applicable (1°). Si tel est le cas, doit être identifié le responsable du traitement (2°) sur qui reposera un certain nombre d'obligations (3°) et qui devra veiller au respect des droits des personnes concernées (4°).

### 1° Circonscrire le champ d'application du RGPD

Le champ d'application du RGPD doit être appréhendé tant d'un point de vue matériel que géographique.
D'un point de vue matériel, sont visés le traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi que le traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier. Par « données personnelles », il convient d'entendre toute information se rapportant à une personne physique identifiée ou identifiable, étant précisé qu'est réputée être une 'personne physique identifiable' une personne physique qui peut être identifiée,

directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale. Quant à la notion de traitement, elle recouvre toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

Du point de vue territorial, le RGPD s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union. Est également concerné le « traitement transfrontalier », notamment lorsque le traitement a lieu dans l'UE dans le cadre des activités d'un établissement unique d'un responsable du traitement ou d'un sous-traitant, mais qui affecte sensiblement ou est susceptible d'affecter sensiblement des personnes concernées dans plusieurs États membres.

[1]Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JOCE, n° L 281 du 23.11.1995 pp. 31-50. La directive a été transposée en droit belge par la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

[2] V. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, in JOUE L 119, 4.5.2016, p. 1–88.

## 2°- Identifier le responsable du traitement

Par responsable du traitement, il convient d'identifier la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre.

Le RGPD appréhende par ailleurs deux autres modalités de traitement : d'une part, le traitement conjoint par deux responsables ou plus, à condition qu'un accord entre ces derniers définisse de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences du RGPD ; d'autre part, le traitement sous-traité, dans l'hypothèse où une autre personne physique ou morale, autorité publique, service ou organisme traite des données à caractère personnel « pour le compte » du responsable du traitement. Dans ce dernier cas, le sous-traitant, ainsi que toute personne agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne peuvent pas traiter ces données, excepté sur instruction du responsable du traitement, à moins d'y être obligé par le droit de l'Union ou le droit d'un État membre.

## 3° - Prendre conscience de l'étendue des obligations pesant sur le responsable du traitement

Tout en ayant à l'esprit les dix principes directeurs qui doivent guider l'application du RGPD (licéité, loyauté, transparence, limitation des finalités, minimisation des données, exactitude, limitation de la conservation, intégrité, confidentialité et responsabilité), le responsable du traitement est tenu de mettre en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au RGPD, et ce en tenant compte de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques. Ces mesures doivent être adoptées dès le début des activités de traitement, à savoir tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même.

### Quatre grandes obligations générales pèsent alors sur le responsable du traitement :

- Une obligation de sécurité, en ce sens qu'il doit garantir un niveau de sécurité adapté au risque; à cette fin, il doit pouvoir évaluer les risques en amont et effectuer, sous certaines conditions, une analyse d'impact de toute opération de traitement;

- Un devoir de transparence, avec notamment l'obligation de communiquer dans les meilleurs délais à la personne concernée toute violation de données à caractère personnel susceptible d'engendrer un risque élevé pour ses droits et libertés, de même qu'un certain nombre d'informations à l'autorité nationale de contrôle. A cela s'ajoute, pour les structures comptant plus de 250 employés, la tenue d'un registre des activités de traitement.

● Un devoir de coopération avec l'autorité nationale de contrôle, notamment en cas de violation de données et lorsqu'une analyse d'impact indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque.

● Une exigence d'auto-contrôle: à ce titre, la désignation d'un délégué à la protection des données, jusqu'à présent facultative, est désormais obligatoire. Ce délégué peut être désigné en interne ou être une personne extérieure (sur base d'un contrat de service, par exemple un avocat: voir article par ailleurs). Dans les deux cas de figure, le délégué doit être associé d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel et surtout présenter toute garantie d'indépendance par rapport aux instances dirigeantes. On ajoutera qu'une entreprise peut toujours également adopter des règles internes contraignantes (à faire valider par l'autorité nationale de contrôle compétente) qui confèrent des droits supplémentaires aux personnes concernées.

## 4° - Veiller à respecter et faire respecter les droits des personnes concernées

En tout premier lieu, il doit être vérifié que l'opération de traitement proprement dit est licite en ce sens que soit les personnes concernées ont consenti par écrit au traitement de leurs données à caractère personnel pour une ou plusieurs finalités spécifiques; soit le traitement s'avère nécessaire pour l'exécution d'un contrat (auquel la personne concernée est partie), d'une obligation légale (à laquelle le responsable du traitement est soumis) ou d'une mission d'intérêt public (dont est investi le responsable du traitement); soit encore le traitement est requis pour la sauvegarde des intérêts vitaux de certaines personnes ou des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers (à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant).

En second lieu, le responsable de traitement doit être attentif à ne pas traiter certaines données (sauf exceptions) lorsqu'elles révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.
Les personnes concernées se voient en outre reconnaître une autre série de droits qu'il ne s'agit pas ici d'analyser dans le détail mais juste d'énoncer pour insister sur la nécessité de les respecter : un droit à la transparence et à l'information (pour permettre notamment d'identifier le responsable du traitement, de connaître les finalités du traitement, les destinataires éventuels de ses données, leur durée de conservation…) ; un droit d'accès aux données et à leur portabilité (i.e. la faculté de transmettre les données à un autre responsable du traitement, sauf en présence d'une mission d'intérêt public) ; un droit à la rectification, à l'effacement (sous certaines conditions limitativement énoncées) ou à la limitation du traitement ; un droit d'opposition au traitement (notamment pour tenir compte de la situation particulière de la personne concernée alors même que le traitement est nécessaire à l'exécution d'une mission d'intérêt public) ; un droit de réclamation (devant une autorité de contrôle) et de recours (devant une juridiction compétente).

Il peut être utile de préciser qu'une loi nationale ou une convention collective peut prévoir des règles plus spécifiques pour assurer la protection des droits et libertés en ce qui concerne le traitement des données à caractère personnel des employés dans le cadre des relations de travail.

Il convient enfin d'attirer l'attention sur le double régime visant à garantir l'effectivité dans le respect du RGPD : d'une part, un régime de sanctions administratives confié aux autorités nationales de contrôle (étant précisé que le montant de l'amende peut s'élever jusqu'à 20 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 4 % de son chiffre d'affaires annuel mondial) ; et, d'autre part, un régime de responsabilité ouvrant un droit à réparation pour toute personne ayant subi un dommage matériel ou moral du fait d'une violation du RGPD par le responsable du traitement ou, ce qui est nouveau par rapport au dispositif de la directive 95/46/CE, de manière subsidiaire, par son sous-traitant.

A l'issue de ce très sommaire et rapide tour d'horizon du RGPD, on ne peut que rappeler combien la problématique de la protection des données personnelles ne peut plus être ignorée aussi bien par les administrations que par les entreprises, compte tenu notamment de l'importance qu'elle a acquis au sein de l'ordre juridique de l'Union au nom de la protection du droit fondamental au respect de la vie privée (v. article 8 de la Charte des droits fondamentaux de l'Union et article 8 de la Convention européenne des droits de l'homme).

Administrations, professions libérales, entreprises relevant du RGPD ne peuvent donc qu'être invitées à mettre en place un dispositif adéquat de protection des données personnelles ou, si ce dernier existe déjà, à procéder à son audit au regard du nouveau cadre règlementaire. A cet égard, nous renverrons au document mis en ligne par la Commission de la protection de la vie

privée (CPVP) intitulé : « RGPD : Préparez-vous en 13 étapes », téléchargeable à l'adresse suivante: *https://www.privacycommission.be/sites/privacycommission/files/documents/STAPPENPLAN%20FR%20-%20V2.pdf*

*Le Cabinet L&L se tient à votre disposition pour vous assister dans l'audit juridique de votre dispositif de protection des données personnelles et en vérifier la conformité au regard des nouvelles exigences du RGPD. Mai 2018 est déjà demain !*

## La responsabilité et le rôle de l'avocat dans le traitement des données personnelles de ses clients.

*Par Nathalie Flandin*

De par l'exercice de sa profession, l'avocat est amené à traiter des données personnelles concernant ses clients. Ce traitement en tant que tel rentre dans le champ d'application du règlement (UE) 2016/679 du 27 avril 2016 portant règlement général sur la protection des données (« RGPD »), entrant en vigueur le 25 mai 2018 et qui stipule : « Le (…) règlement s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier ». (article 2, point 1 du RGDP). L'avocat est donc directement confronté à la mise en œuvre du RGDP, sa responsabilité est d'ailleurs encadrée par un certain nombre de principes juridiques que nous rappellerons ci-après (1). Il est intéressant de noter également que la mise en œuvre opérationnelle du RGDP va entraîner pour l'avocat un certain nombre de conséquences tant en ce qui concerne les outils à mettre en place lors du traitement des données personnelles de ses clients qu'en ce qui concerne le nouveau rôle qu'il peut être amené à jouer en tant que délégué à la protection des données (DPD), rôle nouvellement créé par le RGDP (2).

### 1) Les principes encadrant la responsabilité de l'avocat dans le traitement des données à caractère personnel.

Les principes généraux qui s'appliquent au traitement de données personnelles par un avocat sont les suivants :

● Principe de licéité : l'avocat doit s'assurer que les données sont collectées et traitées de manière transparente et loyale. Autrement dit, le consentement du client aux données qu'il fournit doit avoir été donné de façon claire et explicite. Il revient donc à l'avocat désormais de bien évaluer la manière dont il va demander, obtenir et enregistrer le consentement de ses clients lors de la transmission de leurs données personnelles ;

● Principe de finalité : les données doivent avoir été collectées dans un but déterminé, pour une raison précise. En l'espèce, dans le cadre de l'exercice de la profession de l'avocat, il peut être établi que la collecte des données personnelles de ses clients est réalisée aux fins de la représentation et de la défense des intérêts des clients ;

● Principe de proportionnalité : la collecte des données doit être pertinente, en rapport avec la finalité et limitée à ce qui est nécessaire ;

● Principe de durée de conservation : les données doivent être conservées uniquement durant le temps nécessaire à l'accomplissement de l'objectif poursuivi par la collecte. De façon concrète, il reviendra à l'avocat, responsable du traitement de données personnelles, de veiller à bien définir la durée de conservation des données et de mettre en place des mécanismes qui permettront de vérifier qu'au terme de l'écoulement de la période de conservation déterminée, les données personnelles ont bien été rendues indisponibles ;

● Principe de sécurité : la collecte des données personnelles des clients de l'avocat, qu'elle soit automatisée ou sur simple papier doit répondre à un certain nombre de garanties que l'avocat doit mettre en place de façon à ce que toutes les précautions soient prises pour que ces données ne puissent pas être perdues ou violées ;

● Principe de confidentialité : l'avocat doit s'assurer que les données auxquelles il a accès soit préservées de façon confidentielle ;

● Principe des droits de la personne concernée : les clients fournissant des données personnelles à leur avocat ont droit à avoir accès aux fichiers qui reprennent ces données, à la rectification à tout moment de ces données, à leur portabilité, autrement dit au transfert de ses données à un autre avocat, et à l'objection au traitement de ces données.

A noter qu'un certain nombre de principes plus spécifiques existent en cas de transfert de données personnelles à l'étranger. Dans un tel cas de figure, il faut distinguer les situations où le transfert est réalisé à l'intérieur d'un pays de l'Union européenne ou bien hors Union européenne :

● Si le transfert a lieu dans un pays de l'Union européenne, il n'y a pas de démarches particulières à effectuer. Le RGDP a pour but de viser l'harmonisation des différents systèmes nationaux de collecte et de traitement des données personnelles et les principes rappelés ci-avant s'appliquent automatiquement aux différents Etats membres ;

● En revanche si le transfert a lieu dans un pays non membre de l'Union européenne, le responsable du

traitement ne peut effectuer un tel transfert que lorsque la Commission a constaté par voie de décision que le pays en question assure un niveau de protection adéquat (cf. l'article 45 du RGDP qui vise les décisions d'adéquation de la Commission). Un tel transfert ne nécessite pas d'autorisation spécifique. En revanche, en l'absence de décision d'adéquation de la Commission, le responsable du traitement ne peut transférer des données à caractère personnel que s'il a prévu des garanties appropriées, telles que par exemple la signature de clauses contractuelles de protection des données (cf. article 46 du RGDP, des modèles de clauses contractuelles de protection des données sont publiées par la Commission sur son site).

### 2) Les conséquences de la mise en œuvre opérationnelle du RGDP pour les avocats

Dans le cadre de la mise en œuvre opérationnelle du RGDP, l'avocat qui traite des données personnelles dans le cadre de l'exercice de sa profession, en tant que conseil de ses clients, va devoir utiliser un certain nombre d'outils mis en place par le RGDP. Les principaux outils sont les suivants :

● La tenue d'un registre des activités de traitement et la documentation interne. A noter que la tenue de ce registre n'est pas obligatoire pour les entités comptant moins de 250 employés. Cela étant cette exception est fortement limitée par le RGDP qui stipule que tout responsable de traitement sera cependant soumis à cette obligation de documentation interne lorsque le traitement porte sur des données sensibles, c'est-à-dire des données personnelles qui révèlent : l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ou qui sont des données génétiques, biométriques ou qui concernent la santé, la vie sexuelle ou l'orientation sexuelle, lorsque le traitement porte sur des données judiciaires, c'est-à-dire sur des données à caractère personnel relatives aux infractions pénales et aux infractions ou aux mesures de sûreté connexes, lorsque le traitement de données est habituel: traitements liés à la gestion de la clientèle, à la gestion du personnel (ressources humaines) ou encore à la gestion des fournisseurs.

● Les analyses d'impact relatives à la protection des données pour les traitements à risque. Ces analyses ne sont requises en fait que dans des situations à haut risque, par exemple lorsqu'une nouvelle technologie est mise en œuvre ou lorsqu'une opération de profilage peut entraîner des effets considérables pour les personnes concernées. Dans l'exercice de sa profession, l'avocat, régulièrement amené à traiter des données personnelles sensibles, peut être amené également à faire du profilage. Il faut voir alors dans la pratique, si le traitement qu'il réalise peut être considéré comme à haut risque pour les personnes concernées. Si tel est le cas, il doit alors procéder à une analyse d'impact en bonne et due forme et recourir le cas échéant à des mesures de sécurité prévues par le RGDP, telles que la pseudonymisation, l'encryption.

● La sécurité des traitements est un élément essentiel du RGPD. De cette obligation de sécurité découle également l'obligation nouvelle de notifier à l'autorité de contrôle les violations de sécurité.

Il faut noter également que l'avocat peut être amené à exercer un rôle de délégué à la protection des données (DPD) auprès d'entités. Le DPD est celui qui va contrôler les traitements de données au sein d'une entité. Le DPD est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données. Le RGDP indique qu'il peut être un membre du personnel du responsable du traitement ou exercer ses missions sur la base d'un contrat de service.

La question se pose cependant lorsque ce rôle est tenu par un avocat, conseil d'une entité donnée, de la compatibilité de cette fonction avec le respect des règles déontologiques de l'avocat et notamment le respect du secret professionnel envers cette entité. Lorsque un DPD doit dénoncer ainsi des violations dans le traitement de données personnelles par l'entreprise auprès de laquelle il est DPD, à l'autorité de contrôle, il est amené à dévoiler alors un certain nombre de données. Afin d'écarter tout risque de conflit d'intérêts, le Conseil de l'Ordre a statué sur cette question lors de sa séance du 20 juin 2017, et a inséré une nouvelle section dans le Codeon à cet effet (voir article 2.100.d du RDB, *http://www.barreaudebruxelles.info/images/publications/recueil_codeon_rdb.pdf* )

L'avocat ne peut donc exercer un rôle de DPDP auprès d'une entité que s'il n'est pas également le conseil de cette entité.

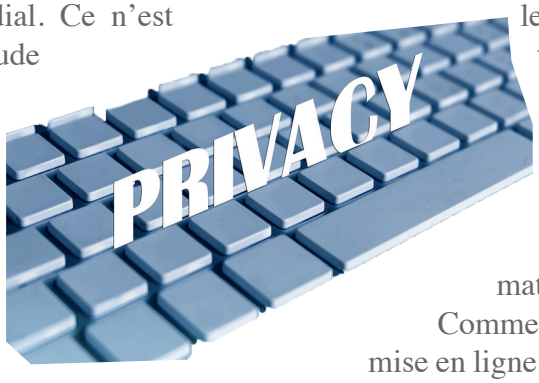
## La cybercriminalité, nouveau défi pour les avocats ?

*Par Annabel Champetier*

L'expansion de la société numérique a donné naissance, ces dernières années, à une véritable explosion de la cybercriminalité. A ce titre, depuis 2013, quatre milliards de données ont été volées et il se trouve, chaque jour, plus d'un million de personnes cibles d'actes de cybercriminalité. Les pertes estimées pour l'économie mondiale se chiffrent à 300 milliards de dollars et pourraient s'élever à 2 200 milliards d'euros d'ici 2020. Piratage de cartes bancaires, pillage de l'intelligence économique des sociétés, vols de consultations stratégiques d'avocats, défiguration de sites internet, infections virales…

De plus en plus, les entreprises sont les cibles de ces attaques. Ainsi, Airbus déjoue en moyenne douze attaques majeures par an. Les moyens de la cybercriminalité sont de plus en plus sophistiqués et les conséquences de plus en plus lourdes. Depuis peu, on assiste à des attaques groupées : le 12 mai 2017, une attaque informatique mondiale a sévi dans une douzaine de pays simultanément (ont été touchés : NHS, Renault, FedEX, Telefonica…). Mais les conséquences ne sont pas toujours uniquement économiques. Ainsi, le site de rencontres AshleyMadison.com a vu les données personnelles de 37 millions de ses abonnés piratées et publiées, entrainant divorces, chantages, possibles licenciements et suicides. Dans certains pays où l'adultère est puni par la loi, certains utilisateurs se sont même retrouvés menacés de poursuites judiciaires.

Face à ce nouveau phénomène, la question de la responsabilité se pose. Qu'en est-il de la responsabilité de la machine, à côté de celle de l'Homme ? La cybercriminalité vise avant tout les systèmes d'information, et peut ainsi être favorisée par des comportements de négligence. On assiste alors à une obligation croissante de sécurité pesant sur les chefs d'entreprise, dont le comportement en « bon père de famille » est alors primordial. Ce n'est pas simple, étant donné la multitude des risques pouvant favoriser une attaque. A titre d'exemple, 70 % des employés n'ont pas conscience du risque lié au transfert des données de l'entreprise vers l'ordinateur professionnel, des tablettes, des smartphones, des applications de partage de fichiers en ligne.. Ces risques sont accrus par la pratique émergente du BDO (« Bring your Own Device ») qui encourage les employés à travailler depuis leurs propres machines. Dans ce cadre, les données personnelles et les données professionnelles sont mixées, entrainant alors un risque accru de piratage. Les défaillances dans les systèmes de sécurité peuvent également être multiples : changement des codes d'accès, récupération des badges, départ de salariés de l'entreprise, appels d'offres…




Face à ces risques grandissant, l'avocat se heurte à de nombreuses difficultés.

Il lui appartient avant tout de maitriser un *dispositif légal extrêmement dense et en évolution permanente*. On a assisté au plan européen à un effort d'harmonisation, avec notamment l'émergence de plusieurs décisions-cadre telle celle du 13 juin 2002 relative à la lutte contre le terrorisme. Après trois ans de négociations, la directive NIS sur la cybersécurité a finalement été adoptée le 6 juillet et est entrée en vigueur le 19 juillet 2016. Elle prévoit le renforcement des capacités nationales de cybersécurité et établit un cadre formel de coopération entre Etats membres. Elle devra être transposée par les ces derniers avant le 9 mai 2018, avec l'aide de l'Agence Européenne chargée de la sécurité des réseaux et des systèmes d'information (ENISA). En outre, depuis le 1er janvier 2013, le Centre européen de lutte contre la cybercriminalité siège à la Haye, dans les locaux d'EUROPOL.

Au-delà de cet arsenal juridique complexe, il existe des difficultés aussi bien au niveau de *l'identification de l'auteur de l'infraction que de l'établissement de la preuve*. Ainsi, comment faire quand le serveur à l'origine du virus vient de ce qu'on appelle le « Web profond », cette partie de l'architecture du web non indexée et donc non accessible via les principaux moteurs de recherche? Les tribunaux exigent la plupart du temps d'importantes garanties en termes d'intégrité de la preuve. Cette dernière est souvent détenue par des opérateurs étrangers et l'intervention d'experts est alors nécessaire. De même, le délai pour agir pose problème. En effet, la cybercriminalité crée des situations dans lesquelles la victime se rend compte souvent bien trop tard de la cyber-infraction dont elle a été la cible. Ainsi, les escroqueries aux faux ordres de virement déstabilisent financièrement les entreprises pendant longtemps avant qu'elles soient mises en lumière. Ce retard dans la prise de conscience de la cyberattaque pose également des problèmes en matière de réparation du préjudice. Comment évaluer le préjudice résultant de la mise en ligne de données personnelles, pendant des mois, avant que la victime ne s'en rende compte ? En outre, rien ne s'oublie sur le net. Un référencement qui cause préjudice ne disparaitra jamais.

Ces obstacles exigent que l'avocat adapte sa façon d'appréhender la cybercriminalité. De plus en plus, *il se doit de prévenir, en amont*. Ainsi, en cas d'attaque du système informatique d'une entreprise par un virus, le juge va rechercher dans un premier temps si le chef d'entreprise avait mis en place un bon système antivirus, l'avait maintenu à jour et avait mis en place, au sein de son entreprise, une charte interne qui interdirait de se connecter à des sites malfaisants.
Cette obligation accrue de se comporter en bon père de famille doit être favorisée par une intervention en amont de l'avocat, qui doit donner à son client les outils afin de se prémunir contre les cyberinfractions.

Lutter contre la cybercriminalité implique d'intervenir dans des dossiers en lien constant avec un système opérationnel technique. L'avocat devrait donc également être familier des rouages et termes techniques

informatiques, rendant sa tâche encore plus complexe. Pour ce faire, il a besoin de s'adresser aux bons interlocuteurs et experts. De plus en plus, des coopérations se développent mais cela reste insuffisant. L'expansion de la société numérique exige qu'une vraie formation soit dispensée, pas uniquement aux avocats, mais également au personnel de police, aux magistrats. Dans tous les cas, afin de lutter efficacement contre la cybercriminalité, il est crucial que soient menés de front des partenariats avec les autorités administratives afin de bloquer les nouvelles pratiques telles que le « revenge porn » ou les sites d'incitation au suicide.
Finalement, la vraie difficulté qui se pose en matière de cybercriminalité reste la difficulté d'obtenir une norme internationale sur certains sujets. S'il est évident que certains sites sont prohibés et que certaines données personnelles ne doivent en aucun cas être dévoilées, comme c'est le cas avec la pédopornographie, le caractère condamnable de certains sites ne fait pas l'unanimité et il reste difficile de déterminer où placer le curseur.

# *Veille juridique*

*Par Margot Celli & Olivier Halein*

*• Loi du 13 mai 2017 insérant un article 134 septies dans la Nouvelle Loi communale en vue de permettre au Bourgmestre de fermer les établissements suspectés d'abriter des activités terroristes*

Cette loi, publiée le 16 juin 2017, insère dans la Nouvelle Loi communale un nouvel article 134 septies lequel autorise, désormais, un bourgmestre à procéder à la fermeture d'un établissement dans la mesure où des indices sérieux quant à l'existence et la présence d'activités de nature terroriste au sein de ce même lieu, seraient relevés.

*• Loi du 17 mai 2017 modifiant diverses lois en vue de compléter la procédure de dissolution judiciaire des sociétés*

Cette loi, publiée le 12 juin 2017, comporte des modifications importantes concernant la procédure de dissolution judiciaire des sociétés. Ces modifications touchent tant le Code judiciaire (modification des articles 764 et 1391), le Code des sociétés (modification substantielle de l'article 182, insertion des articles 182/1, 182/2, 182/3), que la loi du 8 août 1997 sur les faillites (abrogation de l'article 63 alinéa 3), ou encore la loi du 31 janvier 2009 relative à la continuité des entreprises (modification de l'article 12).

Le nouvel article 182 du Code des sociétés établit, notamment, les conditions et les modalités selon lesquelles un juge pourra, désormais, consécutivement à la non production par une société de ses comptes annuels, prononcer la dissolution d'une société.

*• Loi du 6 juin 2017 portant insertion d'un titre 3 « l'action en dommages et intérêts pour les infractions au droit de la concurrence » dans le livre XVII du Code de droit économique.*

Cette loi, publiée le 12 juin 2017, insère désormais un titre 3 dans le livre XVII du Code de droit économique ainsi que des définitions propres au livre XVII, insérées au sein du livre 1er.

Il s'agissait, pour le législateur national, de transposer la directive 2014/104/UE du Parlement Européen et du Conseil du 26 novembre 2014 relative à certaines règles régissant les actions en dommages et intérêts en droit national pour les infractions aux dispositions du droit de la concurrence des Etats membres et de l'Union européenne et de garantir aux entreprises ainsi qu'aux citoyens lésés par une infraction au droit européen et/ou national de la concurrence l'exercice d'un recours en dommages et intérêts devant les juridictions de fond.

Ce principe est, dorénavant consacré au sein de l'article XVII.72 du Code de droit économique : *« Toute personne physique ou morale qui a subi un dommage causé par une infraction au droit de la concurrence a le droit d'obtenir la réparation intégrale du dommage, conformément au droit commun ».*

*• Loi du 8 juin 2017 transposant en droit belge la directive 2014/26/UE du Parlement européen et du Conseil du 26 février 2014 concernant la gestion collective des droits sur des œuvres musicales en vue de leur utilisation en ligne dans le marché intérieur*

Cette loi, publiée le 27 juin 2016, transpose la fameuse directive 2014/26/UE dont les objectifs étaient les suivants : offrir un cadre juridique permettant de favoriser un bon fonctionnement des organes de gestion collective (notamment, en promouvant la transparence de leurs politiques de gestion, en améliorant leur gouvernance, en renforçant leurs obligations d'information et le contrôle de leurs activités par les titulaires de droits), de faciliter l'octroi de licences de droit d'auteur et de droits voisins pour l'utilisation de musique sur internet.

Ces objectifs devaient être rencontrés en recourant, notamment, aux mesures suivantes : un versement plus rapide des montants dus aux membres, la communication d'informations supplémentaires aux titulaires de droit, l'instauration de mécanismes pour la résolution des litiges pouvant survenir entre les organismes, les utilisateurs et les titulaires de droits.

Bon nombre de ces objectifs et dispositions de la directive avaient, néanmoins, déjà été atteints et intégrés par le législateur belge, dans l'ancienne loi belge sur les droits d'auteur du 30 juin 1994, modifiée par une loi du 10 décembre 2009 modifiant, en ce qui concerne le statut et le contrôle des sociétés de gesion des droits, la loi du 30 juin 1994 relative au droit d'auteur et aux droits voisins.

Cependant, les dispositions relatives à la propriété intellectuelle, figurant dorénavant au sein du Code de droit économique, devront faire l'objet de futurs amendements, afin de se conformer au prescrit de la directive, notamment en ce qui concerne les articles 9, 10 et 13 de la directive (fonction de surveillance des organismes de gestion collective, obligations incombant aux personnes gérant les activités de l'organisme, délais endéans desquels les organismes de gestion collective doivent verser les montants au bénéfice des titulaires de droits)

• *Loi du 25 juin 2017 réformant des régimes relatifs aux personnes transgenres en ce qui concerne la mention d'une modification de l'enregistrement du sexe dans les actes de l'état civil et ses effets*

La nouvelle loi du 25 juin 2017 adapte le Code civil et le Code judiciaire en ce qui concerne les personnes transgenres.

Si ces deux textes avaient été modifiés, au préalable, par la loi du 10 mai 2007 relative à la transsexualité, réglant la procédure et les conditions à respecter pour modifier l'enregistrement de son sexe dans les actes d'état civil, il reste que cette loi présentait deux difficultés majeures dès lors qu'elle imposait, d'une part, la stérilisation aux personnes désirant acter leur changement de sexe et d'autre part, que les liens de filiation des personnes transgenres après le changement de l'enregistrement du sexe officiel n'étaient pas réglés.

A cet égard, le nouveau texte simplifie la procédure de changement de nom, supprime les conditions médicales antérieurement exigées et supprime la possibilité pour toute personne intéressée de s'opposer à un changement de sexe dans l'acte de naissance.

Des garanties contre la fraude et les changements de l'enregistrement du sexe irréfléchis sont également instaurées. De même qu'un certain nombre d'éléments et de formulations imprécis de la loi du 10 mai 2007 ont été éliminés.

• *Loi du 6 juillet 2017 portant simplification, harmonisation, informatisation et modernisation de dispositions de droit civil et de procédure civile ainsi que du notariat, et portant diverses mesures en matière de justice (« Pot-pourriV »)*

Ce 24 juillet 2017, la loi du 6 juillet 2017 portant simplification, harmonisation, informatisation et modernisation de dispositions de droit civil et de procédure civile ainsi que du notariat, et portant diverses mesures en matière de justice, plus communément appelée « Pot-pourri V », a été publiée au Moniteur belge.

Parachevant l'exécution du Plan Justice du Ministre de la Justice, ce cinquième et dernier « Pot-pourri » met l'accent sur la protection de l'enfant, le rôle des notaires et l'organisatoin de l'Ordre judiciaire. Outre les modifications apportées au droit de la famille, au droit pénal ou encore au droit international privé, on retiendra la modification de l'article 1047 du Code judiciaire, limitant désormais la procédure d'opposition aux jugements par défaut « rendu[s] en dernier ressort ».

LALLEMAND & LEGROS

19 avenue Emile De Mot - 1000 Bruxelles
Téléphone : + 32 (0)2 648 75 30
- Fax : + 32 (0)2 648 78 41
Mail : info@lallemand-legros.be
Visitez notre site internet
www.lallemand-legros.be