LA LETTRE DU CABINET
TECHNOLOGIES DE L'INFORMATION

EDITO

Nous avons le plaisir de vous adresser le dix-septième numéro de notre Newsletter.

Cette lettre est organisée autour des thématiques suivantes : un flash spécial pour l'adoption du règlement européen sur la protection des données personnelles, puis des points sur la réglementation ou la jurisprudence dans les domaines du droit de l'informatique, de l'internet, de la protection des données personnelles, de la propriété intellectuelle et des marques, la santé numérique, le droit des affaires et le droit fiscal, le droit international et enfin la vie du Cabinet. Nous souhaitons par ce moyen vous informer des derniers développements du droit des technologies de l'information.

Si vous le souhaitez, merci de nous faire part de vos impressions, critiques ou suggestions.

Nous vous souhaitons une bonne lecture.

SOMMAIRE

ⓘ FLASH (P. 2-3) : ADOPTION DU RÈGLEMENT EUROPÉEN SUR LA PROTECTION DES DONNÉES PERSONNELLES

INFORMATIQUE (p.3-4)
Jurisprudence
- En l'absence de cession des droits, les codes sources des sites web appartiennent à la société les ayant développés
- La cour de cassation reconnaît la validité d'un contrat d'assurance conclu en ligne

INTERNET (p.4-7)
Réglementation
- Projet de loi pour une République numérique adopté en première lecture par le Sénat
- La Commission européenne présente une série de mesures visant à faciliter le passage de l'industrie au numérique
- Publication du décret précisant les modalités de l'obligation d'information à la charge des sites comparateurs
- L'Autorité de la concurrence rend un avis défavorable sur deux projets d'arrêtés sur la vente en ligne de médicaments
- Les autorités de la concurrence française et allemande publient une étude des effets du Big Data sur la concurrence
Jurisprudence
- Un site web condamné pour absence de dispositif de signalement de contenus illicites

PROTECTION DES DONNÉES PERSONNELLES (p.7-9)
Réglementation
- Point sur l'accord « EU-US Privacy Shield » sur le transfert de données vers les Etats-Unis
Prospective
- La CNIL lance un pack de conformité "véhicule connecté"
Jurisprudence
- La société Google sanctionnée par la CNIL pour son application restrictive du droit à l'oubli
- La CEDH valide l'accès par l'employeur aux emails privés des salariés

PROPRIÉTÉ INTELLECTUELLE ET MARQUES (p.9-10)
Jurisprudence
- La société Playmedia condamnée à verser 1M € à France Télévisions pour violation du droit d'auteur
- La société Moncler récupère 50 noms de domaine contrefaisants via la procédure UDRP de l'ICANN

SANTE NUMÉRIQUE (p.10)
Réglementation
- Les conditions de l'hébergement des données de santé modifiées par la loi du 26 janvier 2016

DROIT DES AFFAIRES (p.11-12)
Réglementation
- Adoption de la directive sur la protection du secret des affaires par le Parlement européen
- Allongement de la garantie légale de conformité
- Les dernières sanctions de la DGCCRF pour non-respect des délais de paiement

DROIT FISCAL ET E-COMMERCE (p.12)
Réglementation
- Abaissement du seuil de perception de TVA après des sites de e-commerce étrangers

INTERNATIONAL (p.12-13)
Réglementation
- Ratification de la Convention de la Haye sur les clauses attributives de juridiction par l'Union européenne et Singapour

VIE DU CABINET (p.13)

ⓘ FLASH – ADOPTION DU RÈGLEMENT EUROPÉEN SUR LA PROTECTION DES DONNÉES PERSONNELLES

Après plus de quatre ans de discussions, le règlement général sur la protection des données (RGDP) a finalement été promulgué le 27 avril 2016. Le règlement sera applicable dans tous les Etats membres dans deux ans, à compter du 25 mai 2018.
Le règlement remplacera la directive 95/46 CE du 24 octobre 1995 sur la protection des données personnelles. Ce texte constituera la référence européenne en matière de réglementation des données personnelles avec un ensemble unique de règles (à quelques exceptions près). Les principales dispositions peuvent être résumées ainsi :

Concernant les droits des personnes, on notera un raffermissement des droits existants sur leurs données personnelles. Les principales évolutions concernent notamment :

- Un renforcement des conditions de l'obtention du consentement des personnes (art. 7): les termes relatifs au consentement doivent être rédigés de manière claire et explicite. La personne concernée pourra à tout moment revenir sur son consentement ;
- La modification du droit à l'information dans le sens de la transparence et de la simplification (art. 12, 13 et 14) : l'information doit être concise, claire, compréhensible (en particulier lorsqu'elle est destinée aux enfants) et facilement accessible ;
- Le règlement consacre le "droit à l'oubli numérique" (art. 17) ;
- Le droit à la portabilité des données (art. 20) est un nouveau droit pour les personnes, qui pourront demander au responsable de traitement de récupérer ou transmettre leurs données personnelles à un nouveau responsable de traitement (par exemple, transferts entre services similaires proposés par des concurrents) ;
- Le règlement consacre le principe d'une protection spécifique des données personnelles des mineurs de moins de 16 ans (art. 8). Lorsque des services en ligne sont destinés aux enfants, les traitements de données de mineurs de moins de 16 ans seront soumis à l'accord ou l'autorisation de la personne exerçant l'autorité parentale.

Concernant les droits des responsables de traitement, on notera la simplification des formalités, mais des obligations plus strictes à leur égard. Le plafond des sanctions est nettement plus élevé que dans le système actuel. Le règlement a vocation à s'appliquer au sein de l'Union européenne, mais produira

également des effets extra-territoriaux (art. 3). Le règlement s'applique :
. aux responsables de traitement situés dans l'Union, que le traitement soit réalisé ou non sur le territoire de l'Union européenne,
. aux traitements de données personnelles de citoyens et résidents d'un pays membre, réalisés par un responsable de traitement ou un sous-traitant non situé dans l'UE, dès lors que l'offre de produits ou de services cible le marché européen ;

- Le recours aux traitements automatisés et aux techniques de profilage - qui prennent un nouvel essor avec le déploiement des techniques liées au Big data notamment, sera encadré (art. 22). Ces traitements seront autorisés sous certaines conditions et si la personne a donné son consentement ;
- Le responsable de traitement devra déployer des règles internes claires et facilement accessibles afin de garantir et démontrer le respect de la réglementation en matière de recensement des traitements, de sécurité, et le cas échéant d'accomplissement des formalités préalables et de désignation d'un délégué à la protection des données (notion d'"accountability") (art. 5 et 24) ;
- Lors du développement de nouveaux produits ou services, les responsables de traitement devront intégrer par défaut la protection des données personnelles dans la définition des moyens de traitement et dans le traitement lui-même (principe de "protection de la vie privée dès la conception" ou "privacy by design") (art. 5 et 25) ;
- Afin de prendre en compte l'évolution des techniques et des usages, le règlement reconnaît désormais la notion de co-responsabilité (ou responsabilité conjointe) de deux, ou plus, responsables de traitement. (art. 26) Les sous-traitants voient ainsi leur responsabilité reconnue au même titre que celle de leur client ;
- L'obligation de déclaration préalable d'un traitement de données est supprimée, (art. 30) sauf dans le cas d'un transfert de données hors de l'Union européenne, pour lequel un régime spécifique a été instauré. En contrepartie, le responsable de traitement est tenu (i) soit de tenir un registre interne recensant les traitements mis en œuvre, (ii) soit de se conformer à une consultation préalable de l'autorité de supervision pour les cas où la mise en place des traitements a nécessité une étude d'impact et comporte des risques particuliers ;
- Le règlement prévoit des règles de sécurité accrues pour la protection des données à caractère personnel, en étendant l'obligation de notification des failles de sécurité à tous les responsables de traitement. (art. 5, et 32 à 34) ;
- Un délégué à la protection des données devra être désigné dans les entreprises ayant pour "activité de base" la gestion de données personnelles "à grande échelle" ou le contrôle et suivi du comportement des personnes (art. 37, 38 et 39) ;
- Les règles de transfert des données hors Union européenne évoluent peu (art. 44 à 50) ;
- Les entreprises présentes dans plusieurs Etats membres désigneront une autorité de contrôle comme autorité principale compétente, notamment en cas de litige (art. 56) ;
- Le règlement prévoit un pouvoir de sanction des autorités de contrôle plus large et dissuasif (art. 83). Selon le type de violation à la loi retenu, les autorités de contrôle pourront prononcer des amendes administratives pouvant s'élever soit à 10 millions d'euros ou 2% du chiffre d'affaires total mondial de l'entreprise pour l'exercice précédent, le montant le plus élevé étant retenu, soit à 20 millions d'euros ou 4% du chiffre d'affaires total mondial de l'entreprise pour l'exercice précédent.

Les entreprises disposent de cette période de transition de deux ans pour préparer leur mise en conformité juridique et opérationnelle. Cette mise en conformité implique une mise à niveau des conditions d'utilisation et politiques de protection des données des services proposés ainsi que des politiques internes de protection des données applicables aux salariés. *(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 de données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement générale sur la protection des données)*

INFORMATIQUE

JURISPRUDENCE

Code source – En l'absence de cession des droits, les codes sources des sites appartiennent à la société les ayant développés

Courant 2011, la société LDG Constructions avait commandé à la société Mediacom Studio le développement de sites internet pour les sociétés de son groupe, ainsi que la réservation des noms de domaine et l'hébergement des sites. Dans un courrier du 8 mars 2013, la société LDG

Constructions a informé le prestataire de son souhait de reprendre l'hébergement de ses sites web en interne. La société Mediacom Studio a considéré que LDG Constructions avait ainsi pris la décision de résilier son contrat d'hébergement à la date d'échéance annuelle, ce que LDG Constructions contestait. Mediacom a informé la société LDG Constructions que la résiliation du contrat d'hébergement des sites mettrait un terme au droit d'utilisation des sites. En effet, les droits de propriété intellectuelle sur les sites, développés par Mediacom, n'avaient pas été cédés à la société LDG Constructions. La résiliation du contrat d'hébergement des sites a donc entraîné leur suspension. La société LDG Constructions a assigné la société Mediacom pour résiliation fautive du contrat d'hébergement.
Dans un jugement du 23 mars 2016, le tribunal de commerce de Besançon a suivi les arguments de la société prestataire en constatant que par son courrier du 8 mars 2013, la société LDG Constructions avait dénoncé le contrat d'hébergement et que le prestataire était fondé à refuser de communiquer le code source des sites internet à la société LDG Constructions en l'absence de cession des droits de propriété intellectuelle du code. *(T. Com. Besançon, jugement du 23 mars 2016, LDG Construction c/ Mediacom Studio)*

Signature électronique – La Cour de cassation reconnaît la validité d'un contrat d'assurance conclu en ligne
Une personne avait fait une demande d'adhésion en ligne à une assurance complémentaire, mais a ensuite nié avoir conclu un contrat en ligne et refusé de payer la somme due au titre du contrat souscrit. Le tribunal d'instance de Montpellier avait vérifié que la signature électronique avait été établie par un dispositif sécurisé de création de signature électronique et a donc reconnu la validité du contrat conclu en ligne. Estimant que le juge n'avait pas vérifié les conditions de validité de la signature électronique, le particulier s'est pourvu en cassation.
Dans sa décision du 6 avril 2016, la Cour de cassation a confirmé le jugement ayant reconnu la validité de la signature électronique, en énonçant que « *le jugement retient que la demande d'adhésion sous forme électronique a été établie et conservée dans des conditions de nature à garantir son intégrité, que la signature a été identifiée par un procédé fiable garantissant le lien avec la signature électronique avec l'acte auquel elle s'attache, et que la demande d'adhésion produite à l'audience porte mention de la délivrance de ce document par la plateforme de contractualisation en ligne Contraleo (…)* ». En conséquence, le pourvoi a été rejeté. *(C. cass. Ch. Civ. 1, arrêt du 6 avril 2016, M. X c/ Alptis Individuelles Santé)*

INTERNET

RÉGLEMENTATION

Projet de loi pour une République numérique – Adoption par le Sénat et nouvelles dispositions relatives à l'accessibilité numérique
Après son adoption en première lecture par l'Assemblée nationale le 26 janvier 2016, le Sénat a adopté une version profondément amendée le 3 mai dernier. Le texte devrait maintenant être examiné en commission paritaire et être voté dans les prochains mois.
Pour rappel, la loi pour une République numérique modifiera et complétera la loi Informatique et Libertés, en intégrant quelques notions que l'on retrouve dans le nouveau Règlement général sur la protection des données, telles que le renforcement de l'information des personnes concernées, la création d'un "droit à l'oubli numérique" (droit à l'effacement des données) spécifique pour les mineurs, la reconnaissance d'un nouveau droit à la portabilité et à la récupération des données.
A noter que dans la version votée par le Sénat figurent des dispositions visant à faire progresser l'accessibilité numérique des services en ligne. Le projet de loi comporte une section 2 intitulée « Accès des personnes handicapées aux sites internet publics ». L'article 47 de la loi n°2005-102 du 11 février 2005 pour l'égalité des droits et des chances, la participation et la citoyenneté des personnes handicapées serait modifié et son champ d'application élargi aux sociétés privées : « *Art. 47. – I. – Les services de communication au public en ligne des services de l'État, des collectivités territoriales et des établissements publics qui en dépendent ainsi que ceux des organismes délégataires d'une mission de service public, des services de communication des entreprises bénéficiant d'un financement public et des entreprises fournissant des services d'intérêt général doivent être accessibles aux personnes handicapées.*
« L'accessibilité des services de communication au public en ligne concerne l'accès à tout type d'information sous forme numérique, quels que soient le moyen d'accès, les contenus et le mode de consultation et vise notamment les sites internet, intranet, extranet, applications mobiles, progiciels et

mobilier urbain numérique. Les recommandations internationales pour l'accessibilité de l'internet doivent être appliquées pour les services de communication publique en ligne. (…)
« III - Le défaut de mise en conformité d'un service de communication au public en ligne avec les obligations prévues au II fait l'objet d'une sanction administrative dont le montant, qui ne peut excéder 5 000 €, est fixé par le décret en Conseil d'État mentionné au IV. Une nouvelle sanction est prononcée chaque année lorsque le manquement à ces dispositions perdure. » (Projet de loi pour une République numérique, adopté en 1ère lecture par le Sénat le 3 mai 2016, Petite loi)

Marché unique numérique - La Commission européenne présente une série de mesures visant à faciliter le passage de l'industrie au numérique

Le 19 avril dernier, la Commission a présenté une série de mesures destinées à soutenir les initiatives nationales pour le passage au numérique de l'industrie et des services connexes, ainsi qu'à stimuler l'investissement au moyen de partenariats et réseaux stratégiques.
Bien que plusieurs États membres aient déjà déployé des plans pour le numérique dans l'industrie, une approche pan-européenne permettrait d'éviter la fragmentation des marchés et de tirer profit des évolutions numériques telles que l'internet des objets.
La Commission propose des mesures pour accélérer l'élaboration de normes communes dans des domaines prioritaires, tels que les réseaux de communication 5G ou la cybersécurité, et de moderniser les services publics.
Dans le cadre de cette approche, la Commission souhaite notamment cibler les investissements dans des partenariats public-privé européens, investir 500 millions d'euros dans un réseau paneuropéen de «plateformes d'innovation numérique» (centres d'excellence technologique) au sein duquel les entreprises pourront obtenir des conseils et tester les innovations numériques, mettre en place des projets pilotes à grande échelle afin de renforcer l'internet des objets et les technologies de fabrication avancées dans des villes et maisons intelligentes, des voitures connectées ou des services de santé mobile et adopter une législation qui favorisera la libre circulation des données et clarifiera la question de la propriété des données obtenues par des capteurs et dispositifs intelligents.
La Commission propose par ailleurs des mesures pour accélérer l'élaboration de normes, pour favoriser la communication entre les systèmes. A cette fin, l'accent sera mis sur cinq domaines prioritaires, à savoir : la 5G, le Cloud computing, l'internet des objets, les technologies des données et la cybersécurité. Des cofinancements seront proposés pour les essais et l'expérimentation des technologies afin d'accélérer la définition de normes, notamment dans le cadre de partenariats public-privé.
Ce plan ambitieux doit aussi permettre d'accélérer le développement et l'adoption de technologies telles que les réseaux intelligents, les services de santé mobile, ou les véhicules connectés. Un volet « services publics numériques » est également prévu avec 20 mesures devant être lancées d'ici à la fin de 2017. Ce volet services publics numériques comprend la création d'un portail numérique unique, l'interconnexion de tous les registres du commerce et registres d'insolvabilité qui seront par ailleurs reliés au portail e-Justice, qui deviendra un guichet unique. Enfin, le développement des services de santé en ligne à caractère transfrontalier est également prévu, comprenant les prescriptions en ligne et les dossiers des patients. *(Commission européenne - Communiqué de presse "La Commission présente des mesures en vue du passage au numérique de l'industrie européenne", 19 avril 2016*)

Sites comparateurs – Publication du décret précisant les modalités de l'obligation d'information à la charge des sites comparateurs

Les sites comparateurs sont de plus en plus utilisés par les consommateurs, notamment dans les domaines tels que les voyages, l'assurance, les restaurants, pour s'étendre à tous types de produits et services.
L'ordonnance du 14 mars 2016 prévoit au nouvel article L.111-6 du Code de la consommation que « *toute personne dont l'activité consiste en la fourniture d'informations en ligne permettant la comparaison des prix et des caractéristiques de biens et de services proposés par des professionnels est tenue d'apporter une information loyale, claire et transparente, y compris sur ce qui relève de la publicité au sens de l'article 20 de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique* » (LCEN).
Les modalités et le contenu de cette information viennent d'être fixées par le décret du 22 avril 2016, venant compléter la partie réglementaire du Code de la consommation. Sont ainsi précisés le type d'activité de comparaison soumis aux obligations d'information et le contenu de ces obligations. Par ailleurs, l'exploitant du site doit afficher le caractère publicitaire d'une offre référencée à titre payant et dont le classement dépend de la rémunération perçue. Ces dispositions entreront en vigueur le 1er juillet 2016. *(Ordonnance n°2016-301 du 14 mars 2016 et décret n° 2016-505 du 22 avril 2016)*

Vente en ligne de médicaments– L'Autorité de la concurrence rend un avis défavorable sur deux projets d'arrêtés

L'ordonnance du 19 décembre 2012 prévoit le droit pour les pharmaciens établis en France de vendre des médicaments en ligne, sous certaines conditions décrites dans un arrêté du 20 juin 2013. Ces conditions, considérées comme trop rigides, n'ont résulté que dans un développement très faible de cette activité en France.

Deux nouveaux projets d'arrêtés relatifs à la vente en ligne de médicaments (« *Bonnes pratiques de dispensation des médicaments par voie électronique et Règles techniques applicables aux sites internet de commerce électronique de médicaments* ») ont été soumis à l'Autorité de la concurrence qui vient d'émettre un avis défavorable, notamment dans la mesure où ces textes reprennent des dispositions dont le caractère restrictif avait déjà été souligné par celle-ci dans de précédents avis.

De plus, ces projets d'arrêtés introduisent de nouvelles dispositions qui créent des contraintes additionnelles disproportionnées par rapport à l'objectif de protection de la santé publique, ainsi qu'un régime discriminatoire par rapport à la vente au comptoir. Par un encadrement trop contraignant de la vente de médicaments en ligne, ces textes auraient pour effet de brider la concurrence, alors que la vente en ligne de médicaments devrait dynamiser et moderniser l'activité des pharmaciens, au bénéfice des consommateurs (prix plus attractifs et meilleurs information sur les prix). *(Autorité de la concurrence, Avis 16-A-09 du 26 avril 2016 relatif à deux projets d'arrêtés concernant le commerce électronique de médicaments)*

Big Data – Etude des effets du Big Data par les autorités de la concurrence française et allemande

Les autorités de la concurrence française et allemande (Bundeskartellamt) viennent de publier une étude en date du 10 mai 2016 sur le Big Data et les enjeux du développement de cette pratique sur le droit de la concurrence. Les autorités de la concurrence française et allemande ont ainsi analysé les implications et les défis posés par la collecte et le traitement de masse des données face au droit de la concurrence. « *Déterminer pourquoi, comment et dans quelle mesure les données pourraient devenir un instrument de pouvoir de marché est un sujet important pour les autorités de concurrence dans le monde*. »

Deux questions principales sont abordées : le problème de l'accessibilité des données par les concurrents et l'importance de la variété et du volume des données. L'étude comprend un aperçu de la pratique décisionnelle, de la jurisprudence et de la doctrine à ce jour. *(« Competition law and data » étude conjointe de l'Autorité de la concurrence et du Bundeskartellamt du 10 mai 2016)*

JURISPRUDENCE

LCEN - Un site web condamné pour absence de dispositif de signalement de contenus illicites

Les associations Union des Etudiants Juifs de France (UEJF) et Action Internationale pour la Justice (AIPJ) ayant notamment pour objet la lutte contre le racisme, l'antisémitisme et le négationnisme, ont assigné l'association Egalité et Réconciliation, qui édite un site web du même nom après avoir constaté la présence sur ce site de textes, images et dessins susceptibles de contrevenir aux dispositions sanctionnant l'apologie de crimes contre l'humanité et l'incitation à la haine raciale, et l'absence de dispositif de signalement de contenus illicites.

Dans un jugement rendu le 13 avril 2016, le tribunal de grande instance de Paris a rappelé que, même si en application de l'article 6.I-7 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN), les personnes mentionnées à cet article (hébergeant des données communiquées par des tiers au service) ne sont pas soumises à une obligation générale de surveillance des informations transmises ou stockées, certains contenus font l'objet d'un statut particulier. Ainsi, en vertu de l'article 6.I.-7 de la LCEN, « *compte tenu de l'intérêt général attaché à la répression de l'apologie des crimes contre l'humanité, de la provocation à la commission d'actes de terrorisme et de leur apologie, de l'incitation à la haine raciale (…)* », les hébergeurs de contenus fournis par des tiers, tels que définis dans la LCEN, sont tenus de mettre en place un dispositif facilement accessible et visible de signalement de ces contenus illicites afin de concourir à la lutte contre la diffusion des infractions visées à l'article 24 al.5- 7 et 8 de la loi du 29 juillet 1881 sur la liberté de la presse et aux articles 227-23, 227-24 et 421-2-5 du code pénal.

Les magistrats rappellent également que les hébergeurs de contenus tiers ont l'obligation d'informer promptement les autorités publiques compétentes de toutes activités illicites mentionnées ci-dessus qui leur seraient signalées et de rendre publics les moyens qu'ils consacrent à la lutte contre ces activités illicites. Tout manquement à ces obligations est puni d'un an d'emprisonnement et de 75.000€ d'amende (art. 6.-III.-1. de la LCEN).

En l'espèce, le tribunal a ordonné à l'association Egalité et Réconciliation de se mettre en conformité avec ses obligations légales, à savoir mettre en place un dispositif de signalement des contenus illicites, facilement accessible et visible. *(TGI Paris, ordonnance de référé du 13 avril 2016, UEJF et AIPJ c/ Egalité et Réconciliation)*

PROTECTION DES DONNÉES PERSONNELLES

RÉGLEMENTATION

Transfert de données vers les Etats-Unis – Point sur l'accord « EU-US Privacy Shield »

Un nouvel accord dénommé Privacy Shield (Bouclier de protection de la vie privée), a été adopté entre l'UE et les Etats-Unis en remplacement du Safe Harbor, pour permettre aux entreprises européennes de transférer des données personnelles vers les Etats-Unis, à des entreprises américaines adhérant au système. L'entrée en vigueur du Privacy Shield est à la publication par la Commission européenne de la décision d'adéquation aux règles de protection de la vie privée en Europe. L'avis des membres du G29 (« CNIL » européennes) sur la décision d'adéquation de cet accord à la réglementation européenne a été rendu public le 13 avril 2016. Bien qu'il reconnaisse des améliorations significatives par rapport au Safe Harbor, le G29 relève plusieurs points qui devraient être revus.

Le G29 souligne un manque de clarté dû à la multiplicité des documents (document principal et plusieurs annexes) et le manque de cohérence entre le Privacy Shield et la réglementation européenne concernant leurs champs d'application respectifs ou la terminologie employée. Notamment, des principes clés de la protection des données de la réglementation européenne n'ont pas d'équivalent dans le Privacy Shield.

Par ailleurs, les règles du Privacy Shield permettront le transfert subséquent des données en dehors des Etats-Unis. Or dans sa version actuelle, le texte n'offrirait pas assez de garanties pour l'application d'un niveau de protection identique en cas de transfert vers des pays tiers.

Concernant l'accès des autorités publiques aux données transférées, le G29 relève que les autorités américaines n'ont pas apporté de garanties suffisantes pour écarter la possibilité d'une surveillance massive des données de citoyens européens, problématique à l'origine de l'affaire "Snowden" et l'une des raisons de l'invalidation du système de Safe Harbor.

Enfin, le G29 propose d'intégrer une clause de révision du Privacy Shield pour prendre en compte l'évolution de la réglementation européenne sur la protection des données lorsque le règlement européen sera applicable.

Bien que l'avis du G29 n'ait pas de valeur contraignante, les autorités de protection demandent néanmoins à la Commission européenne de répondre à leurs préoccupations et d'apporter les précisions nécessaires pour améliorer le projet de décision d'adéquation du Privacy Shield au droit européen. Ce nouvel accord devrait entrer en vigueur au mois de juin 2016. *(G29 Opinion 01/2016 on the EU-US Privacy Shield draft adequacy decision – 13.04.2016)*

PROSPECTIVE

IoT - Lancement d'un pack de conformité "véhicule connecté" par la CNIL

Le 23 mars 2016, la CNIL a lancé les travaux sur un pack de conformité « véhicule connecté ». Ces travaux sont réalisés avec la participation d'acteurs de la filière automobile, d'entreprises innovantes du secteur des assurances et des télécoms, et des autorités publiques. Les véhicules connectés seront des outils de traitement de données, notamment personnelles concernant le conducteur du véhicule et son interaction avec l'environnement. L'objectif de la CNIL est de proposer des lignes directrices aux parties prenantes, via une « boîte à outils » de la conformité, spécifique au véhicule connecté (voir les démarches de « privacy by design »). Ce pack de conformité est également l'occasion de préparer les acteurs du secteur au règlement européen sur les données personnelles, applicable en mai 2018. (*Communication CNIL "En route vers un pack de conformité consacré aux véhicules connectés" 23 mars 2016*)

JURISPRUDENCE

Délibération CNIL – La société Google sanctionnée pour son application restrictive du droit à l'oubli

Depuis la décision du 13 mai 2014 de la Cour de Justice de l'Union européenne (CJUE), les internautes résidant en Europe peuvent demander aux moteurs de recherche, sous certaines conditions, le déréférencement d'informations les concernant (« droit à l'oubli »). Les décisions de

refus de déréférencement peuvent être contestées notamment auprès de la CNIL (pour la France). La CNIL a ainsi été saisie par des internautes s'étant vu refuser le déréférencement de liens sur le moteur de recherche Google.
Google limite le déréférencement aux extensions géographiques européennes du moteur de recherche et n'intervient pas sur les extensions non-européennes ni sur le .com, sur lesquelles les liens déréférencés pour l'Europe restent actifs. En mai 2015, la Présidente de la CNIL a mis en demeure Google d'étendre le déréférencement à toutes les extensions du moteur de recherche. Google ne s'étant pas exécuté dans le délai imparti par la mise en demeure, la CNIL a engagé une procédure de sanction à l'encontre de la société.
Le 10 mars 2016, la CNIL a prononcé une sanction pécuniaire de 100.000€ à l'encontre de la société Google inc., suite au non-respect de la mise en demeure de la Présidente de la CNIL de procéder au déréférencement sur l'intégralité des extensions du nom de domaine de son moteur de recherche. Dans sa décision, la formation restreinte de la CNIL considère que :

- le moteur de recherche Google constitue un traitement unique, les différentes extensions géographiques (".fr", ".es", "com", etc.) ne pouvant être considérées comme des traitements distincts ;
- pour que le droit au déréférencement des personnes résidant en France soit effectivement respecté, il doit être exercé sur l'ensemble du traitement de données, et donc sur toutes les extensions du moteur de recherche ;
- contrairement à la position de Google, le déréférencement sur toutes les extensions du moteur ne limite pas la liberté d'expression, dans la mesure où il n'entraîne aucune suppression de contenu sur internet, mais consiste uniquement à retirer, à la demande d'une personne physique, de la liste des résultats d'une recherche effectuée à partir de ses prénom et nom, des liens renvoyant vers des pages de sites web. Ces pages sont en principe toujours accessibles (sauf suppression du contenu sur le site d'origine) lorsque la recherche est réalisée à partir d'autres termes, ou en se rendant directement sur les sites d'origine.

La société Google inc. vient d'annoncer qu'elle faisait appel de cette décision devant le Conseil d'Etat, contestant notamment le caractère extraterritorial de la décision de la CNIL. *(Délibération de la formation restreinte n°2016-054 du 10 mars 2016 prononçant une sanction pécuniaire à l'encontre de la société Google inc.)*

Cybersurveillance des salariés - Décision de la CEDH sur le droit de l'employeur de consulter les emails des salariés

En France, la jurisprudence relative au droit de l'employeur de consulter les emails de ses employés est clairement définie par la jurisprudence de la Cour de cassation. Ainsi, non seulement les emails adressés par le salarié grâce aux moyens mis à sa disposition par son employeur sont présumés avoir un caractère professionnel, mais l'utilisation abusive d'internet pour des raisons personnelles pendant les heures de travail est par ailleurs considérée comme constitutive d'une faute grave, pouvant justifier un licenciement.
Dans un arrêt du 12 janvier 2016, la Cour européenne des droits de l'homme (CEDH) a à son tour validé le droit de l'employeur de consulter les emails des salariés.
Dans cette affaire, M. Barbulescu, ressortissant roumain, avait été licencié par son employeur pour avoir utilisé à des fins personnelles pendant les heures de travail, le compte email mis à sa disposition par sa société, malgré le règlement interne qui interdisait une telle utilisation. Ce salarié avait ouvert un compte Yahoo Messenger à la demande de son employeur, pour une utilisation professionnelle. Le 13 juillet 2007, il fut informé par son employeur que ses communications avaient été surveillées entre le 5 et le 13 juillet 2007. Or, les enregistrements montraient qu'il avait utilisé internet à des fins personnelles. Le 1er août 2007, l'employeur le licenciait pour violation du règlement intérieur de la société qui interdisait l'usage de ses ressources à des fins personnelles. M. Barbulescu contesta son licenciement devant les tribunaux, arguant notamment que son employeur avait violé son droit à la correspondance privée en consultant ses communications en violation de la Constitution roumaine et du code pénal. L'employeur a eu gain de cause devant les tribunaux roumains, en première instance puis en appel.
M. Barbulescu a alors décidé de former un recours devant la Cour européenne des droits de l'Homme (CEDH) sur la base de l'article 8 de la Convention européenne des droits de l'homme (droit au respect de la vie privée et familiale, du domicile et de la correspondance), au motif que la décision de licenciement reposait sur la violation de sa vie privée.
Dans sa décision du 12 janvier 2016, la CEDH a considéré que n'était pas abusif le fait qu'un employeur vérifie que ses salariés accomplissent leurs tâches professionnelles pendant les heures de travail. La Cour relève que l'employeur a accédé au compte de M. Barbulescu, pensant qu'il contenait les communications de celui-ci avec les clients. La Cour relève en outre que M. Barbulescu a pu faire

valoir ses moyens relatifs à la violation de sa vie privée et de sa correspondance devant les tribunaux roumains. Or, les juges roumains n'ont utilisé les relevés des communications qu'aux fins de prouver que le salarié avait utilisé l'ordinateur de sa société pour un usage personnel pendant les heures de travail, sans divulguer l'identité des personnes avec lesquelles il avait communiqué. La Cour en a conclu que les juridictions roumaines avaient respecté l'équilibre entre le droit du demandeur au respect de sa vie privée et de sa correspondance et les intérêts de son employeur. En conséquence, la CEDH a conclu que l'article 8 de la Convention européenne des droits de l'homme n'avait pas été violé. *(CEDH aff. Barbulescu c/ Roumanie, requête n°61496/08, 12 janvier 2016)*

PROPRIÉTÉ INTELLECTUELLE

JURISPRUDENCE

Droit d'auteur - Playmedia condamnée à verser 1M € à France Télévisions

Dans un arrêt du 2 février 2016, la Cour d'appel de Paris a confirmé le jugement du TGI de Paris qui avait condamné la société Playmedia, éditeur du service Playtv.fr, à verser un million d'euros à la société France Télévisions pour avoir diffusé ses programmes sans son autorisation et en contrefaçon de ses droits d'auteur, de ses droits voisins, de producteurs de vidéo et de ses marques.

Depuis 2010, le service Playtv.fr diffuse les programmes de France Télévisions, sans autorisation ni contrat. Playmedia diffuse désormais les programmes au moyen de liens profonds vers le site de France Télévision, Pluzz. La société France Télévisions, radiodiffuseur de programmes audiovisuels, est présumée être titulaire des droits d'auteur sur les émissions qu'elle a produites, co-produites ou dont elle a acquis les droits. France Télévisions est par ailleurs autorisée à diffuser des programmes de tiers, sous licence. Certains titulaires de droits n'ont cependant pas autorisé France Télévisions à diffuser ou à faire diffuser leurs programmes sur internet.

La société Playmedia considérait qu'elle pouvait bénéficier du régime du "must carry", prévu par la loi du 30 septembre 1986 sur la liberté de communication, en application de la directive "service universel", qui impose l'accès aux programmes des chaînes de télévision. France Télévisions aurait donc commis un abus en refusant de conclure des accords avec elle, alors que le CSA avait validé son service d'abonnés lancé en 2013.

Selon les juges, l'exercice de la liberté de communication par la libre retransmission de programmes audiovisuels doit s'exercer dans le respect des droits d'autrui. La déclaration déposée auprès du CSA n'implique aucun contrôle ni autorisation ou validation de l'offre Playtv et n'implique pas automatiquement l'application de la règle du "must carry", ni la dispense du respect des droits de propriété intellectuelle ou de la conclusion de contrats de reprise, préalablement à la diffusion des chaînes concernées.

La Cour d'appel a également examiné le nouveau mode de diffusion et d'exploitation des chaînes de France Télévisions par la présence, à partir du service Playtv.fr, de liens profonds vers Pluzz, qui donnent automatiquement accès aux programmes de France Télévisions. La Cour d'appel a condamné la société Playmedia pour atteinte aux droits voisins de France Télévisions, pour diffusion des programmes au moyen de liens profonds vers le site Pluzz, sans l'accord de l'ayant droit.

La Cour d'appel a ajouté aux condamnations précédentes 200.000 € de dommages et intérêts à l'encontre de la société Playmedia et l'interdiction d'insérer les liens profonds vers le site Pluzz. La Cour considère que France Télévisions conserve son droit d'autoriser la diffusion de ses programmes, "y compris par le recours à des liens profonds par la technique de la transclusion". *(Cour d'appel de Paris, pôle 5 ch.1, arrêt du 2 février 2016 France Télévisions c/ Playmedia)*

Marques et Cybersquatting – La société Moncler récupère 50 noms de domaine contrefaisants

La société italienne Moncler fabrique et commercialise des vêtements de sport haut de gamme. Elle est par ailleurs titulaire de nombreuses marques. Trois ressortissants chinois avaient enregistré une cinquantaine de noms de domaine comprenant la marque Moncler, aux fins de vendre des articles contrefaisants.

La société Moncler a introduit une action en récupération des noms de domaine via la procédure Uniform Domain Name Dispute Resolution Policy (UDRP). Cette procédure, lancée par l'ICANN, permet à des titulaires de marque, de récupérer des noms de domaine enregistrés par des cybersquatteurs, par une procédure rapide pouvant être traitée par l'OMPI, évitant la lourdeur d'une procédure judiciaire. La procédure UDRP se déroule entièrement en ligne et dure en moyenne 60 jours à compter de la réception de la plainte par le Centre de l'OMPI. Selon la demande du requérant, la procédure peut aboutir à la suppression ou au transfert du nom de domaine concerné. Trois conditions doivent être réunies pour engager une procédure UDRP et récupérer un nom de domaine :

1) le demandeur doit avoir un intérêt légitime sur le nom de domaine litigieux, 2) le nom de domaine doit être identique ou similaire à la marque du demandeur et le nom de domaine contesté doit créer un risque de confusion avec la marque du demandeur, et 3) le nom de domaine a été enregistré par le tiers de mauvaise foi. (art. 4 a des principes directeurs UDRP)
Dans cette affaire, la société Moncler a invoqué le fait que tous les noms de domaine concernés contenaient la marque Moncler et que la plupart des sites vers lesquels ces noms de domaine pointaient, reproduisaient les contenus et la charte graphique du site du titulaire. Enfin, les sites proposaient à la vente des produits contrefaits. Dans sa décision du 18 janvier 2016, le Centre d'Arbitrage et de Médiation de l'OMPI a retenu que la société Moncler satisfaisait aux trois conditions sus-visées pour obtenir le transfert d'un nom de domaine. Moncler a ainsi obtenu gain de cause et pu récupérer les cinquante noms de domaine litigieux. *(WIPO Arbitration and Mediation Center, Administrative Panel décision, Moncler S.p.A. v. Yao Tom, Lee Fei & Geriy Wang, Case n°D2015-2244)*

SANTÉ NUMÉRIQUE

RÉGLEMENTATION

Loi de modernisation de notre système de santé – Modification des conditions de l'hébergement des données de santé
Depuis l'entrée en vigueur de la loi "Kouchner" de 2002, les prestataires hébergeurs de données de santé doivent être agréés. La loi du 26 janvier 2016 de modernisation de notre système de santé a modifié l'article L.1111-8 du Code de la santé publique relatif à l'hébergement de données de santé. Le périmètre des données, et les catégories de personnes concernées par l'hébergement agréé, ont été élargis. L'obligation d'agrément est maintenue et renforcée.
Les catégories de données concernées par l'hébergement agréé : dans son ancienne rédaction, l'article L.1111-8 al.1 du CSP disposait que les données de santé à caractère personnel "*recueillies ou produites à l'occasion des activités de prévention, de diagnostique ou de soins*" étaient concernées par cette obligation d'hébergement agréé. Or, si la question était claire pour les données de santé recueillies par les professionnels et les établissements de santé (médecins, infirmiers, hôpitaux et cliniques), la situation était plus confuse pour les autres acteurs pouvant intervenir, même à titre accessoire, dans le domaine de la santé.
Cette ambigüité est levée avec la nouvelle rédaction de l'article L.1111-8 qui étend les catégories de données concernées et inclut désormais les données recueillies à l'occasion du "*suivi social et médico-social*".
Les parties concernées par l'hébergement agréé : selon l'ancien article L.1111-8 al.1 du CSP les professionnels de santé, les établissements de santé et la personne concernée étaient les seules parties explicitement visées par cette obligation.
Le nouvel article ne précise plus les personnes concernées par la collecte et le traitement. En pratique, toute personne physique ou morale qui collecte et/ou traite des données de santé à caractère personnel et souhaite les faire héberger par un tiers, est soumise à l'obligation d'avoir recours à un hébergeur agréé.
Ainsi, non seulement les médecins et autres professionnels de santé (professions para-médicales), les établissements de santé restent concernés mais également les compagnies d'assurance et les mutuelles, les maisons de retraite (EHPAD), les services de santé au travail, ou les fédérations sportives.
Stockage de données en interne et stockage mutualisé : les parties qui collectent et traitent des données de santé sans hébergement tiers ne sont pas soumises à l'agrément. Ainsi, un établissement hospitalier qui stockerait les données de ses patients sur ses propres serveurs en interne n'est pas concerné par l'obligation d'agrément. En revanche, l'établissement qui stocke ses propres données de santé, mais également celles d'établissements ou de médecins tiers, agira pour ces données, en qualité d'hébergeur tiers, soumis à l'agrément.
Les conditions de l'agrément : les conditions de l'agrément n'ont pas changé avec la loi du 26 janvier 2016. Celles-ci ont été fixées par deux décrets de 2006 et 2011, codifiés aux articles R.1111-9 et suivants du CSP, et précisées par l'ASIP-Santé. *(Loi n°2016-41 du 26 janvier 2016 de modernisation de notre système de santé et article L.1111-8 du Code de la santé publique)*

DROIT DES AFFAIRES

RÉGLEMENTATION

Règlementation UE – Adoption de la directive sur la protection du secret des affaires par le Parlement européen

Le Parlement européen a adopté la directive pour la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) le 14 avril 2016. La directive doit encore être votée par le Conseil de l'UE. Les Etats-membres auront ensuite deux ans pour transposer ce texte en droit interne. L'harmonisation sera minimale puisque les Etats pourront prévoir une protection plus étendue que celle définie dans la directive.

Pour rappel, l'objectif de la directive est d'assurer une protection améliorée et harmonisée des secrets d'affaires des entreprises en luttant contre l'espionnage industriel et le vol de données. Il s'agit des informations secrètes, c'est-à-dire, non publiques, qui présentent une valeur compétitive et commerciale pour l'entreprise et qui ont fait l'objet de mesures destinées à les garder secrètes, telles que les informations d'ordre stratégique (business plan), commerciales (fichiers clients), techniques (savoir-faire) ou marketing (plans de communication).

La directive prévoit notamment :

- la possibilité de prévenir et de réprimer l'obtention, la divulgation et l'usage illicites d'un secret d'affaires appartenant à autrui. Ainsi, engageront leur responsabilité, non seulement les personnes qui ont obtenu ou capté le secret de façon illicite, mais aussi les personnes qui en feront un simple usage dès lors qu'elles savaient ou ne pouvaient pas ignorer l'origine illicite de l'information ;
- la possibilité d'obtenir - sous certaines conditions - des mesures provisoires et rapides (interdiction, saisie des produits litigieux) dans le cas d'atteinte avérée ou imminente à un secret ;
- l'aménagement des règles de procédure habituelles afin d'éviter la divulgation du secret dans le cadre de la procédure elle-même (huis clos, etc.).

Les sociétés victimes d'actes d'espionnage industriel ou de vol de données devront établir un préjudice chiffré justifiant l'allocation de dommages et intérêts. La réparation sera uniquement civile, la directive ne comportant pas de dispositions pénales.

Le texte prévoit néanmoins des limites à cette protection. Ainsi, l'obtention, l'utilisation ou la divulgation d'informations sont considérées comme licites si cela résulte d'une découverte ou d'une création indépendante, d'une opération d'ingéniérie inverse (reverse engineering) ou encore si cela procède de l'exercice du droit des représentants des salariés ou d'autres usages commerciaux honnêtes.

Cette directive a fait l'objet de nombreuses critiques concernant le droit d'investigation des journalistes et les lanceurs d'alerte. Le texte a été complété afin de protéger le droit à la liberté d'expression et d'information (art. 5). Cependant, les lanceurs d'alerte ne font pas l'objet d'une protection particulière. Celle-ci doit faire l'objet d'une directive séparée.

A noter que les Etats-Unis, dont plusieurs états fédérés disposent déjà de lois protégeant pénalement contre le vol d'informations, viennent d'adopter une loi fédérale de protection des secrets d'affaires (Defend Trade Secrets Act – DTSA). *(Proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure - Analysis of the final compromise text with a view to agreement, Interinstitutional File: 2013/0402 (COD), Brussels, 18 December 2015.)*

Droit de la consommation - Allongement de la garantie légale de conformité

Le vendeur professionnel doit livrer un produit conforme au contrat. Le consommateur bénéficie de la part du vendeur professionnel de deux garanties légales (obligatoires) : la garantie légale de conformité et la garantie légale des vices cachés. Le vendeur peut également proposer une garantie contractuelle supplémentaire et facultative.

La garantie légale de conformité vise à protéger le consommateur contre tout défaut de conformité du produit vendu par le professionnel (B-to-C). Jusqu'à présent, la garantie de conformité était de 6 mois à partir de la délivrance du bien. Pendant ce délai, le consommateur peut invoquer un défaut de conformité, présumé exister au moment de l'achat.

La loi « Hamon » du 17 mars 2014 a modifié le régime applicable à la garantie légale de conformité, en allongeant ce délai de 6 à 24 mois (sauf pour les biens d'occasion pour lesquels le délai est de 6 mois). Cette modification est entrée en vigueur le 18 mars 2016. Le nouvel article L.211-7 du Code de la consommation est désormais rédigé comme suit :

« *Les défauts de conformité qui apparaissent dans un délai de vingt-quatre mois à partir de la délivrance du bien sont présumés exister au moment de la délivrance, sauf preuve contraire.*

Pour les biens vendus d'occasion, la durée mentionnée au premier alinéa du présent article est ramenée à six mois.
Le vendeur peut combattre cette présomption si celle-ci n'est pas compatible avec la nature du bien ou le défaut de conformité invoqué. » *(Loi n°2014-344 du 17 mars 2014 et article L.211-7 du Code de la consommation)*

JURISPRUDENCE

DGCCRF– Plusieurs entreprises sanctionnées pour non-respect des délais de paiement
Le délai de paiement entre professionnels est prévu à l'article L.441-6 I du code de commerce qui dispose que ce délai *« (…) ne peut dépasser soixante jours à compter de la date d'émission de la facture. Par dérogation, un délai maximal de quarante-cinq jours fin de mois à compter de la date d'émission de la facture peut être convenu entre les parties, sous réserve que ce délai soit expressément stipulé par contrat et qu'il ne constitue pas un abus manifeste à l'égard du créancier*. »
Dans sa conférence de presse du 23 novembre 2015, Emmanuel Macron, ministre de l'Économie, avait annoncé un renforcement de son action dans la lutte contre le non-respect des délais de paiement, les contrôles étant réalisés par la DGCCRF. Depuis octobre 2015, 12 entreprises ont été sanctionnées pour non-respect des délais de paiement, dont 4 en mars 2016. Les dernières amendes imposées par la DGCCRF vont de 50.000€ à 375.000€, soit 50.000€ à l'encontre de la société Générix (décision du 8 mars 2016), 375.000€ à l'encontre de la société Alstom Grid (décision du 18 mars 2016), 160.000€ à l'encontre de la société Atos Intégration (décision du 18 mars 2016) et 375.000€ à l'encontre de la société réunionnaise de radiotéléphone (SRR) (décision du 22 mars 2016). On constate ainsi que la DGCCRF n'hésite pas à appliquer les sanctions maximum aux entreprises ne respectant pas leurs engagements en matière de délais de paiement. Ces décisions sont néanmoins susceptibles de recours devant les juridictions. *(voir site economie.gouv.fr/dgccrf/sanctions-delais-paiement)*

DROIT FISCAL ET E-COMMERCE

RÉGLEMENTATION

TVA– Abaissement du seuil de perception de TVA auprès des sites de e-commerce étrangers
La loi de finance 2016 a modifié l'article 258B du code général des impôts concernant la TVA intracommunautaire pour les biens achetés à distance.
Entrée en vigueur le 1er janvier dernier, cette disposition a pour effet d'abaisser le seuil du montant des ventes en ligne à partir duquel le commerçant établi dans un autre Etat-membre doit appliquer les taux de TVA français. Le seuil à partir duquel un site de e-commerce européen est soumis à la TVA française passe ainsi de 100.000 euros à 35.000 euros par année civile. Ces dispositions s'appliquent aux sites de e-commerce B-to-C établis dans un pays de l'Union autre que la France, mais ayant une activité de vente à des consommateurs résidant en France. Les principaux pays concernés sont les pays limitrophes de la France (Benelux notamment). En pratique, les sites de e-commerce concernés doivent s'assurer que les prix affichés sont corrects (en fonction du pays d'origine du client), que la société est dûment immatriculée auprès du DRESG et qu'elle fait les déclarations périodiques réglementaires. Cela démontre une fois encore l'absence d'harmonisation fiscale au niveau européen. *(Loi n°2015-1785 du 29 décembre 2015 dite « loi de finance 2016 » et modification de l'article 258B du code général des impôts)*

INTERNATIONAL

RÉGLEMENTATION

Commerce international– Ratification de la Convention de la Haye sur les clauses attributives de juridiction par l'Union européenne et Singapour
Le 11 juin 2015, l'Union européenne a ratifié la Convention de la Haye du 30 juin 2005 sur les accords d'élection de for (ou clauses attributives de juridiction), suivie par Singapour le 14 avril 2016. La clause attributive de juridiction permet aux parties à un contrat commercial international de désigner une juridiction compétente pour tout litige relatif à ce contrat. La Convention de la Haye vient compléter le règlement de Bruxelles I bis (règlement UE n°1215/2012) qui assure au sein de l'UE l'efficacité des clauses attributives de juridiction ainsi que la reconnaissance et l'exécution des jugements des autres Etats-membres en supprimant l'exequatur entre ces Etats. L'objectif de la Convention est de garantir

la prévisibilité en cas de litige puisque la juridiction désignée au contrat et la décision en découlant sera reconnue et exécutée à l'étranger. Par exemple, une clause contractuelle qui désignerait de manière exclusive les tribunaux singapouriens signifie que ceux-ci devront accepter cette désignation. En revanche, en cas de désignation des tribunaux d'un pays tiers, les tribunaux singapouriens ne pourront se reconnaître compétents. Enfin, le jugement rendu par un tribunal d'un pays membre de la Convention de la Haye sera reconnu et exécuté à Singapour, sans nécessiter de procédure d'exequatur. Ces dispositions ne concernent que les contrats commerciaux internationaux, à l'exclusion de certains domaines (telles que les affaires de liquidation, le droit de la concurrence, la propriété intellectuelle). La Convention de la Haye est en cours de ratification aux Etats-Unis, au Mexique et en Ukraine. Plusieurs autres pays étudient leur adhésion à la Convention, notamment : l'Argentine, l'Australie, le Canada, la Nouvelle Zélande et la Russie. *(Convention de la Haye du 30 juin 2005 sur les accords d'élection de for / Hague Convention on Choice of Court Agreements)*

VIE DU CABINET

EQUIPE

Après plusieurs années de collaboration, Betty Sfez a quitté le Cabinet fin mars pour de nouveaux projets.

DÉMÉNAGEMENT

Le Cabinet déménage à Paris et Singapour.

Nos nouveaux locaux sont situés depuis le 1er avril - **5, rue Tronchet – 75008 Paris**
à partir du 1er juillet - **30 Saunders Road – Singapore 228270**

PUBLICATIONS ET PRÉSENTATIONS

Vous trouverez sur le Blog du Cabinet (http://dwavocat.blogspot.com/), toutes nos dernières publications :
- Hébergement de données de santé : les modifications apportées par la loi du 26 janvier 2016
- Transferts de données personnelles vers les Etats-Unis : un bouclier de protection des données pour remplacer la sphère de sécurité

Nos dernières publications sur notre blog en anglais (http://dwavocatit.blogspot.com/)
- Legal requirements applicable to importing or exporting encryption software and equipment in/from France
- Personal data transfers from the EU to the US after the cancellation of Safe Harbor by the CJEU

Directeur de la publication : Bénédicte DELEPORTE
Editeur : DELEPORTE WENTZ AVOCAT - 5, rue Tronchet – 75008 Paris - Tel 01.40.17.95.86