LA LETTRE DU CABINET

TECHNOLOGIES DE L'INFORMATION

EDITO

Nous avons le plaisir de vous adresser le sixième numéro de notre Newsletter.

Cette Newsletter est organisée autour des thématiques suivantes : Informatique, Internet, Protection des données personnelles, Propriété intellectuelle, Cybercriminalité et enfin Vie du Cabinet. Nous souhaitons par ce moyen vous informer des derniers développements du droit des technologies de l'information, en matière réglementaire et jurisprudentielle notamment.

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

Bonne lecture !

SOMMAIRE

INFORMATIQUE

1. OPEN DATA ET BASES DE DONNÉES

Jurisprudence – Refus de la libre réutilisation des données publiques sur le fondement du droit des bases de données
Dans cette affaire, le Conseil général de la Vienne avait refusé de fournir à la société Notrefamille.com, exploitant un site de généalogie, les archives numérisées de cahiers de recensement, pour une réutilisation commerciale. La délibération du Conseil général ne permettait que la consultation sur place des archives départementales, et n'autorisait la cession des fichiers numérisés de certains fonds d'archives publiques que lorsque la cession était nécessaire à l'accomplissement d'une mission de service public, qu'elle était gratuite et effectuée dans le cadre d'une convention précisant les limites de la réutilisation. Estimant que ces règles restrictives contrevenaient à la loi du 17 juillet 1978, qui a instauré un droit de réutilisation des informations publiques, la société avait déposé une requête en annulation de cette délibération. Elle invoquait le fait que ces règles faisaient obstacle à son projet, consistant à exporter les données numérisées selon des "*techniques d'aspiration des données à partir du site internet du département"* pour les intégrer à ses bases de données, et soutenait en outre, qu'il n'existait aucun motif d'intérêt général de nature à justifier les restrictions. Par décision du 31 janvier 2013, le Tribunal administratif de Poitiers a refusé d'annuler la délibération du Conseil général. Le Tribunal a estimé que le Conseil général était producteur de base de données, au sens des articles L.342-1 et suivants du Code de la propriété intellectuelle, à raison des investissements substantiels qu'il avait engagés dans la création des fichiers numérisés (la numérisation des documents d'archives avait duré huit ans et avait coûté environ 200.000€). Or, le Tribunal rappelle que ce droit n'impose pas au producteur de délivrer une licence. En principe, seul le droit de propriété intellectuelle d'un tiers peut justifier un refus de fournir des informations publiques, et non celui de la personne qui détient les informations. Sans doute le statut spécifique du service d'archives départementales a-t-il justifié la position du Tribunal. En effet, les services d'archives départementales relèvent de la catégorie des services culturels, lesquels ont le droit de fixer leurs propres conditions de réutilisation de leurs informations publiques. *(Tri. Adm. Poitiers, 2nd ch., 31 janvier 2013, Notrefamille.com / Département de la Vienne).*

2. CONTREFAÇON DE LOGICIEL

Jurisprudence – Rappel des conditions de recours à l'expertise en cas de contrefaçon de logiciel
En application de l'article 9 du Code de procédure civile, "*il incombe à chaque partie de prouver conformément à la loi les faits nécessaires au succès de sa prétention*". En matière de contrefaçon de logiciel, le demandeur doit ainsi dans un premier temps, identifier les logiciels respectifs, décrire les caractéristiques du logiciel sur lequel il revendique des droits ainsi que son caractère original, et celles du logiciel incriminé et dans un deuxième temps, identifier les éléments contrefaisants dans le logiciel du défendeur. Dans une affaire opposant un ayant droit aux sociétés PayPal et eBay, le tribunal de grande instance de Paris a jugé, le 8 février 2013, que "*si en matière de contrefaçon de logiciel, le recours à une expertise se justifie pour effectuer des comparaisons des logiciels ou même pour décrire dans le détail (…) les caractéristiques du logiciel revendiqué, comme celles du logiciel contesté, il ne saurait en revanche pallier l'absence totale, comme ici, de présentations des caractéristiques et de l'originalité du logiciel (…)."* Constatant l'absence des moyens de fait et de droit qui auraient dû permettre aux défendeurs de connaître précisément les comportements fautifs reprochés et de se défendre, le tribunal a donc purement et simplement annulé les assignations. *(TGI Paris, 3é ch., 2é section, 8 février 2013, M. José M. / sociétés PayPal et eBay)*

INTERNET

1. E-COMMERCE

Réglementation – La nouvelle réglementation française portant sur la vente de médicaments sur internet

Bien que jusqu'à présent le Code de la santé publique (CSP) n'interdisait pas expressément la vente de médicaments en ligne, ce mode de distribution n'était pas pour autant autorisé dans la mesure où les dispositions légales ne permettaient pas en pratique d'utiliser ce canal de vente en France. Avec la directive européenne du 8 janvier 2011 autorisant la vente de médicaments sur internet, la plupart des pays voisins de la France avaient adopté une législation autorisant ce type de vente. Depuis fin décembre 2012, la vente de médicaments sur internet est encadrée par le droit français. La vente en ligne de médicaments est soumise à plusieurs conditions, notamment : (i) elle est réservée aux pharmaciens titulaires d'une officine et aux médicaments dits de "médication officinale" pouvant être présentés "en accès direct" au public en officine, dont la liste est fixée par le DGARS et ayant obtenu une autorisation de mise sur le marché. L'interdiction de vente en ligne est donc maintenue pour les médicaments délivrés sur ordonnance ; (ii) elle est soumise au dépôt d'une demande d'autorisation auprès du directeur général de l'Agence Régionale de Santé (DGARS) dans le ressort duquel est située l'officine et à l'information du Conseil de l'Ordre dont le pharmacien relève. Cependant, à la suite de l'adoption de l'ordonnance de décembre 2012, le Conseil d'Etat a été saisi d'un recours pour excès de pouvoir, déposé par un pharmacien estimant que la nouvelle réglementation française était plus restrictive que le droit européen. Dans une décision de février 2013, le Conseil d'Etat a constaté que le droit européen faisait une distinction entre les médicaments à prescription médicale, ne pouvant être vendus sur internet, et ceux non soumis à prescription (médicaments "OTC" ou "over the counter"), pouvant être vendus sur internet. Le Conseil d'Etat relève que la nouvelle réglementation française ne limite pas l'interdiction de vente en ligne aux seuls médicaments soumis à prescription obligatoire mais qu'elle étend cette interdiction à tous les médicaments non soumis à prescription n'étant pas des médicaments dits de "médication officinale". Par conséquent, le Conseil a ordonné la suspension des dispositions légales françaises n'autorisant la vente en ligne qu'aux seuls médicaments de médication officinale. Par le biais de cette décision, le Conseil d'Etat ouvre le commerce en ligne à tous les médicaments vendus sans ordonnance. *(Ordonnance n°2012-1427 du 19 décembre 2012 relative au renforcement de la sécurité de la chaîne d'approvisionnement des médicaments, à l'encadrement de la vente de médicaments sur internet et à la lutte contre la falsification de médicaments. Décret d'application n°2012-1562 du 31 décembre 2012 et Conseil d'Etat, 14 février 2013, Ord. N°365.946, M.L).*

Jurisprudence - Site d'enchères par voie électronique et conditions d'agrément du CVV

Cette affaire opposait une société exploitant un site d'enchères par voie électronique spécialisé dans la vente de véhicules d'occasion au Conseil des ventes volontaires de meubles aux enchères publiques (CVV). Le CVV avait engagé une action en justice pour que soit interdite la poursuite de l'activité de la société, au motif qu'elle exerçait sans son agrément. Selon le CVV, la société devait obtenir un agrément puisqu'elle agissait, conformément à l'article L.321-3 du Code de commerce, comme mandataire des propriétaires des biens mis en vente et qu'il y avait adjudication des biens. Toutefois, par décision du 19 février 2013, la Cour de cassation a jugé que le site internet n'était pas soumis à la réglementation des ventes volontaires de meubles aux enchères publiques et ne devait pas de ce fait obtenir un agrément : la société n'était qu'un intermédiaire qui mettait en relation vendeurs et acheteurs, en qualité de courtier. En outre, la Cour a constaté que si la vente était proposée au plus offrant, celui-ci devait néanmoins, après la clôture de la vente, procéder seul, sans l'intervention de la société, à une nouvelle manœuvre pour confirmer son accord. Ainsi, le bien mis en vente n'était pas adjugé à l'issue des enchères. Le dernier enchérisseur restait libre de ne pas contracter. *(Cass. civ. 1e, 19 février 2013, n°11-23.287).*

Jurisprudence - Condamnation de la revente en ligne des places de spectacles sans autorisation des producteurs

Dans cette affaire, deux sociétés productrices de concerts et spectacles étaient opposées à l'exploitant d'un site internet de vente de billets de concert. Ayant constaté la vente, sans leur autorisation, de billets de concerts qu'elles produisaient, les deux sociétés ont assigné l'exploitant du site litigieux afin d'interdire la commercialisation de ces billets. Depuis une loi du 12 mars 2012, le fait "*de vendre, d'offrir à la vente ou d'exposer en vue de la vente ou de la cession ou de fournir les moyens en vue de la vente ou de la cession des titres d'accès à une manifestation sportive, culturelle ou commerciale ou à un spectacle vivant, de manière habituelle et sans l'autorisation du producteur, de l'organisateur ou du propriétaire des droits d'exploitation de cette manifestation ou de ce spectacle"* est pénalement sanctionné d'une amende de 15.000€. Par ordonnance de référé en date du 13 mars 2013, le tribunal de commerce de Nanterre a condamné l'exploitant du site web : (i) à retirer tout

contenu relatif aux concerts litigieux, sous astreinte de 1.000€ par jour de retard, et (ii) à publier, sur sa page d'accueil, une partie de la décision de justice et laisser en ligne cet encart pendant trois mois, sous astreinte de 500€ par jour de manquement constaté. *(Trib. Com. Nanterre, Ordonnance de référé 13 mars 2013, TS3, Nous / Yamson Event).*

2. RÉSEAUX SOCIAUX

Jurisprudence – Twitter enjoint de communiquer les données d'identification d'un internaute ayant créé un faux profil

Un internaute avait découvert qu'un faux profil public avait été créé avec ses nom, prénom, état civil et images sur le réseau de micro blogging Twitter. L'usurpateur d'identité avait posté près de 5000 tweets et communiqué par SMS avec des "followers". Plusieurs demandes de suppression du faux profil avaient été adressées à la société Twitter, sans succès. L'internaute dont l'identité avait été usurpée a donc assigné la société Twitter en référé afin qu'elle supprime le faux profil et communique les éléments d'identification de son auteur. La société Twitter, qui a attendu la veille de l'audience des plaidoiries pour supprimer le profil litigieux, a invoqué le fait que les données d'identification de l'usurpateur étaient stockées aux Etats-Unis et qu'elle les communiquerait uniquement sur commission rogatoire pénale internationale. Par décision du 4 avril 2013, le Tribunal de grande instance de Paris a considéré que cette commission rogatoire n'était pas nécessaire puisque la société Twitter était en mesure de fournir ces données. Par conséquent, le Tribunal a fait injonction à Twitter de communiquer les données d'identification de l'usurpateur, sous astreinte de 500€ par jour de retard. *(TGI Paris, Ordonnance de référé 4 avril 2013, Mathieu S. / Twitter Inc.).*

PROTECTION DES DONNÉES PERSONNELLES

1. LÉGISLATION EUROPÉENNE

Règlement – La prochaine réforme de la réglementation de la protection des données personnelles en Europe

La directive européenne sur la protection des données personnelles date d'octobre 1995. Pour prendre en compte les évolutions, notamment le développement des usages d'internet et des réseaux sociaux, mais également des technologies utilisant des données personnelles, la Commission européenne a publié le 25 janvier 2012, une proposition de règlement relatif à la protection des données personnelles. Les deux grands axes à retenir de ce projet sont un renforcement des droits des personnes concernées sur leurs données, notamment en matière d'information préalable, de consentement, de droit d'opposition et de droit à l'oubli, et en parallèle, un renforcement des obligations des entreprises en matière de collecte et de traitement des données personnelles, avec des sanctions alourdies en cas de non-respect de la nouvelle réglementation. Notamment, les formalités déclaratives seraient simplifiées, et pour certaines catégories de traitements, supprimées. En contrepartie, les entreprises devront déployer des procédures internes pour assurer le respect des principes de protection des données personnelles. Ces procédures, créant une véritable politique de gouvernance en matière de protection des données personnelles, comprendront : audits, registres, études d'impact, prise en compte de la protection des données dès la conception des nouveaux produits et services (mise en œuvre des principes de "Privacy by design" ou de "Privacy by default"), codes de conduite, etc. La proposition a fait l'objet de nombreuses réserves et critiques depuis sa première publication et a donné lieu à plusieurs résolutions, amendements ou avis mettant en relief ses points faibles ou manquements. Les négociations entre le Parlement, la Commission et le Conseil européen débuteront à partir de mai 2013 en vue d'obtenir un compromis et un texte final d'ici le début de l'année prochaine. Une fois entré en vigueur, le règlement sera d'application immédiate et uniforme dans l'ensemble de l'Union européenne et viendra remplacer la directive de 1995 et les différentes lois nationales de protection des données personnelles. *(Proposition de règlement du parlement européen et du conseil 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 du 25 janvier 2012, (2012/0011 (COD)).*

2. POUVOIRS DE CONTRÔLE ET DE SANCTION DE LA CNIL

Contrôle CNIL – Programme des contrôles de la Commission pour l'année 2013

La CNIL a réalisé 458 contrôles de conformité et a reçu 6000 plaintes en 2012. Le 28 février dernier, la CNIL a adopté son programme des contrôles pour l'année 2013. Cette année, la Commission a pour objectif d'effectuer 400 contrôles de conformité, dont 1/4 porteront sur les dispositifs de vidéosurveillance. En outre, la CNIL a fixé deux axes prioritaires : la protection des personnes

vulnérables, et la coopération internationale entre les autorités de protection des données. En sus, la Commission a déterminé les thématiques principales suivantes : le traitement des données par les instituts de sondage ; les données traitées dans le cadre de l'internet en libre accès ; le traitement par les collectivités locales des données relatives aux difficultés sociales des personnes ; les données des personnes détenues en établissements pénitentiaires et le contrôle des services opérationnels de police et de gendarmerie, qui faisait déjà partie des priorités dans la programme 2012. *(Communiqué CNIL du 19 mars 2013 intitulé "Protection des personnes vulnérables et coopération internationale : deux axes majeurs au programme des contrôles 2013").*

Délibération CNIL – L'utilisation d'un dispositif de vidéosurveillance disproportionné
Par délibération du 3 janvier 2013, la formation restreinte de la CNIL a sanctionné le placement sous vidéosurveillance permanente d'agents de sécurité au sein d'un PC sécurité situé dans un immeuble parisien. Saisie d'une plainte émanant des agents de sécurité, la CNIL a mis en demeure le syndicat de copropriété. Face à leur refus, la Commission a effectué un contrôle sur place. Ce contrôle a révélé que le dispositif mis en place avait non pas pour objectif de veiller à la protection des biens et des personnes de l'immeuble, mais de contrôler en permanence le travail des agents de sécurité. La CNIL a jugé le dispositif disproportionné et a condamné le syndicat à une sanction d'un euro symbolique, assortie d'une injonction de mettre un terme au caractère continu du traitement *(Délibération de la formation restreinte de la CNIL 2012-475 du 3 janvier 2013 Syndicat des copropriétaires des "Arcades des Champs Elysées").*

Communiqué CNIL – L'utilisation d'un dispositif de cybersurveillance (keylogger) des salariés disproportionné
Dans un communiqué du 20 mars 2013, la CNIL a rappelé que la surveillance des salariés par l'employeur ne doit pas porter une atteinte disproportionnée à leurs droits. Or, tel est le cas des dispositifs "keylogger", permettant de surveiller de façon constante et permanente l'activité professionnelle (et personnelle) des salariés, depuis leur poste informatique. Ces logiciels se lancent automatiquement au démarrage de la session de l'utilisateur de l'ordinateur à l'insu du salarié et permettent d'enregistrer toutes les actions effectuées par les salariés sur leur ordinateur. Toute frappe saisie et tout écran ou pages web consultés sont enregistrés avec un horodatage. En outre, selon le type de logiciels, des alertes et des rapports d'activité peuvent être adressés automatiquement à l'employeur ayant installé le dispositif. Aussi, la CNIL affirme que le recours à un tel dispositif ne peut être justifié qu'en cas d'impératifs forts de sécurité et moyennant une information des personnes concernées. *(Communiqué CNIL du 20 mars 2013 intitulé "Keylogger : des dispositifs de cybersurveillance particulièrement intrusifs").*

3. CYBERSURVEILLANCE DES SALARIÉS

Jurisprudence – Une clé USB utilisée au bureau est présumée être à usage professionnel
Dans une décision du 12 février 2013, la Cour de cassation a affirmé que l'employeur peut accéder au contenu, non identifié comme personnel, d'une clé USB connectée à l'ordinateur mis à la disposition du salarié par l'employeur. En l'espèce, une salariée avait été licenciée pour faute grave après que son employeur eut constaté l'enregistrement, sur une clé USB connectée à l'ordinateur professionnel de l'intéressée, d'informations confidentielles relatives à l'entreprise et de documents personnels de collègues et dirigeants de l'entreprise. La Cour d'appel avait considéré le licenciement dépourvu de cause réelle et sérieuse, au motif que le moyen de preuve invoqué par l'employeur était illicite. En effet, la clé USB était la clé personnelle de la salariée et la salariée, absente lorsque sa clé a été consultée, n'avait pas été informée de son droit d'en refuser le contrôle ou d'exiger la présence d'un témoin. Toutefois, la Cour de cassation a cassé l'arrêt d'appel au motif que dès lors que la clé USB était connectée à l'ordinateur mis à la disposition de la salariée par l'employeur dans le cadre de son travail, elle était présumée être utilisée à des fins professionnelles. L'employeur pouvait avoir accès aux fichiers non identifiés comme personnels qu'elle contenait, et ce hors de la présence de la salariée. (*Cass. soc., 12 février 2013, n°11-28.649*).

Jurisprudence – Les emails d'un salarié, consultables depuis une boîte email mise à sa disposition par l'employeur, sont présumés professionnels
Dans une décision du 16 mai 2013, la Cour de cassation a affirmé que l'employeur pouvait prendre connaissance des messages personnels émis et reçus par les salariés, grâce à l'outil informatique mis à leur disposition pour leur travail. En l'espèce, une société avait assigné un de ses anciens salariés, et son nouvel employeur, pour détournement de clientèle et concurrence déloyale pendant l'exécution du préavis du salarié. Au cours de la procédure, les défendeurs ont invoqué le fait que le constat

d'huissier versé aux débats par la société demanderesse, ne constituait pas un mode de preuve licite. Ce constat avait été réalisé à partir de la boîte email de l'ancien salarié, dont l'adresse électronique ne comportait pas le nom de la société, et hors la présence du salarié concerné. Si le salarié utilisait cette messagerie dans un cadre professionnel, il y recevait également des messages personnels, protégés par le secret des correspondances et le droit au respect de la vie privée. Cependant, la Cour de cassation a jugé que "*les courriels adressés et reçus par le salarié à l'aide de l'outil informatique mis à sa disposition par l'employeur pour les besoins de son travail sont présumés avoir un caractère professionnel, en sorte que l'employeur est en droit de les ouvrir hors la présence de l'intéressé, sauf si le salarié les identifie comme personnels*." En conséquence, tous les fichiers et emails édités et reçus par un salarié, à l'aide de l'outil informatique mis à sa disposition par l'employeur, peuvent être consultés par l'employeur, sauf s'ils sont identifiés comme personnels. *(Cass. soc., 16 mai 2013, n°12-11866).*

PROPRIÉTÉ INTELLECTUELLE

NOMS DE DOMAINE

Jurisprudence – Utilisation de la dénomination et du nom de domaine d'un concurrent via le service de référencement Google Adwords

La Cour d'appel de Paris avait condamné, pour concurrence déloyale et publicité trompeuse, une société qui utilisait la dénomination et le nom de domaine de l'un de ses concurrents à titre de mot-clé sur internet pour générer un lien commercial, via le service Google Adwords. La Cour d'appel avait également retenu la responsabilité de la société Google. La Cour de cassation a cassé l'arrêt d'appel au motif que la Cour avait retenu, à tort, la responsabilité du moteur de recherche. Les juges ont en effet considéré que la société Google devait bénéficier du régime de responsabilité aménagée des prestataires techniques, prévu par la loi dite LCEN. En outre, la Cour de cassation a reproché aux juges du fond de ne pas avoir recherché l'existence d'un risque de confusion entre les sites web litigieux, rappelant le principe selon lequel le démarchage de la clientèle d'autrui est licite s'il n'est pas accompagné d'actes déloyaux. Il appartenait donc à la Cour d'appel de rechercher des éléments factuels de nature à établir la déloyauté. Dès lors, la reprise à titre de mot-clé de la dénomination, du nom de domaine et de la marque d'un concurrent n'est pas en soi fautif. (*Cass. com., 29 janvier 2013, n°11-21.011 et n°11-24.713*).

Jurisprudence – Conflit entre deux noms de domaine descriptifs et génériques : absence de concurrence déloyale

La Cour d'appel de Bastia a rendu le 20 mars 2013 une décision conforme à la jurisprudence actuelle en matière de noms de domaine. Dans cette affaire, le titulaire du nom de domaine "mariagesencorse.com" avait assigné en concurrence déloyale, le titulaire du nom de domaine "mariageencorse", enregistré postérieurement. Le demandeur réclamait que la société concurrente soit condamnée (i) à ne plus utiliser le nom de domaine litigieux, (ii) à procéder aux formalités de transfert du nom de domaine au profit du demandeur et (iii) à payer des dommages et intérêts pour préjudice commercial et moral. Le demandeur a été débouté de ses demandes. En effet, la Cour d'appel de Bastia rappelle qu'en vertu du principe de la libre concurrence, seul le titulaire d'un nom de domaine distinctif peut se prévaloir d'une protection. Or, la Cour constate que le nom de domaine du demandeur "*est une juxtaposition d'un mot usuel et d'une provenance ou d'un lieu géographique, qui évoque l'objet et le lieu de l'activité de son titulaire*". Aussi, la Cour conclut que "*même s'il existe une confusion dans l'esprit des internautes,* (les demandeurs) *ne peuvent valablement se prévaloir de la protection d'un nom de domaine, s'agissant d'un nom de domaine générique et descriptif de l'activité de la société* (…)". En conséquence, l'exploitation par la société concurrente d'un nom de domaine similaire à celui du demandeur ne constitue pas une faute. (*CA Bastia, ch. civ. B, 20 mars 2013, Angela A. c/ Iris Média et autres*).

CYBERCRIMINALITÉ

CYBERSÉCURITÉ

Politique européenne - Développement d'une politique européenne de la sécurité des réseaux et des systèmes d'information

Face à l'accroissement du nombre d'attaques informatiques, l'Union européenne a pris la décision de poser les contours d'un cadre commun à tous les Etats membres en matière de sécurité des réseaux numériques, de lutte contre la criminalité en ligne et de protection des consommateurs. Les

institutions européennes ont publié, le 7 février 2013, une stratégie commune de cybersécurité ainsi qu'une proposition de directive instaurant des mesures visant à assurer un niveau élevé commun de sécurité des réseaux et de l'information (SRI). Ces deux textes fixent les mesures proposées par la Commission européenne, les objectifs à atteindre par les Etats membres et les obligations qui viendront peser sur les entreprises et administrations publiques. La stratégie de la Commission repose sur cinq axes : (i) parvenir à la cyber-résilience, (ii) faire reculer considérablement la cybercriminalité, (iii) développer une politique et des moyens de cyberdéfense liés à la politique de sécurité et de défense commune (PSDC), (iv) développer les ressources industrielles et technologiques en matière de cybersécurité, et enfin (v) instaurer une politique internationale de l'Union européenne cohérente en matière de protection du cyberespace. La proposition de Directive impose notamment aux entreprises de notifier à l'autorité compétente (l'ANSSI en France), les incidents (perte, vol, piratage de données, etc.) qui ont un impact significatif sur la sécurité des services qu'elles fournissent. Cette proposition de directive devrait, selon l'avancée des débats, être définitivement adoptée d'ici 2014. Le texte définitif devra ensuite faire l'objet d'une transposition dans les droits nationaux dans les 18 mois suivant l'adoption de la directive, soit entre fin 2015 et mi-2016. (*Communication conjointe au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions. Proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union, Bruxelles, le 7.2.2013 COM(2013) 48 final 2013/0027 (COD)).*

VIE DU CABINET

1. PUBLICATIONS

Vous trouverez sur le **Blog du Cabinet** (http://dwavocat.blogspot.com/), toutes nos dernières publications, notamment :

- Marques de vins et alcools : ne pas négliger les règles relatives à la publicité,
- La nouvelle réglementation française sur la vente de médicaments sur internet,
- La prochaine réforme de la protection des données personnelles en Europe : vers un renforcement des droits des personnes et des obligations des entreprises,
- La directive DME2 relative aux établissements de monnaie électronique enfin transposée en droit français,
- Cybersécurité : le développement d'une politique européenne de la sécurité des réseaux et des systèmes d'information,
- Les soldes : des méthodes de vente encadrées, même sur internet,
- Cyberdéfense : la stratégie nationale dévoilée dans le dernier Livre blanc sur la Défense et la Sécurité nationale,
- Protection des données personnelles : qui est responsable en cas de manquement à la loi ?

2. CONFÉRENCES

Le Cabinet a participé aux salons **CARTES** et **E-commerce Asia expo & conference** les 27 et 28 mars derniers à Hong Kong et a donné une présentation sur le thème: "The major legal constraints applicable to international online sales", le 28 mars 2013 à Hong-Kong (http://www.cartes-asia.com et http://ecom-asia.com/).

Lors de ce déplacement, nous avons également noué des contacts avec des avocats chinois (Shanghai et Hong Kong) afin de pouvoir accompagner nos clients dans le cadre de leur développement international vers l'Asie.

Directeur de la publication : Bénédicte DELEPORTE
Editeur : DELEPORTE WENTZ AVOCAT - 7, rue de Madrid – 75008 Paris - Tel 01.44.90.17.10