LA LETTRE DU CABINET

TECHNOLOGIES DE L'INFORMATION

EDITO

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

Cette Newsletter est organisée autour des thématiques suivantes : Informatique, Protection des données personnelles, Propriété intellectuelle, Sécurité informatique, Innovation et enfin Publications 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.

Nous vous souhaitons une bonne lecture et un agréable été !

SOMMAIRE

ⓘ FLASH ACTUALITÉ DU CABINET

1. DELEPORTE WENTZ AVOCAT À SINGAPOUR... COMING SOON !

Notre Cabinet poursuit son développement à l'international à destination de l'Asie du sud-est, depuis Singapour, formidable porte d'entrée vers le marché asiatique. L'objectif est d'aider et accompagner nos clients français et européens dans leurs projets d'expansion vers cette région du monde, mais également de conseiller des entreprises du continent asiatique souhaitant développer leurs activités en Europe. Nous vous tiendrons informés des futures étapes de cette expansion dans les prochains numéros de notre newsletter.

2. PARTENARIAT AVEC ESSEC BUSINESS SCHOOL

Depuis quelques mois, Deleporte Wentz Avocat est partenaire de l'Incubateur ESSEC. Dans le cadre de cette collaboration, le Cabinet conseille les incubés et start-up du programme « ESSEC Ventures » souhaitant lancer une activité ayant une composante informatique ou internet. ESSEC Ventures est un dispositif lancé en 2000 afin d'accompagner les étudiants de l'ESSEC porteurs de projets d'entreprise. Il se compose d'un incubateur, d'une pépinière, d'un fonds d'amorçage dédié ainsi que d'événements rassemblant entrepreneurs et investisseurs.
(http://www.essec.fr/lessec/essec-ventures/a-propos-dessec-ventures.html)

INFORMATIQUE

1. MAINTENANCE

Jurisprudence – Limitation de la responsabilité du prestataire pour perte de données
Un groupement d'officines pharmaceutiques avait conclu un contrat de maintenance de l'ensemble de son parc informatique avec un prestataire. Lors d'une intervention du prestataire informatique dans les locaux du groupement, l'ensemble des données stockées sur les trois disques durs du serveur a été endommagé et perdu. Les différentes tentatives de récupération de ces données ont échoué. A cette occasion, le groupement s'est rendu compte que son système de sauvegarde des données n'était plus opérationnel depuis plusieurs mois, et que de ce fait, il ne disposait plus d'aucun moyen lui permettant de récupérer les données.
Le groupement, estimant avoir subi un préjudice s'élevant à près de 160.000€, a assigné le prestataire informatique en responsabilité. Le groupement invoquait que celui-ci avait manqué à ses obligations contractuelles, qu'il qualifiait de "résultat", et en conséquence, commis une faute lourde.
Dans une décision du 2 mai 2014, le Tribunal de commerce de Nanterre a rejeté en partie les prétentions du groupement. Le Tribunal a considéré que le contrat liant les parties était un simple contrat de "moyens", ne transférant sur le prestataire aucune autre responsabilité que celle d'assurer la maintenance des matériels et logiciels du groupement d'officines. Dans ces conditions, il n'est pas possible de justifier que le prestataire, qui par ailleurs n'était pas responsable des sauvegardes non effectuées par sa cliente, ait eu un comportement d'une exceptionnelle gravité, justifiant sa condamnation pour faute lourde.
Le Tribunal considère cependant que la responsabilité du prestataire ne peut être totalement écartée, mais que cette responsabilité est limitée, conformément à la clause contractuelle, à hauteur de 7.280€, cette somme correspondant au montant forfaitaire payé annuellement par le groupement. En conséquence, le Tribunal a condamné le prestataire au versement de ce montant forfaitaire, par application des conditions prévues au contrat. *(Trib. com. Nanterre, 2e ch., 2 mai 2014, Pharmodel c/ Tamaya Telecom, Patrick L.)*

2. DÉVELOPPEMENT DE SITE WEB

Jurisprudence – Condamnation du client pour rupture brutale et abusive du contrat
Une société spécialisée dans l'organisation d'événements avait conclu un contrat de développement de site web ainsi qu'un contrat de maintenance avec un prestataire. Un acompte avait été versé le jour de la signature du contrat par la cliente. Considérant que les conditions de réalisation du site web n'étaient pas satisfaisantes, la cliente a notifié la résolution des deux contrats par lettre recommandée et demandé le remboursement de l'acompte. Face au refus du prestataire, la cliente a décidé de l'attraire en justice. La demanderesse invoquait des retards dans le développement du site web et des défauts de fonctionnement du site (site inachevé ne correspondant pas aux exigences contractuelles

et nombreux bugs le rendant inutilisable, au point qu'elle a dû faire appel à un autre prestataire).
Dans un jugement du 25 avril 2014, le Tribunal de commerce de Marseille, se fondant sur les conditions d'exécution du projet, a débouté la demanderesse et l'a condamnée au versement d'un montant total supérieur à 9.000€. Selon le Tribunal, les retards invoqués par la cliente étaient dus, d'une part, à l'absence de communication par cette dernière des informations nécessaires à la réalisation du projet et, d'autre part, à la modification de sa stratégie, ayant nécessité de nombreuses adaptations au projet initial. Le Tribunal a par ailleurs relevé que la lettre notifiant la résolution du contrat aux torts du prestataire, n'était précédée d'aucune mise en demeure de pallier les différents manquements invoqués et mentionnait des fautes du prestataire, sans justification. Dès lors, le Tribunal a jugé que la résolution du contrat aux torts du prestataire n'était pas fondée.
Le Tribunal a donc condamné la demanderesse à payer au prestataire le solde du contrat de développement du site, les indemnités contractuelles, augmentés de dommages et intérêts pour manque à gagner relatif au contrat de maintenance et pour rupture brutale, et donc abusive, du contrat liant les deux sociétés. *(Trib. com. Marseille, 25 avril 2014, Open Up c/ Simpliciweb)*

3. PRESTATION D'EMAILING

Jurisprudence – Le non respect des modalités de résiliation du contrat relevé par le Tribunal
Une société, ayant pour activité le marketing en ligne, avait conclu un contrat avec un prestataire de routage pour l'acheminement de campagnes publicitaires par email. Le prestataire de routage a alors mis à la disposition du client sa plateforme de routage. Suite à des envois d'emails non sollicités à des consommateurs, qui s'en sont plaint, le client a demandé au prestataire de l'assister pour résoudre ces dysfonctionnements. Le prestataire a tenté, à plusieurs reprises, de pallier ces difficultés. Cependant, les dysfonctionnements étaient dus à une mauvaise utilisation de l'outil de routage par le client qui avait notamment refusé de suivre la formation proposée en début de contrat pour utiliser cet outil. Par la suite, faute d'accord entre les parties, le prestataire a notifié au client sa décision de résilier le contrat et a réclamé le paiement des factures restées impayées. Le client, contestant la rupture du contrat et les sommes facturées, a été assigné par le prestataire.
Dans une décision du 6 juin dernier, le Tribunal de commerce de Paris ne s'est pas prononcé sur les dysfonctionnements, mais sur les conditions de la suspension anticipée des prestations et du contrat. Le Tribunal a relevé que le prestataire avait effectivement la possibilité contractuelle de résilier le contrat par anticipation. Toutefois, il constate que le prestataire n'a pas respecté les formes stipulées au contrat (préavis de 30 jours pour remédier aux manquements contractuels). Le Tribunal, considérant ainsi que le contrat n'a pas été régulièrement et valablement résilié, déboute les parties de toutes leurs demandes ; il condamne néanmoins le client au règlement du solde des factures restées impayées avant la résiliation du contrat. *(Trib. com. Paris, 15e ch., 6 juin 2014, Emailvision c/ Ray Pro Mailing)*

4. CLOUD COMPUTING

Europe – Publication de lignes directrices en matière de contrats de niveau de service (SLA)
Le 26 juin 2014, la Commission a publié des lignes directrices en matière de Cloud computing ayant pour objet d'uniformiser les règles de terminologie et les paramètres applicables aux contrats de niveau de service (Service level agreement – SLA). Ces lignes directrices résultent des travaux réalisés par un groupe de sociétés et associations du secteur du Cloud (dont IBM, Microsoft, SAP, Telecom Italia, EuroCloud, Enisa, etc.). Selon la Commission, l'objectif de ces lignes directrices est d'aider les utilisateurs professionnels de "l'informatique en nuage" à vérifier que certains éléments essentiels figurent dans les contrats qu'ils concluent avec les fournisseurs de services Cloud. Les éléments essentiels identifiés sont : la disponibilité et la fiabilité du service, la qualité des services d'assistance, les niveaux de sécurité et les moyens de gérer les données stockées. *(Cloud service level agreement – Standardisation guidelines, 24/06/2014, et Communiqué de presse de la Commission européenne "De nouvelles lignes directrices pour aider les entreprises de l'Union à utiliser l'informatique en nuage" 26/06/2014)*

5. BASES DE DONNÉES

Jurisprudence – Un éditeur de bases de données sanctionné par l'Autorité de la concurrence pour abus de position dominante et refus de vente
La société Cegedim, spécialisée dans le secteur de la santé, édite des bases de données d'informations médicales (comprenant les coordonnées des médecins, adresses des cabinets et heures de visites) et des logiciels de gestion de clients (CRM) permettant d'exploiter ces informations. Cegedim est considérée comme leader sur le marché des bases de données médicales. La société

Euris édite un logiciel de CRM. Depuis 2007, Cegedim refusait de commercialiser sa base de données OneKey aux laboratoires pharmaceutiques utilisant le CRM Euris, Cegedim justifiant ce refus par l'existence d'un contentieux pour contrefaçon en cours avec Euris. Or, le refus de vente de sa base de données aux laboratoires pharmaceutiques utilisant le CRM Euris a empêché le développement de l'activité commerciale de cette société sur le marché des logiciels de CRM, les laboratoires étant alors obligés d'utiliser des outils concurrents. Au moins 400 laboratoires auraient été concernés par un tel refus de vente. Euris a ainsi perdu 70% de sa clientèle entre 2008 et 2012.
Euris a saisi l'Autorité de la concurrence, qui a rendu sa décision le 8 juillet 2014.
L'Autorité a reconnu un abus de position dominante de la part de la société Cegedim par son refus de vendre sa base de données aux laboratoires utilisateurs du CRM Euris. L'Autorité a condamné Cegedim au règlement d'une sanction pécuniaire de 5,7 millions d'euros, en prenant en compte la durée de l'infraction (avril 2007 à avril 2013), la gravité de la pratique (refus de vente) et le dommage à l'économie (exclusion d'un concurrent du marché). *(Décision de l'Autorité de la concurrence n°14-D-06 du 8 juillet 2014 relative à des pratiques mises en œuvre par la société Cegedim dans le secteur des bases de données d'informations médicales)*

PROTECTION DES DONNÉES PERSONNELLES

1. LÉGISLATION

Règlement européen – Une avancée dans la réforme de la protection des données personnelles
En mars 2014, le Parlement européen a modifié le projet de texte voté en janvier 2012 et adopté la proposition de règlement sur la protection des données personnelles en première lecture. La proposition de règlement amendée est venue modifier et compléter quelques dispositions du texte initial. Le texte adopté par le Parlement a été renvoyé en première lecture devant le Conseil de l'Union européenne.
Le 6 juin 2014, la réforme de la protection des données a connu une avancée, lors de la réunion des ministres européens chargés de la Justice. Les ministres ont entériné une orientation générale partielle portant sur deux "piliers" de la future réforme :
- *Sur la question de la portée territoriale de la réglementation*, les ministres ont confirmé que les futures règles européennes s'appliqueraient à toutes les sociétés étrangères (non européennes) exerçant des activités sur le sol de l'Union et/ou fournissant des services pour les consommateurs européens ;
- *Sur la question des modalités du transfert de données vers des pays tiers*, les ministres ont confirmé d'une part, que le transfert pourrait avoir lieu lorsque la "Commission a constaté que ce pays tiers ou cette organisation assure un niveau de protection des données personnelles adéquat". Les critères retenus pour définir le caractère "adéquat" du niveau de protection sont la primauté du droit, le respect des droits de l'homme et des libertés fondamentales, les règles en matière de protection des données – une législation locale "robuste" et l'existence d'une autorité de protection des données –, ainsi que les mesures de sécurité en vigueur. D'autre part, les groupes de sociétés exerçant une activité économique commune seraient autorisés à pratiquer des transferts internationaux vers des entités du même groupe lorsque des "garanties appropriées" existent, notamment "des règles d'entreprise contraignantes" (ou BCE - Binding Corporate Rules) approuvées par les autorités nationales de protection des données. (*Europa Press Release « Today's Justice Council - A council of Progress - Data protection » - 06.06.14*)

2. DÉCISIONS JUDICIAIRES ET DÉLIBÉRATION CNIL

Décision Pages Jaunes – Confirmation de la condamnation CNIL par le Conseil d'Etat
Début 2010, la société PagesJaunes, éditrice des services d'annuaires Pages Jaunes et Pages Blanches sur internet, a lancé un nouveau service en ligne mettant en oeuvre une fonctionnalité de "web crawling". Par le biais d'un logiciel de collecte automatique de données sur internet, la société a récupéré les données d'utilisateurs inscrits sur plusieurs réseaux sociaux pour compléter les informations disponibles sur le site des pages blanches. La société a ainsi indexé sur son site près de 34 millions de profils communautaires, issus de 6 réseaux sociaux : Facebook, Twitter, Viadeo, LinkedIn, Trombi et Copains d'avant.
Saisie de plaintes de particuliers ne parvenant pas à faire valoir leur droit d'opposition à la réutilisation des données les concernant, la CNIL a ordonné une mission de contrôle sur place, dans les locaux de la société.
Lors de ce contrôle, la CNIL a notamment pu constater que : (i) les informations personnelles

"aspirées" puis mises en ligne par la société PagesJaunes avaient été collectées sans le consentement des utilisateurs des réseaux sociaux. En outre, la collecte pouvait concerner des données relatives à des mineurs et à des personnes inscrites sur la liste rouge téléphonique ; (ii) les personnes ne souhaitant pas apparaître sur le site des Pages Blanches avaient la possibilité de s'y opposer, a posteriori, en remplissant un formulaire en ligne. Or, l'intéressé devait remplir autant de formulaires que de profils détenus sur les réseaux sociaux et toute demande d'opposition imprécise n'était pas traitée. La CNIL a donc considéré que les procédés de collecte et de traitement des données personnelles, mis en oeuvre par la société PagesJaunes, n'étaient pas conformes à la loi Informatique et Libertés, et a prononcé à son encontre un avertissement rendu public.
La société PagesJaunes a demandé l'annulation de cette décision auprès du Conseil d'Etat. Celui-ci a confirmé la sanction prononcée par la CNIL. *(Conseil d'État 10e et 9e sous-sections réunies, Décision du 12 mars 2014, PagesJaunes Groupe c/ CNIL)*

Décision Google – La Cour de Justice de l'Union européenne consacre le "droit à l'oubli"
Cette affaire a commencé en 2010, lorsqu'un Espagnol a adressé à l'Agence espagnole de protection des données (AEPD) une réclamation à l'encontre de l'éditeur d'un quotidien espagnol et des sociétés Google Spain et Google Inc. Ce particulier faisait valoir que, lorsqu'un internaute saisissait son nom dans le moteur de recherche de Google, la liste de résultats affichait des liens vers deux pages du quotidien faisant état des dettes de sécurité sociale dues par ce particulier alors que celles-ci étaient réglées depuis plusieurs années. Cette information était désormais dépourvue de toute pertinence, et le particulier réclamait à ce titre la suppression des contenus litigieux.
L'AEPD a rejeté la réclamation contre le quotidien, estimant que celui-ci avait légalement publié les informations en cause. En revanche, la réclamation a été accueillie contre les sociétés Google. L'AEPD a demandé aux deux sociétés de prendre les mesures nécessaires pour retirer les données de leur index et pour en rendre l'accès impossible à l'avenir. Google a alors introduit deux recours, concluant à l'annulation de la décision de l'AEPD. C'est dans ce contexte que la juridiction espagnole a déféré une série de questions à la CJUE, portant sur l'interprétation de la directive de 1995 relative à la protection des données.
Dans sa décision du 13 mai 2014, la CJUE affirme qu'une personne peut s'adresser directement à un moteur de recherche pour obtenir la suppression des liens vers des pages web contenant des informations portant atteinte à sa vie privée. Néanmoins, la Cour précise que ce "droit à l'oubli" n'est pas absolu et le soumet à plusieurs conditions.
Depuis cette décision, Google a mis en ligne un formulaire permettant aux citoyens européens de demander la suppression de résultats qu'ils jugent inappropriés dans le moteur de recherche. *(CJUE 13 mai 2014, aff. c-131/12, Google Spain SL et Google Inc. c/ AEPD et Mario Costeja González)*

Données de santé – Le Conseil d'Etat valide l'exploitation des feuilles de soins à des fins statistiques
En septembre 2011, la CNIL avait autorisé la société Celtipharm à effectuer un traitement de données à caractère personnel, issues de feuilles de soins électroniques anonymisées, afin de réaliser des études relatives à la consommation des produits de santé. Les organismes techniques, assurant le routage des feuilles de soins électroniques vers les caisses d'assurance-maladie, pour le compte et sur instruction des pharmaciens d'officine, transmettaient ainsi à la société Celtipharm ces données après avoir anonymisé celles relatives aux patients de manière irréversible, et celles relatives aux professionnels de santé sous forme cryptée. La société Celtipharm procédait ensuite à une seconde anonymisation des données relatives aux patients, et au décryptage et à l'anonymisation des données relatives aux professionnels de santé.
En décembre 2011, la société IMS Health a présenté une requête aux fins d'annulation pour excès de pouvoir de la délibération de la CNIL. La société invoquait la méconnaissance par la CNIL de sa propre interprétation des dispositions législatives et réglementaires, dont elle a pour mission d'assurer l'application. Le Conseil d'Etat a décidé de rejeter cette requête et, ainsi, d'autoriser le traitement des données aussi sensibles que celles relatives à la santé des personnes à des fins statistiques et de recherche scientifique.
La société requérante invoquait notamment la violation du secret professionnel et du droit des patients au respect de leur vie privée. Le Conseil d'Etat considère que, dans la mesure où les données en cause ont fait l'objet d'une anonymisation irréversible avant d'être transmises à la société Celtipharm, le traitement autorisé par la délibération de la CNIL ne saurait avoir pour effet de porter atteinte au secret professionnel et au droit des patients au respect de leur vie privée. En effet, les données resteront rattachables à un même individu via un identifiant unique, mais chaque individu restera parfaitement anonyme.

Par ailleurs, la société requérante arguait l'illégitimité du traitement des données, au regard des dispositions de la loi du 6 janvier 1978 disposant que les données à caractère personnel "*sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs*". Le Conseil d'Etat a alors effectué un contrôle de proportionnalité, considérant que les finalités du traitement autorisé par la délibération de la CNIL devaient être regardées comme légitimes eu égard à leur objet, qui tend à l'amélioration de la connaissance relative à la consommation des produits de santé, et que les données, dès lors qu'elles faisaient l'objet d'un processus d'anonymisation, sont également adéquates, pertinentes et non excessives au regard des finalités poursuivies. *(Conseil d'Etat, section du contentieux, 9e et 10e sous-section, 26 mai 2014, IMS Health)*

DHL International Express France – Avertissement public de la CNIL pour fuite de données
La CNIL a effectué un contrôle dans les locaux de la société DHL après avoir été alertée d'une possible faille de sécurité sur les sites internet de la société. Les constations des agents de la CNIL ont ainsi révélé la fuite de plus de 680.000 fiches clients, librement accessibles sur internet. Ces fiches clients comportaient : l'identité, l'adresse, les numéros de téléphone et adresses électroniques des personnes concernées ainsi que certaines informations détaillées permettant de faciliter la livraison de colis, telles que les indisponibilités pour raisons de santé ou la sécurisation des accès aux logements.
La société a indiqué que cette faille résultait d'un défaut de conception de l'application informatique dédiée au service concerné et fournie par un sous-traitant ; elle a justifié, en outre, avoir adopté des mesures correctives rendant inaccessibles les données litigieuses.
Malgré cette régularisation, la CNIL a, par délibération du 12 juin 2014, condamné d'un avertissement la société DHL pour manquement à son obligation de sécurité des données clients et à son obligation de limiter la conservation des données clients à un délai raisonnable.
- *Concernant le défaut de sécurité des données*, la CNIL a notamment retenu que bien qu'ayant eu connaissance d'une première faille affectant les accès internes de l'application litigieuse, DHL n'avait pour autant entrepris aucune démarche de vérification de la sécurité de l'ensemble de l'application qui lui aurait permis d'éviter la seconde fuite de données. A ce titre, la Commission a rappelé que la société demeurait responsable de traitement quand bien même l'origine de la faille serait due à un défaut dans la conception de l'application du sous-traitant.
- *Concernant la durée de conservation excessive des données*, la Commission a constaté que les plus anciennes fiches clients présentes dans l'application litigieuse dataient de 2007. Aussi, la CNIL a décidé que la société n'avait pas défini de durée de conservation adaptée à la finalité de son traitement. *(Délibération CNIL n°2014-238 du 12 juin 2014 prononçant un avertissement rendu public à l'encontre de la société DHL)*

PROPRIÉTÉ INTELLECTUELLE

1. DROIT D'AUTEUR

Jurisprudence – L'exploitant d'un site web participatif n'est pas titulaire des droits d'auteur sur les anecdotes postées par les internautes
Le site "Viedemerde" est un site de partage d'anecdotes sur les petits ennuis de la vie quotidienne, dont chaque message, limité à 300 signes, commence par "Aujourd'hui" et se termine par les initiales "VDM". La société éditrice du site a constaté qu'une agence de publicité avait diffusé, pour le compte d'un annonceur, deux spots télévisés présentant des ressemblances avec certaines anecdotes figurant sur le site viedemerde.fr. Aussi, la société éditrice du site, qui estimait être titulaire des droits d'auteur sur le concept du site et son contenu, a assigné l'agence de publicité en vue, notamment, de faire reconnaître que le contenu du site constituait une œuvre collective, et que l'agence avait commis des actes de contrefaçon. Subsidiairement, si la contrefaçon n'était pas reconnue par le Tribunal, la société éditrice réclamait la condamnation de l'agence pour parasitisme. Elle réclamait ainsi 137.000€ au titre de la contrefaçon et 100.000 euros au titre du parasitisme économique.
Dans une décision du 22 mai 2014, le Tribunal de grande instance de Paris a débouté la société éditrice du site de ses demandes sur le préjudice de contrefaçon, mais a reconnu que les agissements de l'agence de publicité constituaient des actes de parasitisme. Pour ces actes, l'agence a cependant été condamnée qu'à hauteur de 5.000€.
Concernant la contrefaçon et l'argument de l'œuvre collective : le Code de la propriété intellectuelle pose deux conditions pour définir la notion d'œuvre collective : (i) qu'elle soit créée sur l'initiative d'une personne physique ou morale qui l'édite, la publie et la divulgue sous sa direction et son nom, et (ii) que la contribution personnelle des divers auteurs participant à l'élaboration de l'œuvre se fonde dans

l'ensemble en vue duquel elle est conçue, sans qu'il soit possible d'attribuer à chacun d'eux un droit distinct sur l'ensemble réalisé. Or, en l'espèce, la condition relative au nom n'est pas remplie puisque le site s'intitule VDM, alors que la société qui l'édite porte un nom différent. La condition relative au fait que les contributions personnelles se fondent dans l'ensemble n'est pas davantage remplie, dans la mesure où chaque contribution peut être publiée sous le nom ou le pseudonyme d'un utilisateur, ce qui permet d'en individualiser l'auteur. Le Tribunal en déduit que les différentes contributions ne se confondent pas en une œuvre collective, unique. En outre, aux termes de ce jugement, le fait que chaque contribution ait une structure précise et similaire, ne peut, à lui seul, être considéré comme une instruction donnée aux auteurs.
Le Tribunal a donc considéré que les éditeurs du site litigieux ne pouvaient invoquer la violation de leurs droits d'auteur : le site, pris dans son ensemble, n'est pas une œuvre collective. *(TGI Paris, 3e ch., 1e section, 22 mai 2014, Bêta et Compagnie et autres / Australie)*

2. MARQUE

Jurisprudence – L'utilisation de la marque d'un concurrent sur internet sous la forme de « backlinks » est constitutive d'actes de concurrence déloyale.
La société Sofigram a découvert que le signe "sofigram", correspondant à sa marque, sa dénomination sociale et son nom de domaine, était utilisé dans le cadre d'une campagne de "backlinks" par une société concurrente.
Les liens retours (backlinks) sont des liens hypertextes pointant vers un site ou une page web, basés sur un mot clé ("ancre") figurant au sein d'un site web qui, en association avec l'adresse d'un site, permettent à l'internaute de naviguer de site en site par un système de renvoi. S'ils ont pour vocation de permettre une navigation simplifiée pour l'internaute et une meilleure appréhension du contenu du web, les backlinks constituent également un outil essentiel dans le cadre de l'optimisation du référencement d'un site web sur les moteurs de recherche. C'est le cas de la société concurrente de Sofigram qui apparaissait dans les premiers résultats sur le moteur de recherche Google.
La société Sofigram a donc assigné son concurrent sur le fondement de la contrefaçon de marque, concurrence déloyale et parasitisme économique. Déboutée en première instance, la société Sofigram a interjeté appel du jugement.
Dans un arrêt du 28 mars 2014, la Cour d'appel de Paris a confirmé le rejet des demandes formées au titre de la *contrefaçon de marque*, aux motifs : (i) que l'utilisation d'un signe dans le cadre de backlinks ne constituait pas un usage de ce signe à titre de marque pour des produits et services ; et (ii) que les liens associés au terme "Sofigram" étaient pour l'essentiel invisibles et donc insusceptibles de générer un risque de confusion dans l'esprit du public.
La Cour retient néanmoins le grief de *concurrence déloyale et parasitaire*, relevant qu' "*en utilisant la dénomination sociale et le nom de domaine d'une société concurrente sous la forme d'un mot clé, utilisé, de façon intense, dans le cadre de création de backlinks, lors de requête de recherches naturelles, à l'effet de tromper le moteur de recherche,* [la société concurrente avait] *provoqué, de ce seul fait, un détournement déloyal de clientèle du site qui risque d'être moins visité, ainsi qu'une utilisation parasitaire de l'investissement effectué par la société Sofigram créée antérieurement largement connue dans le marché considéré, en augmentant de façon détournée ainsi sa visibilité*". *(CA Paris, pôle 5, ch. 2, 28 mars 2014, Sofrogam c/ Carl G., Softbox systems)*

SÉCURITÉ INFORMATIQUE

Politique publique – Rapport sur la cybercriminalité "Protéger les internautes"
Le groupe de travail interministériel présidé par le procureur général près la cour d'appel de Riom, Marc Robert a remis son rapport, le 30 juin 2014, sur les mesures juridiques et techniques à prendre pour améliorer la cybersécurité et la protection des internautes.
Ce rapport réaffirme la nécessité d'adopter une stratégie globale en matière de cybercriminalité. Le groupe formule ainsi 55 recommandations visant une réponse répressive plus efficace et mieux adaptée aux nouvelles méthodes des cyberdélinquants, tout en respectant les exigences tenant à la protection des libertés fondamentales. Les principes suivants sont notamment mis en avant : la prévention des internautes, la sensibilisation et formation des professionnels (policiers, gendarmes, juges, procureurs, etc.), le développement de partenariats public-privé en ce domaine, la réorganisation des services de l'Etat et le renforcement significatif des moyens affectés à la lutte contre la cybercriminalité (notamment ressources humaines et crédits d'investissements).
Parmi les recommandations, on retiendra : 1) l'élaboration d'outils statistiques pour mesurer la réalité des cyberattaques (création d'un observatoire à cet effet) ; 2) la création d'un numéro d'appel

d'urgence pour les internautes ; 3) la création d'un Centre d'alerte et de réaction aux attaques informatique (CERT) visant à centraliser les données techniques concernant les modes d'attaques pour mieux préparer les mesures correctrices ; 4) la mise en place d'une Délégation interministérielle à la lutte contre la cybercriminalité placée sous la responsabilité directe du Premier ministre dont la mission sera de définir et d'impulser une stratégie cohérente des différentes entités de l'Etat intervenant en la matière ; 5) l'aggravation des sanctions pour certaines infractions, telles que l'usurpation d'identité ou les atteintes aux systèmes de traitement automatisé de données (STAD) ; et 6) la création d'une plateforme nationale centralisée pour le traitement des cyber-escroqueries, afin de pallier l'inefficacité du traitement de ces infractions en fonction du lieu de dépôt des plaintes. *(Rapport sur la cybercriminalité intitulé « Protéger les internautes », édité par le groupe de travail interministériel sur la lutte contre la cybercriminalité, remis le 30 juin 2014)*

Bonnes pratiques – L'ANSSI publie un guide sur l'homologation de sécurité

L'Agence nationale de la sécurité des systèmes d'information a publié le 11 juin dernier un guide concernant "l'homologation de sécurité". Si cette homologation est une obligation pour les administrations et les services de l'Etat, elle ne l'est pas pour les autres organismes. Ce guide s'adresse ainsi à tout type d'organisme, public ou privé, quelque soit sa taille.

L'objectif principal de l'homologation est de faire connaître et comprendre aux responsables (autorité administrative, élu, dirigeant d'entreprise) les risques liés à l'exploitation d'un système d'information (SI). Ce processus d'information et de responsabilisation doit aboutir pour le responsable de l'organisme à une décision par laquelle d'une part, il atteste de sa connaissance du SI et des mesures de sécurité (techniques, organisationnelles et juridiques) mises en œuvre et d'autre part, il accepte les risques résiduels. L'homologation de sécurité permet ainsi à un responsable de confirmer aux utilisateurs de SI que les risques qui pèsent sur les informations qu'ils manipulent et les services rendus, sont conformes et maîtrisés. La démarche d'homologation doit être adapté à chaque organisme, en fonction notamment de la complexité du système et la nature des données stockées.

La démarche d'homologation est recommandée depuis plusieurs années par l'Anssi. Elle permet d'instaurer une forme de confiance dans les systèmes d'information d'un organisme et dans leur exploitation. Selon l'Anssi, cette démarche est d'autant plus nécessaire que les systèmes d'information sont de plus en plus complexes et que les impacts potentiels d'un incident de sécurité sont de plus en plus graves.

Conçu comme un mode d'emploi, le guide détaille chaque étape afin de pouvoir être homologué. Le guide contient des recommandations visant à définir la stratégie d'homologation, maîtriser les risques, prendre la décision d'homologation et accepter les risques résiduels et enfin, maintenir et améliorer la sécurité des SI. *(Guide « L'homologation de sécurité en neuf étape simples », publié par l'ANSSI, le 11 juin 2014)*

INNOVATION

Jurisprudence – Première condamnation pénale pour usage illicite d'un drone civil

Fin janvier 2014, un jeune entrepreneur de 18 ans a utilisé un drone équipé d'une caméra GoPro pour survoler et filmer la ville de Nancy en méconnaissance de la réglementation applicable, puis a posté sa vidéo sur internet. Or, la vidéo a notamment été remarquée par les autorités. Dans un premier temps, la Direction régionale de l'aviation civile (DRAC) a rappelé au jeune homme les règles en vigueur en matière d'utilisation de drones et enjoint ce dernier de se mettre en conformité ; dans un second temps, le jeune entrepreneur a été convoqué devant le tribunal correctionnel pour mise en danger de la vie d'autrui.

Par ordonnance d'homologation en date du 20 mai 2014, le Tribunal de grande instance de Nancy a condamné le jeune entrepreneur à une amende contraventionnelle de 100€ et une amende délictuelle de 300€, sur deux fondements :

Le survol de zones non autorisées : il était reproché au prévenu, outre d'avoir "mis en danger" la vie d'autrui, de ne pas s'être conformé à la réglementation impliquant le respect de certaines formalités préalables relatives aux équipements et à l'utilisation du drone (tel que scénario de vol et homologation, compétence du télépilote, mesures liées à la protection des personnes, etc.).

L'utilisation non autorisée d'un dispositif d'enregistrement d'images vidéo : il était reproché au prévenu de ne pas être en possession de l'autorisation applicable aux prises de vues aériennes par appareil photographique ou cinématographique, prévue par le Code de l'aviation civile. (*TGI Nancy, Ordonnance d'homologation, 20 mai 2014, Ministère Public c/ M.T)*

PUBLICATIONS CABINET

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

- Quelles obligations pour les OIV en matière de cybersécurité : exigences européennes et françaises comparées ;
- Droits d'utilisation des logiciels : de la nécessaire gestion des licences au sein de l'entreprise ;
- E-commerce : les nouvelles obligations légales nécessitant une mise en conformité des sites web ;
- Le CSA bientôt régulateur des plateformes internet de contenus vidéo et musicaux ?

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