

LA LETTRE DU CABINET

TECHNOLOGIES DE L'INFORMATION

EDITO

Nous avons le plaisir de vous adresser le huitième 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 (p.2)

1. Marché public : un appel d'offre comportant des spécifications techniques adaptées aux besoins du pouvoir adjudicataire ne peut être annulé.
2. Contrat de développement : l'existence de réserves mineures ne remet pas en cause la bonne fin du projet dès lors que la recette définitive a été prononcée.

INTERNET (p.3/4)

1. Crowdfunding : vers l'adoption d'un cadre juridique pour le financement participatif.
2. E-réputation : Google condamnée pour négligence et faute dans le cadre de l'exploitation du service Google Suggest.
3. E-commerce : juridiction compétente en cas de contrat de vente transfrontières B-to-C.
4. Téléchargement illégal : condamnation d'un internaute français à un million d'euros.

PROTECTION DES DONNÉES PERSONNELLES (p.4/5)

1. Notification de violation de données : mise en œuvre d'une téléprocédure par la CNIL.
2. Données de santé : mise en demeure d'un centre hospitalier pour non-respect de la confidentialité des données des patients.
3. Géolocalisation : le détournement de finalité d'un système de géolocalisation rend le licenciement injustifié.
4. Listes noires : la constitution de listes noires de supporters par le PSG doit être autorisée par la CNIL.

PROPRIÉTÉ INTELLECTUELLE (p.5/7)

1. Contrefaçon : proposition de loi visant à renforcer la lutte contre la contrefaçon.
2. Logiciel :
 - L'absence de preuve de l'originalité d'un logiciel ne permet pas de poursuivre un concurrent en contrefaçon.

- La reproduction servile de logiciels condamnée pour parasitisme économique.
- 3. Base de données : l'absence de caractère substantiel des investissements de constitution d'une base de données ne confère pas de droit de protection.
- 4. Marque : l'exploitation du site blindtest.com constitutif d'actes de contrefaçon et de concurrence déloyale de la marque Blind Test.

CYBERCRIMINALITÉ (p.7)

- Cyberdéfense: projet de loi de programmation militaire comprenant des dispositions sur la protection des infrastructures vitales (OIV) contre la cybermenace.

VIE DU CABINET (p.7/8)

1. Dernières publications
2. Conférences

INFORMATIQUE

1. MARCHÉ PUBLIC

Jurisprudence – Un appel d'offre comportant des spécifications techniques adaptées aux besoins du pouvoir adjudicataire ne peut être annulé

Un appel d'offre avait été publié en avril 2013 par un Groupement d'Intérêt Public (GIP). Cet appel d'offre comportait deux lots : la fourniture de solutions d'hébergement IaaS et la fourniture d'un service de messagerie collaborative. Des spécifications techniques étaient précisées : les offres devaient être adaptées à la version Network du logiciel de messagerie Zimbra.

Deux sociétés, qui souhaitaient soumissionner, ont demandé au juge des référés l'annulation de la procédure de passation au motif que les spécifications techniques étaient discriminatoires et injustifiées ; elles imposaient selon eux le logiciel Zimbra, à l'exclusion d'autres solutions, dont des logiciels libres.

Dans son ordonnance de référé du 26 juin 2013, le Tribunal administratif de Paris n'a pas fait droit à cette demande. En effet, le Tribunal a constaté que le marché ne portait pas sur l'acquisition d'un logiciel, puisque les licences avaient déjà été fournies au GIP, mais sur des solutions d'hébergement, d'exploitation et de maintenance du logiciel de messagerie, en mode IaaS. En outre, le Tribunal a rappelé que la réglementation prévoyait que les spécifications techniques ne pouvaient avoir pour effet de créer des obstacles injustifiés à l'ouverture de marchés à la concurrence, sauf si l'objet du marché le justifiait. Dans le cas présent, le fait d'imposer aux candidats d'adapter leurs offres à la version Network du logiciel de messagerie Zimbra correspondait bien aux exigences du marché et n'était donc pas discriminatoire. (*Trib. Administratif de Paris, Ordonnance de référé, du 26 juin 2013, sociétés Nexedi et Linagora c/ Gip Renater*)

2. CONTRAT DE DÉVELOPPEMENT

Jurisprudence – L'existence de réserves mineures ne remet pas en cause la bonne fin du projet dès lors que la recette définitive a été prononcée

En juin 2003, la société Drilnet a signé un contrat de développement de site web avec un développeur. Le projet de développement a pris du retard. Le portail internet a été mis en ligne près de deux ans après la signature du contrat. Les parties ont cependant continué à travailler ensemble pour faire évoluer le projet jusqu'en 2010, moyennant la signature de plusieurs avenants au contrat initial.

Durant toute la durée des relations commerciales, une tension existait entre les deux sociétés, l'entreprise-cliente n'étant pas satisfaite du travail accompli par le développeur. En 2011, les parties décident finalement de signer un protocole d'accord visant à trouver une solution amiable et à prononcer la réception définitive de la version 2 du site web. Malgré quelques réserves, l'entreprise-cliente a signé le PV définitif de recette.

Le développeur n'ayant pas donné suite aux réserves de l'entreprise-cliente, cette dernière a remis la recette en cause et décidé d'assigner le développeur pour divers manquements (retard de livraison du site, défaillances multiples, bugs récurrents, échec du re-design du site, etc.), réclamant à ce titre plus de 20.000.000€ de dommages et intérêts.

Par jugement du 15 octobre 2013, le Tribunal de commerce de Marseille a débouté l'entreprise-cliente de ses demandes au motif que, compte tenu des manquements invoqués, cette dernière aurait pu mettre fin au contrat, ce qu'elle n'a pas fait. Le Tribunal relève également la difficulté de la demanderesse à exercer son rôle de maître d'ouvrage par les évolutions permanentes du cahier des charges et les changements d'interlocuteurs. Le protocole d'accord stipulait par ailleurs que *“la réception de la recette définitive emporte, pour les parties, renonciation à tout recours dans le cadre des contrats qui avaient été signés”*.

Le Tribunal rappelle enfin l'effet de la recette, à savoir que *“l'usage veut que lorsque l'on prononce une recette et notamment une recette définitive, les réserves sont des points mineurs à finaliser (peu importe leur nombre), ne remettant pas en cause la bonne finalité du projet. A défaut la recette ne doit pas être prononcée”*. (Trib. de commerce de Marseille, 15 octobre 2013, Société Drilnet c/ Christian J.)

INTERNET

1. CROWDFUNDING

Règlementation – Vers l'adoption d'un cadre juridique pour le financement participatif

Le crowdfunding, ou financement participatif, qu'il se réalise sous forme de dons, de prêts ou de participation au capital, n'est actuellement régi par aucun texte spécifique en France. L'exploitation d'une plateforme de crowdfunding nécessite donc aujourd'hui de respecter les obligations réglementaires contraignantes incombant aux établissements bancaires et financiers. Face au potentiel de développement de ce mode alternatif de financement de projet, le gouvernement a décidé de proposer un cadre juridique spécifique, mieux adapté à cette pratique. Moins contraignant, mais sécurisé, ce nouveau régime viserait à faciliter le développement de ce mode de financement, tout en veillant aux impératifs de protection des investisseurs. Présenté en Conseil des ministres début septembre 2013, le projet de loi prévoit : (a) la création d'un statut de Conseiller en Investissement Participatif (CIP), inspiré de celui des Conseillers en Investissements Financiers (CIF), mais sans avoir à constituer de fonds propres ; (b) l'adaptation du régime des offres au public de titres financiers au financement participatif ; (c) la création d'un régime prudentiel dérogatoire pour la réception de fonds en faveur d'un tiers dans un volume limité à trois millions d'euros par mois ; et (d) un assouplissement du monopole bancaire consistant notamment à permettre aux particuliers de réaliser des prêts, dans le cadre de financements participatifs, à destination d'autres particuliers ou d'entreprises. Ces prêts pourront être accordés dès lors que le montant se limite à 250€ par prêteur et à 300.000€ par projet. Ces limitations peuvent cependant paraître trop restrictives et risquent d'être adaptées. Le texte était en consultation publique jusqu'au 15 novembre dernier. Les résultats sont actuellement examinés. (Projet de loi d'habilitation à prendre par ordonnances diverses mesures de simplification et de sécurisation de la vie des entreprises présenté au Conseil des ministres le 3 septembre 2013)

2. E-RÉPUTATION

Jurisprudence - Google condamnée pour négligence et faute dans le cadre de l'exploitation du service Google Suggest

Un professionnel, formateur en développement personnel et gestion du stress, avait constaté que lorsque ses nom et prénom étaient saisis sur le moteur de recherche Google, ils étaient associés aux termes “escroc” et “secte” dans les suggestions de recherche et la rubrique recherches associées. Ce professionnel, puis son Conseil, ont alors demandé à la société Google la suppression de ces suggestions, en vain.

Ils ont alors assigné Google, la demande du professionnel portant sur l'injure publique et subsidiairement sur la faute et la négligence de la société. En effet, selon le demandeur, Google

n'informe pas les utilisateurs du moteur de recherche quant aux règles de fonctionnement du service Google Suggest. En outre, Google a refusé de supprimer les termes litigieux.

Par jugement du 23 octobre 2013, le Tribunal de grande instance de Paris a débouté le professionnel sur la question de l'injure, en raison du caractère automatique de l'apparition des suggestions dans la barre de requêtes du moteur de recherche. A défaut d'intention de la société Google d'émettre les propos en cause, le délit d'injure ne peut être constitué.

Le Tribunal affirme cependant que la responsabilité de Google ne peut être totalement exclue, puisque le caractère automatique de l'apparition des suggestions incriminées n'implique pas qu'elles soient le fruit du hasard. Les suggestions apparaissent en raison des choix techniques faits par Google de mettre en place cette fonctionnalité, et sont le résultat des algorithmes choisis par Google. Google procède par ailleurs à un filtrage des suggestions issues des résultats automatiques. Dès lors, le Tribunal, ayant constaté le défaut d'information des utilisateurs et le refus de supprimer les suggestions litigieuses, a condamné la société Google à verser 4.000€ de dommages et intérêts au demandeur pour préjudice moral. (*TGI Paris, 17^e ch. civ., 23 octobre 2013, Bruno L., c/ Google Inc., Google France*)

3. E-COMMERCE

Jurisprudence – Contrat de vente B-to-C : juridiction compétente en cas de vente transfrontière

La Cour de justice de l'Union européenne (CJUE) vient d'apporter des précisions relatives à la possibilité pour un consommateur d'attirer son cocontractant professionnel étranger en justice devant les tribunaux de son lieu de résidence. En l'espèce, un consommateur allemand avait acheté un véhicule d'occasion auprès d'une société française, dont le siège social était situé près de la frontière allemande. Le site internet du professionnel indiquait un numéro de téléphone en France et en Allemagne. Le consommateur allemand n'avait pas acheté la voiture par le biais de ce site internet, mais directement au siège social du professionnel.

Afin de faire jouer la garantie du vendeur, le consommateur a intenté une action en justice devant les tribunaux allemands, au motif que la réglementation européenne l'autorisait à agir devant sa juridiction locale puisque le professionnel dirigeait ses activités vers l'Allemagne. Ainsi, afin de déterminer si un professionnel dirige ses activités vers le pays d'un consommateur, la jurisprudence a dégagé plusieurs critères. A ce titre, le consommateur soutenait que ni la réglementation européenne, ni la jurisprudence n'exigeaient que le contrat de vente soit conclu à distance ou après que le consommateur ait visité le site internet pour que la saisine des tribunaux de son pays soit valable. Aucun lien de causalité entre l'activité dirigée vers l'Etat membre du consommateur et la conclusion du contrat n'est nécessaire.

La CJUE a confirmé les arguments du demandeur. Selon la Cour, la réglementation européenne n'exige pas la consultation préalable du site internet du professionnel, ni que le contrat entre le consommateur et le professionnel ait été conclu à distance. Néanmoins, selon la Cour, l'existence d'un site internet par le biais duquel le vendeur dirige ses activités vers le pays des consommateurs étrangers peut être retenu comme un critère. (*CJUE, 3^e ch., 17 octobre 2013, Lockman E. c/ Vlado S. et Article 15 paragraphe 1, c) du règlement européen n°44/2001 dit « Bruxelles 1 » sur la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale*).

4. TÉLÉCHARGEMENT ILLÉGAL

Jurisprudence – Condamnation d'un internaute français à un million d'euros

Le créateur d'une plateforme internet permettant l'échange de films, séries et musiques entre internautes a été poursuivi pour contrefaçon notamment par la Société des auteurs, compositeurs et éditeurs de musique (SACEM), la Société civile des producteurs phonographiques (SCPP), et plusieurs sociétés de production (Warner, 20th Century Fox, Disney et Columbia Pictures). Cette plateforme, dénommée ForumDDL, proposait un catalogue de 50.000 oeuvres référencées, avait environ 100.000 membres inscrits, accueillait près de 5.000 visites par jour et comptabilisait 3 millions de téléchargements effectifs. Le Tribunal correctionnel de Thionville a condamné l'exploitant de la plateforme à 10 mois de prison avec sursis et plus d'un million d'euros de dommages et intérêts. (*Tribunal corr., Thionville, 12 nov. 2013*)

PROTECTION DES DONNÉES PERSONNELLES

1. NOTIFICATION DE VIOLATION DE DONNÉES

Règlementation – Mise en place d’une téléprocédure de notification de violation de données par la CNIL

La loi Informatique et Libertés impose notamment aux fournisseurs de téléphonie fixe ou mobile et aux FAI d’informer la CNIL sans délai dès qu’ils constatent une violation de données personnelles (destruction, perte, altération, divulgation ou accès non autorisé). Ils doivent également informer les personnes dont les données ont fait l’objet de la violation, sauf si le fournisseur a mis en œuvre préalablement des mesures techniques qui rendent les données incompréhensibles à toute personne non autorisée à y avoir accès. Le défaut de notification à la CNIL et aux personnes concernées peut faire l’objet de sanctions pénales (5 ans d’emprisonnement et 300.000 € d’amende).

Depuis septembre 2013, la CNIL a mis en place une téléprocédure, accessible depuis son site internet. Tout fournisseur peut remplir directement en ligne le formulaire de notification (précisant les date, heure et circonstances de l’incident, les données concernées, les conséquences et préjudices potentiels, etc.), et dispose d’un outil d’analyse permettant d’évaluer le niveau de gravité de la violation (4 niveaux de gravité : négligeable, limité, important et maximal).

La CNIL va instruire la notification dès réception du formulaire. La procédure relative à la violation notifiée pourra être clôturée si la CNIL constate que : (i) la violation ne porte pas atteinte aux données personnelles ou à la vie privée des personnes, (ii) le cas échéant, le fournisseur a correctement informé les personnes concernées, et (iii) le fournisseur a mis en place, préalablement à la violation, des mesures techniques de protection appropriées. La CNIL pourra imposer d’informer les personnes concernées si elle constate qu’elles n’ont pas correctement été informées et si les mesures techniques de protection mises en place préalablement à la violation ne sont pas appropriées. (*Communiqué CNIL “Notifications de violation de données personnelles : une nouvelle téléprocédure”, du 23 août 2013*).

2. DONNÉES DE SANTE

Délibération CNIL – Mise en demeure d’un centre hospitalier pour non-respect de la confidentialité des données des patients

Par une délibération du 25 septembre 2013, la CNIL a mis en demeure publiquement le centre hospitalier de Saint Malo pour non-respect de la confidentialité des données. En l’espèce, suite à un contrôle réalisé au sein du centre hospitalier, la CNIL a constaté qu’un des prestataires avait accédé, avec l’accord de l’établissement, aux dossiers médicaux de plusieurs centaines de patients, en méconnaissance totale des dispositions du Code de la santé publique et de la loi Informatique et Libertés relatives au respect de la vie privée des patients et à la sécurité de leurs données.

Le sous-traitant avait été mandaté par le centre hospitalier pour une mission de codage des actes médicaux et paramédicaux. Lors de la prise en charge d’un patient par un centre hospitalier, les actes pratiqués sont codés selon une nomenclature correspondant au code de remboursement par l’assurance maladie. Le Code de la santé publique prévoit que les établissements doivent procéder à une analyse de leur activité pour détecter d’éventuelles erreurs de codage. Ces analyses sont généralement sous-traitées par les établissements à des sociétés privées. Or, la loi soumet le traitement de données à caractère personnel à des fins d’évaluation ou d’analyse des activités de soins et de prévention, à l’obtention d’une autorisation préalable. La CNIL veille ainsi, par le biais de contrôles sur place dans les établissements de santé, à ce que ces traitements ne portent pas sur les données nominatives des malades.

La mise en demeure prononcée par la CNIL imposait au centre hospitalier de prendre des mesures garantissant la sécurité et la confidentialité des dossiers médicaux des patients pris en charge et de veiller à ce que ces dossiers ne puissent pas être accessibles aux tiers. En outre, l’établissement de santé devait justifier du respect de cette injonction auprès de la CNIL sous 10 jours. Dans un communiqué d’octobre 2013, la CNIL a annoncé que le centre hospitalier s’était mis en conformité.

(Délibération CNIL n°2013-037 du 25 septembre 2013 mettant en demeure le centre hospitalier de Saint-Malo, et Communiqué CNIL intitulé "Clôture de la mise en demeure adoptée à l'encontre du centre hospitalier de Saint-Malo" du 17 octobre 2013)

3. GEOLOCALISATION

Jurisprudence – Le détournement de finalité du système de géolocalisation rend le licenciement injustifié

Un agent de sécurité s'était vu notifier son licenciement pour avoir, à plusieurs reprises, quitté son poste de surveillance pendant ses heures de travail. Son employeur avait eu connaissance des faits reprochés au moyen du système de géolocalisation installé sur le véhicule de service du salarié. Contestant son licenciement, ce dernier a saisi le conseil de prud'hommes au motif que le mode de preuve utilisé pour justifier son licenciement était illicite. En effet, le salarié invoquait le fait que les institutions représentatives du personnel n'avaient pas été consultées préalablement à l'installation du système de géolocalisation, et que lui-même n'en avait pas été avisé à titre individuel.

Débouté en première instance, le salarié a saisi la Cour d'appel, qui a fait droit à sa demande. La Cour a relevé qu'au moment de l'installation du dispositif de géolocalisation, la société (i) n'était pas soumise à l'obligation de consulter les institutions représentatives du personnel (l'effectif de la société n'atteignant pas le seuil légal) et (ii) avait effectué les formalités préalables auprès de la CNIL. Toutefois, la Cour a constaté que la note d'information faite aux salariés visait l'installation du système de géolocalisation à des fins commerciales (amélioration du service client via la réalisation de statistiques), et non le suivi de l'activité des employés. La Cour a conclu que, du fait du détournement de finalité du dispositif de géolocalisation par rapport à la finalité qui avait été portée à la connaissance des salariés et déclarée à la CNIL, le moyen de preuve devait être considéré comme illicite et le licenciement privé de cause réelle et sérieuse. (CA Lyon, ch. soc. A, 13 mars 2013, *John X. c/ société Y*)

4. LISTES NOIRES

Décision CNIL – La constitution de listes noires de supporters par le PSG doit être autorisée par la CNIL

L'article 45 de la loi Informatique et Libertés dispose que le président de la CNIL peut mettre en demeure le responsable d'un traitement de données personnelles qui ne respecte pas les obligations légales "de faire cesser le manquement constaté dans un délai qu'il fixe". Le PSG avait mis en œuvre deux traitements de données excluant des supporters de stade, la première liste noire ayant pour finalité l'exclusion des personnes frappées d'une peine complémentaire d'interdiction de stade ou d'une mesure de sûreté, la seconde ayant pour finalité l'exclusion des personnes jugées indésirables. En outre, les fichiers étaient communiqués au Paris Handball. Le 29 août 2013, la présidente de la CNIL a pris une décision mettant le PSG en demeure, sous délai d'un mois, de se mettre en conformité avec la loi Informatique et Libertés en demandant des autorisations à la CNIL relatives à la mise en œuvre de ces deux traitements, et de cesser de transmettre ces données au Paris Handball. Par décision du 7 novembre 2013, la CNIL a constaté la mise en conformité du PSG et a clôturé la procédure. (Décision CNIL n°2013-015 du 29 août 2013 mettant en demeure la SASP Paris-Saint-Germain-Football ; Délibération n°2013-235 du 12 septembre 2013 du bureau de la CNIL décidant de rendre publique la mise en demeure ; Clôture de la procédure par courrier de la CNIL du 7 novembre 2013.)

PROPRIÉTÉ INTELLECTUELLE

1. CONTREFAÇON

Réglementation - Proposition de loi visant à renforcer la lutte contre la contrefaçon

En France, le volume et la valeur des marchandises saisies par la douane ont considérablement augmenté (800.000 articles saisis en 2002 pour une valeur de 166 millions d'euros ; 4,6 millions d'articles saisis en 2012 pour une valeur de 287 millions d'euros). Dans ce contexte, une proposition de loi, dont l'objet est de renforcer l'arsenal juridique de lutte contre la contrefaçon, a été déposée au Sénat fin septembre dernier. Parmi les dispositions proposées figurent :

- le renforcement des dédommagements civils accordés aux victimes de contrefaçon. Le texte prévoit (i) l'allocation au titulaire de droits d'une somme spécifique prenant en considération l'ensemble des profits réalisés par le contrefacteur, c'est-à-dire ses bénéfices et ses économies d'investissements, et (ii) trois types d'indemnisation ou postes de préjudice possibles : les conséquences économiques négatives subies par la partie lésée ; le préjudice moral causé à cette dernière et les bénéfices réalisés par le contrefacteur. Ce dispositif est transposé dans l'ensemble des branches de la propriété intellectuelle (propriété littéraire et artistique, dessins et modèles, brevets ; marques, d'indications géographiques, etc.).

- le renforcement des moyens d'actions des douanes. Le texte prévoit notamment : (i) l'harmonisation de la procédure de contrôle des douanes et retenue douanière de marchandises pour tous les droits de propriété intellectuelle ; (ii) l'extension de la compétence des douanes en matière d'infiltration afin de faciliter la constatation du délit de contrefaçon et (iii) l'extension à l'ensemble des marchandises contrefaisantes de la compétence des douanes en matière de "coups d'achat" (procédure qui consiste, pour un douanier, à procéder à l'acquisition d'une certaine quantité de produits soupçonnés de constituer des contrefaçons afin de vérifier si la contrefaçon est ou non avérée). La proposition de loi est en cours examen. (*Proposition de loi tendant à renforcer la lutte contre la contrefaçon, n°866, Enregistré à la Présidence du Sénat le 30 septembre 2013*)

2. LOGICIEL

Jurisprudence – L'absence de preuve de l'originalité d'un logiciel ne permet pas de poursuivre un concurrent en contrefaçon

Deux professionnels estimaient que le logiciel L'assistant financier, commercialisé par la société Microsoft dans la version française de la suite Office édition PME, reproduisait le logiciel dénommé L'analyse mensuelle, qu'ils avaient eux-mêmes conçu et développé. Ils ont donc assigné Microsoft en contrefaçon de leurs droits d'auteur. Déboutés en première instance et en appel au motif qu'ils ne rapportaient pas la preuve de l'originalité du logiciel en cause, les demandeurs ont décidé de se pourvoir en cassation.

Dans un arrêt du 14 novembre dernier, la Cour suprême n'a pas fait droit à leurs demandes. La Cour a constaté que le rapport d'expertise versé aux débats par les demandeurs se bornait à étudier les langages de programmation mis en œuvre, et évoquait les algorithmes et les fonctionnalités du programme, non protégés par le droit d'auteur. Dès lors, selon la Cour, les demandeurs n'ont fourni aucun élément de nature à justifier l'originalité des composantes du logiciel "telles que les lignes de programmation, les codes ou l'organigramme, ou du matériel de conception préparatoire", et donc établissant qu'ils étaient titulaires des droits d'auteur sur le logiciel litigieux. (*Cass. civ. 1, 14 novembre 2013, n°12-20687*)

Jurisprudence – La reproduction servile de logiciels condamnée pour parasitisme économique

Une société spécialisée de développement informatique avait développé deux applications de divertissement pour le compte d'un client. Par la suite, l'un de ses anciens salariés avait développé deux applications similaires. La société, et son client, ont donc assigné l'ancien salarié sur le fondement du parasitisme pour copie servile des applications et détournement des codes sources, afin de le condamner à restituer les applications, ne plus en faire usage et payer une certaine somme d'argent au titre d'une perte de recettes publicitaires.

Dans une décision du 10 octobre 2013, la Cour d'appel d'Aix-en-Provence a fait droit aux demandes des sociétés. En effet, la Cour a constaté que les applications commercialisées par l'ancien salarié étaient "en tous points identiques" à celles développées par les demanderesse. En outre, interrogé sur le procédé informatique de ses applications, l'ancien salarié avait simplement indiqué, sans le démontrer, que l'algorithme utilisé était différent. Selon la Cour, ce dernier "ne justifie, et n'offre pas

plus de le faire, d'aucune nécessité technique, contrainte de production ou de norme existante imposant une reproduction à l'identique des applications litigieuses". La Cour considère donc que le défendeur a nécessairement dupliqué les codes-sources de son ancien employeur pour faire une copie servile des applications. Ces agissements constituent des actes de parasitisme puisqu'ils consistent en "une appropriation sans autorisation du travail ou du savoir-faire d'autrui et de ses investissements, faussant la concurrence entre opérateurs économiques". (CA Aix-en-Provence, civ. 1^{er} ch. C, 10 octobre 2013, Société Reservoir Dev. et Agir Media c/ Ivan C.)

3. BASE DE DONNÉES

Jurisprudence – L'absence de caractère substantiel des investissements de constitution d'une base de données ne confère pas de droit de protection

Une société, exerçant une activité de livraison de fleurs, avait constitué à cette fin, un réseau de fleuristes et deux bases de données à partir d'annuaires professionnels existants. Son ancien directeur commercial avait créé une société ayant la même activité et mis également en place un réseau de fleuristes. La première société a décidé d'attaquer son ancien directeur commercial en contrefaçon de base de données et concurrence déloyale.

La Cour d'appel d'Aix-en-Provence a fait droit à sa demande en concurrence déloyale mais a refusé à la demanderesse la protection conférée au producteur d'une base de données. La demanderesse s'est pourvue en cassation au motif que la juridiction d'appel s'était bornée à affirmer que "la constitution de ses deux bases de données à partir de nombreux annuaires professionnels, la vérification de l'exactitude des éléments recueillis puis leur mise à jour périodique n'avaient pas nécessité de sa part un investissement financier, matériel et humain substantiel lui ouvrant droit à la protection conférée par les articles L.341-1 et suivants du code de la propriété intellectuelle", sans avoir analysé les éléments versés aux débats.

La décision d'appel a été confirmée par la Cour de cassation en juin 2013 au motif que les investissements relatifs à la constitution et au fonctionnement des bases de données litigieuses (réunion des données pertinentes, leur mise à jour, et leur traitement afin de les organiser) pendant une vingtaine d'années, ne s'avéraient pas substantiels. (Cass. civ. 1, 19 juin 2013, Réseau fleuri c/ L'Agitateur floral)

4. MARQUE

Jurisprudence – L'exploitation du site blindtest.com constitutif d'actes de contrefaçon et de concurrence déloyale de la marque Blind Test

L'une des parties à cette affaire était le titulaire de plusieurs marques françaises et communautaires BLIND TEST et d'un site web www.blind-test.com, qu'elle utilisait pour commercialiser notamment des boîtes de jeux, dont le principe consistait à répondre correctement à des questions posées à partir de l'écoute d'extraits sonores. Celle-ci dernier a assigné l'exploitant d'un site internet de jeux de quizz musical intitulé Blind Test, accessible à l'URL www.blindtest.com en contrefaçon et concurrence déloyale.

Pour sa défense, l'exploitant du site internet litigieux invoquait : (i) la nullité de la marque BLIND TEST au motif que l'expression Blind Test est dépourvue de *caractère distinctif* pour désigner des jeux sous forme de quizz ; (ii) la déchéance de la marque BLIND TEST pour dégénérescence et (iii) la déchéance de la marque BLIND TEST pour défaut d'exploitation sérieuse.

La Cour de cassation a débouté le défendeur de l'ensemble de ses demandes. Sur *le caractère distinctif du signe Blind Test* : la Cour rappelle qu'il doit s'apprécier à l'époque du dépôt de la marque. Or, en 2000 et 2003, ce signe n'était pas couramment utilisé pour des jeux en ligne ou quizz musicaux. Sur *la déchéance pour dégénérescence* de la marque : selon la Cour le terme Blind Test n'est pas devenu une désignation usuelle dans le commerce des jeux de quizz musicaux. Enfin, sur *la déchéance pour défaut d'exploitation sérieuse* de la marque : la Cour a constaté que le titulaire de la marque justifiait d'une exploitation sérieuse et continue du signe sur son site blind-test.com.

- *A contrario*, la Cour a fait droits aux demandes du titulaire de la marque BLIND TEST, en condamnant l'éditeur du site litigieux à 10.000€ de dommages-intérêts pour contrefaçon et à 10.000€ pour concurrence déloyale. Pour décider que la contrefaçon était constituée en l'espèce, la Cour a relevé que l'exploitant avait repris le signe Blind Test dans le nom de domaine pour l'exploitation de produits et services similaires (même s'il a collé les termes blind et test, cette différence passant inaperçue aux yeux du consommateur normalement attentif) et avait reproduit la marque Blind Test sur son site, peu important les différences visuelles qui ont été introduites, la cour procédant à une appréciation globale et ayant conclu à un risque de confusion pour le consommateur d'attention moyenne. (CA Paris, pôle 5, ch. 1, 2 octobre 2013, Société Chugulu c/ Antoine de T.).

CYBERCRIMINALITÉ

Législation – Projet de loi de programmation militaire comprenant des dispositions sur la protection des infrastructures vitales (OIV) contre la cybermenace

Le projet de loi de programmation militaire 2014-2019, déposé au Sénat en août 2013 et actuellement en débat à l'Assemblée nationale, comporte un volet relatif à la cyberdéfense, devenue une priorité nationale. Parmi les dispositions proposées, le texte comporte des mesures visant à renforcer la protection des systèmes d'information des OIV. Ces mesures prévoient : l'obligation de mettre en œuvre des systèmes de détection d'attaques informatiques ; l'obligation de notifier tous incidents de sécurité affectant les systèmes d'information à l'Etat ; la possibilité pour l'Agence National de la Sécurité des Systèmes d'Information (ANSSI) de réaliser des audits de sécurité des SI, dont les coûts seront à la charge de l'OIV et enfin, la condamnation à des peines d'amende pouvant atteindre 750.000€ (pour les personnes morales), en cas de manquement aux obligations précitées. (*Projet de loi de programmation militaire 2014-2019, déposé au Sénat le 2 août 2013*)

VIE DU CABINET

Dans le cadre du développement de nos activités dans le domaine de la cyber sécurité, Betty Sfez a obtenu le **Certificat de spécialisation "Sécurité Numérique" de l'INHESJ** (Institut National des Hautes Etudes de la Sécurité et de la Justice) ainsi que le titre de **"Conférencier en Sécurité économique labellisé EUCLES"** (Délégation Interministérielle à l'intelligence économique –D2IE- et INHESJ).

1. DERNIÈRES PUBLICATIONS

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

- Principes et limites à l'accès aux emails des salariés par l'employeur : les dernières décisions jurisprudentielles ;
- Open data : un nouvel élan pour la politique d'ouverture des données publiques ;
- La protection du patrimoine informationnel de l'entreprise : un tour d'horizon ;
- Données de santé : des obligations de sécurité spécifiques pour les professionnels de la santé ;
- Pour ou contre la pratique du BYOD : quelques réponses juridiques.

Par ailleurs, nous avons rédigé un article intitulé "E-réputation : une image de marque à défendre", paru dans le magazine **Face au Risque** de Décembre 2013 (n°498).

2. CONFÉRENCES

Cet automne, le Cabinet a participé à plusieurs salons professionnels :

- **Salon CARTES Secure Connexions**, 19 au 21 novembre 2013 : animation d'une conférence sur le thème : *"Personal Data Privacy in the Cloud: using the Contract as a Management Tool"* (<http://www.cartes.com/>).

- **Salon Cloud & IT Expo** - 16 et 17 octobre 2013 : intervention à une table ronde sur le thème *"Prestations dans le cloud computing : des questions juridiques de plus en plus centrales"* (<http://www.cloud-and-it-expo.fr/>).

- **Salon APS** - 24 au 26 septembre 2013 : conférence intitulée *"La protection du patrimoine informationnel de l'entreprise : la sensibilisation des salariés aux bonnes pratiques à adopter"* (<http://www.salon-aps.com/>).

Le 5 décembre, participation à la première édition de l'émission de Web TV **SaaS discute** organisée par Webcastory et sponsorisée par les sociétés Aspaway et IBM sur le thème *"La conversion des éditeurs de logiciels vers le Cloud : enjeux, challenges, opportunités, réalités, perspectives"* (<http://techtoc.tv/saasdiscute-saison1>).

Directeur de la publication : Bénédicte DELEPORTE

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

Cette Lettre est une publication périodique diffusée gratuitement auprès d'un nombre limité de personnes ayant une relation directe ou indirecte avec le Cabinet. La Lettre ne saurait constituer ou être interprétée comme un acte de conseil juridique. Le destinataire est seul responsable de l'usage qu'il fait des informations fournies dans la Lettre.