LA LETTRE DU CABINET

TECHNOLOGIES DE L'INFORMATION

EDITO

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

Cette Newsletter est organisée autour des thématiques suivantes : Informatique, Internet, Protection des données personnelles, Propriété intellectuelle, Cybersécurité, et 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 et bonne rentrée à tous !

SOMMAIRE

INFORMATIQUE

1. CONTRAT "CLÉS EN MAIN"

Jurisprudence – Les avenants signés postérieurement n'ont pas entraîné la renonciation au contrat d'intégration initial

La compagnie d'assurance MAIF avait conclu avec IBM un contrat d'intégration pour un prix ferme et forfaitaire de 7 millions d'euros, aux termes duquel IBM s'engageait notamment à respecter le calendrier défini. Compte tenu des retards accumulés, des avenants successifs redéfinissant le périmètre et le coût du projet ont été conclus. Constatant l'impossibilité pour IBM de terminer le projet, la MAIF a assigné IBM. Par un jugement du Tribunal de grande instance de Niort du 14 décembre 2009, la MAIF avait obtenu l'annulation du contrat pour vice du consentement (dol) aux motifs qu'IBM l'avait trompée sur sa capacité à mener à bien le projet et sur les conditions de faisabilité dudit projet, et le versement de 11 millions d'euros de dommages et intérêts à la Maif. Ce jugement a été infirmé par la Cour d'appel de Poitiers le 25 novembre 2011. La Cour a notamment rejeté l'argument selon lequel IBM aurait utilisé des manipulations frauduleuses pour tromper la Maif et a considéré que la MAIF ne pouvait être qualifiée de profane en matière informatique. En outre, en se fondant sur les avenants signés postérieurement au contrat initial, il n'était pas établi qu'IBM avait dissimulé à la MAIF *"des informations majeures relatives au calendrier, au périmètre, au budget du projet"*. La Cour d'appel a donc jugé que la MAIF avait accepté, en connaissance de cause, de revoir le projet initial et l'a ainsi condamnée à régler les factures impayées, assorties des intérêts de retard, augmenté de dommages et intérêts (450.000€). Dans une décision du 4 juin 2013, cassant l'arrêt d'appel, la Cour de cassation s'est fondée sur le principe de la novation, prévu aux articles 1271 et suivants du Code civil. La novation consiste notamment pour un débiteur à contracter avec son créancier une nouvelle dette ou obligation qui se substitue à l'ancienne, laquelle s'éteint. Selon l'article 1273 du Code civil, la volonté de nover doit être non équivoque et résulter clairement des actes entre les parties. En l'espèce, la Cour de cassation a relevé que la MAIF n'avait pas manifesté "sans équivoque" sa volonté de "substituer purement et simplement" au contrat d'intégration les avenants signés postérieurement. Les avenants n'ont donc pas entraîné la renonciation des parties au contrat initial. La Cour a ainsi cassé l'arrêt d'appel et renvoyé l'affaire devant la Cour d'appel de Bordeaux. *(Cass. com., 4 juin 2013, IBM France, BNP Paribas Factor et a. c/ Mutuelles Assurance des instituteurs de France (Maif))*

2. CLOUD COMPUTING

Politique européenne – Désignation d'un groupe d'experts chargé d'élaborer des clauses contractuelles

Dans le cadre du suivi du développement des services Cloud, la Commission européenne a publié, le 21 juin dernier, un appel à candidature afin de réunir un groupe d'experts composé de prestataires de services Cloud, de PME, de juristes, de consommateurs et d'universitaires. La mission de ce groupe consistera à élaborer des clauses contractuelles "sûres" et "loyales" en matière de services Cloud. L'objectif d'une telle initiative est de renforcer la confiance des entreprises et des consommateurs à l'égard des services fournis en mode Cloud. Selon la Commission, la publication de ces clauses contractuelles types devra faciliter la conclusion des contrats informatiques entre prestataires et clients, et ainsi contribuer au développement des services Cloud, services à fort potentiel économique. Les experts devraient être nommés dans les prochains mois. *(Communiqué de presse de la Commission européenne du 21 juin 2013, "Développement de l'informatique en nuage : la Commission sollicite des experts pour recenser les clauses contractuelles sûres et équitables")*

Jurisprudence – Un prestataire de services SaaS condamné à faciliter l'exportation des données de son client chez un autre prestataire

Le parti UMP avait conclu avec la société Oracle un contrat SaaS de 2 ans, ayant pour objet la gestion et l'hébergement de données personnelles. L'UMP a souhaité récupérer ses données afin d'en transférer l'hébergement à un nouveau prestataire à l'expiration du contrat le liant à Oracle. Cependant, la société Oracle a invoqué une impossibilité technique. Pour pallier ce dysfonctionnement, Oracle a proposé un correctif spécifique à l'environnement UMP et une solution de contournement en cours de réalisation. Selon l'UMP, cette proposition ne permettait pas la reprise des données par le nouveau prestataire à la date de fin du contrat. Or, à défaut de reprise dans les délais, l'UMP ne pouvait continuer à exploiter sa base de données, et notamment remplir ses obligations légales vis-à-vis de ses adhérents. L'UMP a donc assigné Oracle aux fins d'obtenir sa condamnation à fournir les moyens techniques permettant l'exportation des données. En défense, Oracle a invoqué le fait qu'elle ne garantissait pas contractuellement que ses services seraient exempts d'erreurs ou qu'ils fonctionneraient de manière ininterrompues, ni qu'elle corrigerait les erreurs. En l'espèce, la Cour a rejeté cet argument en précisant que "*la société Oracle ne peut soutenir de bonne foi, qu'elle ne manquerait pas à ses obligations contractuelles si elle ne permettait pas à l'UMP de bénéficier en temps utile de ses données pour permettre au nouveau prestataire de les exploiter et d'être opérationnel dès la fin de sa propre prestation*". Dès lors, le Tribunal a enjoint Oracle, sous astreinte de 5.000€ par jour de retard, à compter de la décision, soit de fournir à l'UMP les moyens techniques lui permettant d'exporter les données, soit de garantir à l'UMP qu'elle lui assurerait, sans frais, la prolongation de l'accès complet à son service, au-delà de la date d'échéance du contrat et jusqu'à ce qu'elle soit en mesure de procéder à l'exportation des données. *(TGI Nanterre, Ordonnance de référé, 30 novembre 2012, UMP c/ Oracle)*

3. Open Data

Politique internationale –Charte du G8 pour l'ouverture des données publiques
Lors du sommet du G8 de juin dernier, les Chefs d'Etat ont signé une Charte pour l'ouverture des données publiques. A travers cette Charte, les Etats membres du G8 souhaitent promouvoir une gouvernance plus ouverte et plus transparente. Ils s'engagent ainsi à permettre l'accès aux données publiques en respectant cinq grands principes : (i) ouvrir par défaut les données publiques, (ii) fournir des données de qualité et en quantité, (iii) fournir des données accessibles et réutilisables par tous (en privilégiant les formats ouverts et non-propriétaires), (iv) améliorer la gouvernance (partager les expériences et compétences techniques), et (v) promouvoir l'innovation. Chaque Etat membre du G8 s'engage à développer un plan d'action d'ici fin 2013, visant à respecter les principes de la Charte. Pour les Etats membres, des données publiques librement accessibles et gratuitement réutilisables peuvent être une source de services et de produits innovants, contribuant à la création de "nouveaux marchés, de nouvelles entreprises et de nouveaux emplois". *(Charte du G8 pour l'Ouverture des Données Publiques du 18 juin 2013, accessible sur le site www.etalab.gouv.fr)*

Directive européenne – Directive du 26 juin 2013 concernant la réutilisation des informations du secteur public
Une nouvelle directive, modifiant la directive de 2003 concernant la réutilisation des informations du secteur public vient d'être publiée. La directive de juin 2013 apporte des précisions relatives au périmètre applicable à l'Open Data, notamment la distinction entre données publiques et données exclues des règles d'accès au public (motif de protection de la sécurité nationale, défense ou sécurité publique, confidentialité des données statistiques, confidentialité des informations commerciales). Les données culturelles (documents détenus par les bibliothèques, musées et archives) sont intégrées dans la sphère des données publiques pouvant être réutilisées. Les documents comportant des données personnelles doivent respecter la réglementation relative à la protection de la vie privée. Cette directive devra être transposée dans le droit des états membres d'ici deux ans. La loi CADA du 17 juillet 1978 devra donc être modifiée pour être mise en conformité. *(Directive 2013/37/UE du parlement européen et du Conseil du 26 juin 2013)*

Internet

1. Moyens de Paiement dématérialisés

Réglementation – Les titres spéciaux de paiement dématérialisés non soumis à la réglementation relative aux établissements de monnaie électronique
Avec la loi du 28 janvier 2013, la France a créé un nouveau cadre légal relatif à l'accès et à l'exercice de l'activité d'établissement de monnaie électronique (EME). Cette loi a été suivie par la publication de plusieurs arrêtés et décrets d'application en mai 2013. Afin de pouvoir émettre et gérer de la monnaie

électronique à titre de profession habituelle, il est désormais nécessaire de remplir certaines conditions telles l'obtention d'un agrément, la détention d'un capital social de 350.000€ minimum, etc. Toutefois, la loi a prévu plusieurs dérogations à ce régime ; il en va ainsi de certains titres spéciaux de paiement dématérialisés. La liste de ces titres vient d'être fixée par arrêté du 17 juin 2013. Il s'agit notamment des titres-restaurant, chèques emploi-service universels préfinancés, chèques-vacances, etc. *(Loi n°2013-100 du 28 janvier 2013 et arrêté du 17 juin 2013 fixant la liste des titres spéciaux de paiement dématérialisés)*

2. RESPONSABILITÉ

Jurisprudence - Qualité d'éditeur du courtier en noms de domaine

Dans un arrêt du 17 avril 2013, la Cour d'appel de Paris a condamné la société Sedo, exploitant un site parking et de vente aux enchères de noms de domaine, pour contrefaçon de marque, en qualité d'éditeur du contenu de son site web. La pratique des "sites parking" consiste à proposer aux réservataires de nom de domaine d'afficher des liens publicitaires sur des pages html accessibles depuis ces noms de domaine, sans autre contenu éditorial, le nom de domaine n'étant pas effectivement utilisé pour désigner un site web actif. Une société avait découvert que des noms de domaine similaires à son nom commercial et à sa marque avaient été réservés par un tiers et qu'ils étaient proposés à la vente aux enchères via le site web de la société Sedo. La société a donc assigné les réservataires des noms de domaine ainsi que la société Sedo en contrefaçon de marque et usurpation de son nom commercial et de ses noms de domaine. Condamnée en première instance, la société Sedo a interjeté appel, faisant valoir son statut d'hébergeur de contenu et le régime de responsabilité allégée y afférent. Après avoir procédé à un examen détaillé des CGU du site et des services proposés par la société Sedo, la Cour d'appel en a conclu que la société Sedo avait la qualité d'éditeur de contenu et que sa responsabilité était donc pleinement engagée pour les contenus publiés sur son site parking. Selon la Cour, les services proposés par Sedo "*dont l'objet est d'optimiser la présentation des offres à la vente et de promouvoir ces offres, impliquent de la part de la société Sedo un comportement non pas neutre entre le client vendeur et les acheteurs potentiels, mais bien un rôle actif de nature à leur conférer une connaissance ou un contrôle des données relatives à ces offres*". La Cour considère ainsi que Sedo exerce une action déterminante sur le contenu des pages parking, en intervenant dans le choix des mots clés et en assurant la fourniture des liens commerciaux, du fait de son partenariat avec Google. La société Sedo est donc condamnée à 75.000€ de dommages et intérêts pour contrefaçon de marque, pour avoir permis l'affichage de liens hypertextes sur les pages parking redirigeant les internautes vers des produits et services similaires à ceux visés par la marque du demandeur. *(CA Paris, pôle 5, ch. 1, 17 avril 2013, n°10/14270 Sedo GmbH, Sedo.com c/ DNX Corp., MKR Miesen)*

3. E-COMMERCE

Réglementation française – Dernières évolutions du nouveau cadre légal de la vente de médicaments sur internet

Depuis l'ordonnance du 19 décembre 2012, la vente de médicaments sur internet est autorisée en France, sous réserve du respect de certaines conditions. Cette réglementation restrictive a cependant subi des péripéties avant de s'aligner sur la directive européenne de 2011. L'arrêté du 20 juin 2013 est venu préciser les bonnes pratiques de dispensation des médicaments pour les officines ayant l'autorisation de vendre en ligne. Entré en vigueur le 12 juillet 2013, l'arrêté définit des conditions spécifiques relatives à la conception et à l'exploitation d'un site de e-pharmacie, à l'exercice de l'activité de e-pharmacien et à la vente de médicaments en ligne. En parallèle, suite à un recours pour excès de pouvoir déposé par un pharmacien, le Conseil d'Etat avait, dans une décision de février 2013, suspendu les dispositions légales françaises qui n'autorisaient la vente en ligne qu'aux seuls médicaments de "médication officinale", la loi française étant donc plus restrictive que la réglementation européenne. Par décision du 17 juillet 2013, le Conseil d'Etat confirme sa position et annule les dispositions légales litigieuses. L'arrêté du 20 juin 2013 est donc dénué, pour partie, de base légale concernant l'étendue des médicaments pouvant être vendus en ligne. *(Arrêté n°AFSP1313848A du 20 juin 2013 relatif aux bonnes pratiques de dispensation des médicaments par voie électronique et Conseil d'Etat, 17 juill. 2013, n°s 365317, 366195, 366272 et 366468)*

4. PUBLICITÉ EN LIGNE

Jurisprudence - Publicité pour une boisson alcoolique via un réseau social non conforme au Code de la santé publique

La publicité pour les boissons alcooliques est strictement réglementée. Le 3 juillet 2013, la Cour de

cassation a confirmé l'arrêt de la Cour d'appel de Paris condamnant la société Ricard pour sa campagne publicitaire intitulée "*un Ricard, des rencontres*", pour manquement à la loi. Cette campagne de juin 2011 était constituée de films et d'affiches, diffusées sur la voie publique, dans la presse, sur internet et à la radio. La publicité était également diffusée via une application mobile accessible sur Facebook, proposant de partager des recettes de cocktails. Estimant que le contenu des publicités sur les différents supports était contraire à la réglementation, une association a assigné la société Ricard en retrait de sa campagne publicitaire. Condamnée en première instance puis en appel, la société Ricard s'est pourvue en cassation. La société invoquait le fait que la loi autorise l'indication de la composition du produit et son mode de consommation dans les publicités pour boissons alcooliques. La Cour de cassation a débouté la société Ricard aux motifs que le slogan "*un Ricard, des rencontres*", la gamme de couleurs et les nuages présents sur les publicités renvoyaient, dans l'esprit du consommateur, non pas à la simple composition du produit ou à son mode de consommation – la rencontre ou le mélange d'ingrédients (le cocktail) - mais au rapprochement entre personnes et à l'incitation à consommer de l'alcool. Le slogan et la publicité Ricard ont donc été jugés illicites car constituant une incitation directe à consommer de l'alcool. Dans cette affaire, la Cour de cassation a étendu l'application des dispositions des articles L.3323-2 et suivants du Code de la santé publique à la diffusion d'une publicité sur un réseau social (Facebook), considérant que le fait que "*le message soit relayé par l'intervention d'un internaute à l'intention de son "réseau d'amis" ne lui faisait pas perdre son caractère publicitaire*." *(Cass. civ. 1, 3 juillet 2013, N° 12-22633, Ricard c/ Anpaa)*

PROTECTION DES DONNÉES PERSONNELLES

1. SÉCURITÉ DES DONNÉES

Règlement – Précisions concernant l'obligation de notifier les violations de données personnelles

Le 24 juin 2013, la Commission européenne a adopté un règlement concernant les mesures relatives à la notification des violations de données à caractère personnel. Ce règlement impose aux fournisseurs de services de communications électroniques accessibles au public (fournisseurs de services déclarés à l'ARCEP, à savoir les FAI ou fournisseurs de téléphonie fixe ou mobile) de notifier tout incident, tel que destruction, perte, accès non autorisé, relatif aux données de leurs clients. Le texte détaille les conditions et modalités de cette notification à l'autorité compétente (la CNIL en France) et, dans certains cas, aux personnes dont les données sont concernées par l'incident. L'information des personnes concernées est obligatoire seulement si l'incident est susceptible de porter atteinte à leurs données ou à leur vie privée (par exemple : vol d'informations financières ou de données de santé ; risque d'usurpation d'identité ou d'atteinte à la réputation). Il n'y a pas d'obligation de notification si le fournisseur de services justifie avoir pris des mesures de protection technique appropriées. La notification, qu'elle soit adressée à l'autorité compétente ou aux personnes concernées, doit être réalisée dans de très brefs délais et comporter un certain nombre d'informations relatives à l'incident, aux données et aux mesures prises. Si le fournisseur sous-traite une partie de ses services à un tiers, non directement lié par contrat avec les personnes concernées, alors ce tiers devra, en cas incident, avertir le fournisseur, mais ne sera pas tenu d'informer les personnes concernées. Les règlements européens étant d'application directe dans les Etats-membres, ces nouvelles dispositions entrent en vigueur en France et dans le reste de l'UE le 25 août 2013. Une nouvelle téléprocédure de déclaration de violation de données personnelles vient d'être mise en ligne par la CNIL. *(Règlement UE n°611/2013 du 24 juin 2013 concernant les mesures relatives à la notification des violations de données à caractère personnel).*

2. LOI INFORMATIQUE ET LIBERTÉS

Jurisprudence - La cession d'un fichier clients jugée nulle pour défaut de conformité à la loi informatique et libertés

Dans une décision du 25 juin 2013, la Cour de cassation a retenu que, dans la mesure où un fichier de données personnelles non déclaré était illicite, ce fichier devait être considéré comme étant hors commerce. Il ne peut donc faire l'objet d'un contrat et donc être commercialisé. Dans cette affaire, deux associés d'une société avaient décidé de céder certains éléments de leur fonds de commerce de vente de vins aux particuliers, dont un fichier clients. Ce fichier comprenait près de 6.000 adresses ; le prix de la cession avait été fixé à 46.000€. L'acquéreur, ayant découvert que le fichier n'avait pas été déclaré à la CNIL, a assigné les vendeurs en résolution de la vente, pour dol et pour non-conformité du fichier clients à la loi. Débouté en première instance et en appel, l'acquéreur a finalement obtenu gain de cause devant la cour suprême. La Cour de cassation a fondé sa décision sur l'article 22 de la

loi Informatique et Libertés qui prévoit l'obligation de déclarer à la CNIL tout traitement automatisé de données personnelles et sur l'article 1128 du Code civil qui dispose qu'il ne peut y avoir de contrat valable que sur un objet licite. La Cour a ainsi considéré que "*tout fichier informatisé contenant des données à caractère personnel doit faire l'objet d'une déclaration auprès de la CNIL et que la vente d'un tel fichier qui, n'ayant pas été déclaré, n'est pas dans le commerce, a un objet illicite*". La sanction de l'illicéité étant la nullité, ceci implique pour le vendeur d'un fichier non-déclaré l'obligation de rembourser à l'acheteur le prix de la vente, son fichier étant sans valeur juridique ni commerciale. (*Cass. com., 25 juin 2013, n°12-17.037)*

3. Cybersurveillance des salariés

Jurisprudence - Les emails d'un salarié émis depuis son ordinateur personnel sont présumés professionnels

La jurisprudence récente tend à affirmer que tous les fichiers et emails édités et reçus par un salarié, à l'aide de son ordinateur professionnel, peuvent être consultés par l'employeur, sous réserve qu'ils ne soient pas identifiés comme personnels. Dans une décision du 19 juin 2013, la Cour de cassation a étendu cette règle aux emails émis depuis l'ordinateur personnel du salarié, avec son adresse personnelle, puis transférés sur son ordinateur professionnel. Dans cette affaire, un salarié avait été licencié pour faute grave, à savoir pour concurrence déloyale. Une expertise de son disque dur professionnel avait révélé l'échange de nombreux emails, depuis son ordinateur et adresse de messagerie personnels, avec des salariés d'un concurrent, qu'il avait ensuite transférés sur son ordinateur professionnel. Ces emails n'étaient pas intitulés "personnel" dans leur objet et ne figuraient pas dans des dossiers identifiés comme "personnel" dans son ordinateur professionnel. Ainsi, plusieurs dossiers et fichiers expressément nommés "perso" ou "personnel" découverts sur le disque dur, avaient été exclus du rapport d'expertise. Contestant son licenciement, le salarié a saisi la juridiction prud'homale. Il affirmait que l'accès à ses messages personnels, effectué par un expert mandaté par l'employeur, hors sa présence, constituait une atteinte au respect de sa vie privée. Les constatations effectuées par l'expert lui étaient donc inopposables. Selon le salarié, l'employeur ne pouvait ni lire ni se servir de ces emails comme preuve d'une faute ; le licenciement était donc dépourvu de cause réelle et sérieuse. La Cour n'a pas suivi cette argumentation. *(Cass., soc., 19 juin 2013, N°12-12138)*

Propriété Intellectuelle

1. Droit d'auteur

Jurisprudence – Condamnation à 1 million d'euros pour reproduction et exploitation de catalogues de vente aux enchères et photographies

La maison de vente aux enchères Camard et Associés et un photographe ont assigné, pour contrefaçon, concurrence déloyale et parasitisme, la société Artprice, exploitant un site web d'information sur le marché de l'art, au motif que cette dernière avait reproduit sans autorisation plus de 71 catalogues et 12.150 photographies, dont ils étaient les auteurs. Dans une décision du 26 juin 2013, la Cour d'appel de Paris a condamné la société Artprice. La Cour, après examen des catalogues et photographies litigieuses, a reconnu le caractère original d'une grande partie d'entre eux, et de ce fait leur a reconnu une protection au titre du droit d'auteur. En effet, la Cour a relevé que les catalogues, par leur composition et la mise en œuvre des lots, présentés selon un certain ordre et de façon méthodique "*présentent une physionomie propre qui les distinguent des autres catalogues de ventes aux enchères et qui traduit un parti pris esthétique empreint de la personnalité de leur auteur*". En outre, la Cour a relevé que les photographies reflétait la personnalité du photographe par ses choix esthétiques arbitraires dans le positionnement des objets, le cadrage et l'angle de prise de vue des objets, le jeu des ombres et de la lumière, et le travail de retouches de ces photo. Enfin, la Cour a constaté que l'exploitant du site web avait numérisé et mis à la disposition du public les photographies et catalogues litigieux, sur lesquels apparaissait la marque de la maison de vente. En conséquence, la société Artprice a été condamnée à verser, à la maison de vente, 340.000€ de dommages et intérêts pour contrefaçon de catalogues et de marque, et parasitisme, du fait d'avoir tiré un profit illégitime des investissements réalisés par la maison de vente, et 644.298€ au photographe, pour préjudice économique et moral. *(CA Paris, pôle 5, ch. 1, 26 juin 2013, Stéphane B., Camard et associés c/ Artprice.com)*

2. MARQUE

Jurisprudence – L'exploitation, même tardive, d'une marque permet d'éviter la déchéance
La société titulaire de la marque NORTHLAND, enregistrée pour désigner divers produits, dont des vêtements de sport, a assigné en contrefaçon deux autres sociétés qui avaient commercialisé des vêtements sur lesquels étaient apposés les signes "Northland" et "Northland Expedition". Les défendeurs ont contesté cette action au motif que le demandeur était déchu de ses droits sur la marque litigieuse, pour défaut d'usage sérieux au sens de la loi. L'article L.714-5 du Code de la propriété intellectuelle dispose que le titulaire d'une marque, ne faisant pas un usage sérieux de son signe pendant une durée de 5 ans, peut être déchu de ses droits sur la marque. La preuve de l'exploitation de la marque incombe au titulaire de la marque dont la déchéance est réclamée. Les défendeurs avaient obtenu gain de cause en première instance puis en appel, et la déchéance des droits sur la marque NORTHLAND avait été prononcée, le titulaire de la marque litigieuse n'ayant pas rapporté la preuve de son usage effectif et sérieux. Le titulaire déchu s'est alors pourvu en cassation. La Cour s'est prononcée en faveur du titulaire, relevant que celui-ci avait rapporté la preuve d'une exploitation de sa marque postérieurement à la date d'assignation mais antérieure de plus de trois mois à la demande de déchéance. Or, la loi prévoit qu'une marque ne peut être frappée de déchéance dès lors que son titulaire a repris un usage sérieux de celle-ci plus de trois mois avant la demande en déchéance. *(Cass. com., 19 mars 2013, n°11-29.016, société SMSTIC c/ Eurauchan)*

3. NOM DE DOMAINE

Jurisprudence – Conflit entre noms de domaine descriptifs : absence de concurrence déloyale
Dans une décision du 24 mai 2013, le Tribunal de commerce de Paris a rappelé que le titulaire d'un nom de domaine, descriptif de l'objet même du site web auquel il renvoie, ne peut se prévaloir d'une quelconque protection juridique. En conséquence, l'exploitation par un concurrent d'un nom de domaine similaire ne constitue pas une faute. Cette affaire opposait une société exploitant un site web proposant des services d'obsèques dans toute la France, à l'URL e-obseques.fr (enregistré en 2010), à une autre société exploitant un site web fournissant des services funéraires à Paris et en proche banlieue, à l'URL i-obseques-paris.fr (enregistré en 2011). La première société a assigné la seconde au motif que l'utilisation d'un nom de domaine, proche du sien, créait une confusion avec son propre site web et qu'en faisant ce choix de nom de domaine la société concurrente agissait de façon déloyale. Toutefois, elle a été déboutée de toutes ses demandes. En effet, le Tribunal a relevé que : (i) l'adresse internet choisie par la demanderesse pour exercer son activité est la simple juxtaposition du mot obsèques et de la lettre "e-" ; (ii) dans l'environnement internet, la lettre "e-" associée au terme "commerce" évoque le commerce électronique ; (iii) l'adresse "e-obseques.fr" signifie donc "commerce électronique d'obsèques", ce qui est l'exacte activité du site internet exploité par la demanderesse. Or, selon le Tribunal, en choisissant des termes intégralement descriptifs, la demanderesse s'exposait à retrouver les mêmes termes dans des sites concurrents. Aussi, compte tenu de ce choix de nom de domaine, qui lui a évité les investissements indispensables pour donner une notoriété propre à une adresse internet non descriptive, le Tribunal a jugé que la demanderesse ne pouvait revendiquer une protection qui aboutirait à lui reconnaître un monopole d'utilisation d'un terme descriptif. *(Trib. Com. Paris, 15e ch., 24 mai 2013, C. Davril, Le Passage c/ SAEM Services Funéraires de la Ville de Paris)*

CYBERSECURITE

FRAUDE INFORMATIQUE

Jurisprudence – Accès frauduleux à un STAD : absence de condamnation pour défaut de sécurité de l'entreprise victime
Une personne avait accédé au système informatique et récupéré des documents internes à l'Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail (l'Anses), via l'extranet de cette dernière. L'Anses a porté plainte auprès des services de police pour intrusion dans son système d'information et vol de données. L'Agence, considérée comme opérateur d'importance vitale (OIV), a vu son enquête diligentée par la DCRI, qui a décelé une erreur de paramétrage du serveur hébergeant l'extranet de l'Anses et permis de citer l'auteur des faits à comparaître. Si ce dernier a bien reconnu avoir récupéré des documents via son VPN, il a néanmoins indiqué être arrivé par erreur jusqu'au coeur de l'extranet de l'Anses et avoir eu librement accès aux documents litigieux, sans passer par la page d'accueil du site web de l'Agence, qui était sécurisée par un identifiant et un mot de passe. Dans un jugement du 23 avril 2013, le Tribunal de grande instance de Créteil a relaxé le prévenu des deux chefs d'accusation, pour les motifs suivants : d'une part, le Tribunal considère que "*le maître du système, l'Anses, en raison de la défaillance technique, n'a pas manifesté*

clairement l'intention de restreindre l'accès aux données récupérées par (le prévenu) aux seules personnes autorisées". Dès lors, selon le Tribunal, le prévenu avait pu légitimement penser que, si l'accès à certaines données du site de l'Agence nécessitait un code d'accès et un mot de passe, les données qu'il avait récupérées étaient en libre accès. D'autre part, le Tribunal considère qu'en l'absence de soustraction matérielle des documents appartenant à l'Anses (simple téléchargement), et donc en l'absence d'appréhension d'une chose, le délit de vol n'était pas constitué. Le prévenu avait donc pu légitimement penser que les documents litigieux étaient librement téléchargeables, puisque non protégés par un quelconque système. Il n'y a pas eu de sa part une volonté d'appropriation frauduleuse des fichiers informatiques et donc pas d'élément intentionnel de l'infraction. *(TGI Créteil, 11e ch. correctionnelle, 23 avril 2013, Ministère Public c/ Olivier L.)*

Jurisprudence – Accès frauduleux à un fichier clients : condamnation atténuée pour défaut de sécurité de l'entreprise victime

La société Sarenza, exploitant un site de vente en ligne de chaussures, s'était fait pirater son fichier clients, contenant 4,7 millions d'adresses email. Elle avait pourtant mis en place plusieurs mesures de sécurité, telles que l'insertion d'adresses pièges, l'accès aux postes des salariés par des identifiants et mots de passe, l'insertion d'une clause de confidentialité dans les contrats de travail de ses salariés, la mise en place du tracking des accès à sa base de données, etc. La fraude avait été réalisée par une société tierce, avec l'aide d'une employée de Sarenza qui disposait des codes d'accès au fichier clients. Ainsi, durant plusieurs semaines, l'auteur de la fraude avait consulté, exploité et cédé le contenu du fichier à d'autres sociétés. La fraude découverte, la société Sarenza a assigné les sociétés fautives pour contrefaçon de sa base de données, concurrence déloyale et parasitisme et évalué son préjudice à 4,5 millions d'euros. Dans une décision du 21 février 2013, le Tribunal de grande instance de Paris a condamné l'un des défendeurs pour négligence fautive pour avoir acquis une base de données sans s'être assuré de son origine (une base de données volumineuse, cédée à un prix dérisoire, par une société inconnue sur le marché). En revanche, le Tribunal a débouté la société Sarenza de ses demandes relatives à la contrefaçon et à la concurrence déloyale. Enfin, le Tribunal a relevé que l'identifiant utilisé par la salarié fautive était utilisé par 4 autres salariés de Sarenza. Le Tribunal a donc considéré que la société Sarenza était responsable de son préjudice, à hauteur de 30%, du fait de l'absence de mesures de sécurité strictes relatives à la gestion des identifiants et mots de passe, et a ainsi ramené la condamnation des responsables du piratage de 100.000€ à 70.000€. *(TGI Paris, 3e section, 4e ch., 21 février 2013, Sarenza c/ Jonathan et autres)*

VIE DU CABINET

PUBLICATIONS

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

- Accès frauduleux à un STAD : de la nécessité de sécuriser le système d'information de l'entreprise
- Conflit entre les noms de domaine e-obseques.fr et i-obseques-paris.fr : absence de concurrence déloyale
- E-pharmacie : les conditions de vente de médicaments sur internet enfin précisées
- Une nouvelle norme AFNOR pour assainir le domaine des avis de consommateurs sur internet
- Cybercriminalité : la réponse pénale de l'Union européenne aux attaques contre les systèmes d'information
- Annulation du contrat de cession d'un fichier d'adresses clients non déclaré à la CNIL

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