LA LETTRE DU CABINET
TECHNOLOGIES DE L'INFORMATION

EDITO

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

Cette Newsletter est organisée autour des thématiques suivantes : Internet, Protection des données personnelles, Propriété intellectuelle, Cybercriminalité et pénal du numérique, 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.

Nous vous souhaitons une bonne lecture et une très bonne année 2015 !

SOMMAIRE

ⓘ FLASH – PROTECTION DES SITES WEB CONTRE LES CYBERATTAQUES

CYBERCRIMINALITÉ – COMMUNIQUÉ DE L'ANSSI

Dans un communiqué du 14 janvier, l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) souligne le fait que, depuis l'attentat du 7 janvier 2015, de nombreux sites internet français auraient été piratés.

Selon l'Agence, deux catégories d'attaques ont été répertoriées : la défiguration de site internet et le déni de service (DDoS). Une défiguration peut se définir comme « *une attaque par laquelle une personne malveillante modifie l'apparence ou le contenu du site pour remplacer ou pour mettre en ligne un contenu illégitime, par exemple pour relayer un message politique, pour dénigrer le propriétaire du site ou pour revendiquer son attaque comme preuve d'un savoir-faire* ». Le déni de service a pour objet de rendre le site attaqué indisponible pour ses utilisateurs légitimes, et donc inaccessible à la consultation. Ces attaques peuvent avoir de lourdes conséquences pour l'entreprise victime du piratage (atteinte à l'e-réputation et/ou perte de chiffre d'affaires).

Ces attaques, menées semble-t-il de manière non cordonnée par des individus ou des groupes indépendants, sont susceptibles de s'intensifier dans les semaines à venir. Plusieurs groupes d'attaquants ont diffusé des messages de propagande incitant à démultiplier ces actes contre des sites institutionnels français. Aussi, face à une telle menace, l'ANSSI rappelle la nécessité pour les organismes, publics et privés, de protéger leurs sites internet et leurs systèmes d'information. Cette protection peut passer par la mise en œuvre de mesures simples de sécurité techniques et organisationnelles. A ce titre, l'ANSSI vient d'éditer des fiches listant quelques bonnes pratiques pour prévenir ce type d'acte et réagir en cas d'intrusion. *(Voir notamment communiqué Anssi du 14 janvier 2015, « Protéger son site internet des cyberattaques »).*

INTERNET

1. RÉGLEMENTATION

Recommandation – Les clauses abusives dans les contrats de services des réseaux sociaux

La Commission des clauses abusives a publié une recommandation, datée du 7 novembre 2014 relative aux clauses abusives dans les contrats de services de réseaux sociaux.

La Commission recommande que 46 clauses soient éliminées des contrats proposés par les exploitants des plateformes web communautaires. Il en va notamment des clauses ayant pour objet ou pour effet : de rendre opposable, aux utilisateurs du service la version en langue étrangère du contrat ; de présumer le consentement des utilisateurs du service aux conditions générales d'utilisation du seul fait qu'ils utilisent le réseau social ; de limiter abusivement le droit de rétractation ; de réserver à l'exploitant du réseau social le droit de modifier unilatéralement le contrat, sans en informer préalablement l'utilisateur. La Commission propose également de supprimer les clauses

interdisant aux utilisateurs du réseau social de participer à une action de groupe ou encore de laisser croire aux utilisateurs qu'ils ne bénéficient pas des dispositions impératives de la loi française. Les prestataires de réseaux sociaux doivent donc revoir leurs conditions d'utilisation (CGU) à la lumière de cette recommandation afin de s'assurer de leur conformité au droit français, ou en cas de soumission à un droit étranger, de leur conformité aux règles d'ordre public français. *(Recommandation n°2014-02 relative aux contrats proposés par les fournisseurs de services de réseaux sociaux, du 7 novembre 2014)*

Position de l'ACPR sur les paiements réalisés via les plateformes internet

Depuis près d'un an, l'ACPR (Autorité de contrôle prudentiel et de résolution), dépendant de la Banque de France, dans une interprétation extensive de la réglementation issue de la directive sur les services de paiement (DSP), a décidé d'étendre le champ d'application de la réglementation aux prestataires non bancaires, qui reçoivent des fonds et les retransmettent à leurs clients, dans le cadre de leur activité commerciale (encaissement de fonds pour le compte de tiers).

En effet, dans une interprétation étendue des termes de la DSP et des articles du code monétaire et financier (textes de transposition de la directive en droit français), il semble possible d'intégrer de nombreuses activités considérées hors du champ de compétence de la profession bancaire, dans le périmètre de cette réglementation. Cette interprétation concerne au premier chef les activités relatives au financement participatif (crowdfunding), aux monnaies virtuelles (bitcoins), mais également les plateformes de services internet fonctionnant sur le mode de l'intermédiation (telles les places de marché).

L'application de cette réglementation particulièrement contraignante aux plateformes internet impliquerait pour les exploitants de ces plateformes, soit de faire une demande d'agrément d'établissement de paiement auprès de l'ACPR, soit de faire une demande d'exemption, soit encore de modifier les conditions de paiement en utilisant les services d'un prestataire agréé. La situation est assez confuse pour l'instant. Un projet de directive "services de paiement 2" (DSP2) est actuellement en cours d'examen par la Commission européenne. Nous reviendrons sur cette question dans une prochaine newsletter. *(Voir notamment Communiqué ACPR du 29 janvier 2014 sur les monnaies virtuelles ; Guide du financement participatif à destination des plates-formes et des porteurs de projet, ACPR, 14 mai 2013)*

Nouvelles règles de TVA applicables aux services numériques dans le cadre du commerce B-to-C à compter du 1er janvier 2015

Depuis le 1er janvier 2015, de nouvelles règles de TVA sont applicables aux services numériques rendus entre professionnels et consommateurs (B-to-C). Ces nouvelles dispositions, issues d'une directive européenne de 2008, prévoient désormais l'imposition des particuliers, ressortissants de l'Union européenne, à la TVA de leur pays de résidence (résidence habituelle ou domicile), et non plus la TVA du lieu d'établissement fiscal du prestataire. Ainsi, quel que soit le pays dans lequel un particulier européen achète un « e-service », il sera soumis à la TVA de son pays de résidence. Par exemple, un résident français qui achète un service à prestataire allemand, sera soumis à la TVA française (20%) ; un client polonais télécharge une application mobile depuis un site finlandais, le prestataire finlandais facturera la TVA polonaise.

Ce nouveau dispositif s'applique à tous les prestataires, qu'ils soient ou non établis dans l'UE. Dès lors, un particulier résidant à Barcelone faisant appel à une entreprise américaine pour avoir accès aux chaînes de télévision US : l'entreprise américaine devra lui facturer la TVA espagnole.

Trois types de services sont visés par la nouvelle réglementation : les services de télécommunications (téléphonie fixe et mobile, fourniture d'accès à internet), de radiodiffusion et de télévision (diffusion de programmes audiovisuels sur des réseaux de télévision ou de radio) et les services électroniques (applications mobiles, téléchargement de musique, livres électroniques, jeux vidéos).

Aucune démarche particulière n'incombe aux consommateurs. La TVA sera reversée par les prestataires via un guichet unique, ou portail internet créé à cet effet (« MOSS ») et mis à leur disposition par l'administration fiscale de chaque Etat-membre. Il appartiendra ainsi aux consommateurs de vérifier leurs données de facturation.

Enfin ces nouvelles règles, pouvant avoir un impact sur les tarifs, à la hausse ou à la baisse, ne concernent pas les relations entre deux professionnels (B-to-B).

(Voir notamment Directive 2008/8/CE du Conseil du 12 février 2008 modifiant la directive 2006/112/CE en ce qui concerne le lieu des prestations de services)

2. JURISPRUDENCE

Responsabilité – Condamnation de Dailymotion pour défaut de suppression de contenus

manifestement illicites
Les sociétés du groupe TF1 avaient constaté la diffusion sur le site Dailymotion de contenus audiovisuels sur lesquels elles détenaient des droits. Après de nombreuses mises en demeure de supprimer ces contenus litigieux, restées infructueuses, les sociétés du groupe TF1 ont assigné la société Dailymotion.
Les demanderesses estiment qu'en sa qualité d'hébergeur de contenus et au regard des dispositions de l'article 6.I.2 de la loi pour la confiance dans l'économie numérique (LCEN), la société Dailymotion avait l'obligation de supprimer promptement les vidéos des émissions télévisées illicitement mises en ligne, après en avoir été informée par celles-ci. Les sociétés du groupe TF1 reprochaient en effet à Dailymotion de ne pas avoir réagi promptement malgré les mises en demeure qui lui avaient été adressées, ni d'avoir entrepris la moindre action à l'encontre des usagers inscrits sur sa plateforme.
Dans un arrêt du 2 décembre 2014, la Cour d'appel de Paris a constaté que la société Dailymotion avait commis près de 570 manquements à son obligation de retrait et notamment que certaines vidéos litigieuses avaient été laissées en ligne jusqu'à 104 jours après avoir reçu des notifications de retrait. La Cour considère que ces manquements ont causé un préjudice aux sociétés du groupe TF1, dont les émissions, mises illicitement en ligne sur Dailymotion, génèrent un nombre très important de visualisations (jusqu'à 370.000 vues pour une émission), permettant aux internautes de se dispenser de regarder ces émissions lors de leur diffusion sur les chaînes du groupe TF1 et d'utiliser le site Dailymotion comme un service de rattrapage de ces émissions. Ceci a eu un impact négatif sur l'audience télévisée de TF1, et par voie de conséquence sur ses recettes publicitaires. Aussi, selon la Cour, les agissements de la société Dailymotion sont constitutifs d'actes de concurrence déloyale et parasitisme. La Cour a condamné la société Dailymotion à plus 1.200.000 euros de dommages et intérêts. (*CA Paris, pôle 5, ch.1, 2 décembre 2014, TF1 et autres / Dailymotion)*

Responsabilité – L'exploitant d'un site internet, qualifié d'éditeur de contenus, condamné pour diffamation
Un particulier avait intenté une action en réparation pour préjudice subi du fait de la publication d'un article, jugé diffamatoire, dans un journal national chypriote et mis en ligne sur deux sites internet. La juridiction chypriote, estimant que l'affaire dépendait en partie de l'interprétation de la réglementation européenne sur la responsabilité des acteurs de l'internet, a décidé de surseoir à statuer et de poser une question préjudicielle à la Cour de justice de l'Union européenne (CJUE).
La principale question soulevée dans ce litige consistait à déterminer le régime de responsabilité applicable à l'éditeur de presse ayant publié l'article diffamatoire sur ses sites internet. Celui-ci pouvait-il invoquer la qualité d'hébergeur et la responsabilité atténuée y afférente ou devait-il être considéré comme un éditeur de contenu et endosser de ce fait une responsabilité plus large ?
Pour répondre à cette question, la CJUE a examiné l'activité du défendeur à l'action, au regard de la réglementation et des critères dégagés par la jurisprudence européenne. La Cour rappelle qu'un prestataire peut endosser la qualité d'hébergeur de contenus sous réserve que son activité soit purement technique, automatique et passive, n'impliquant aucune connaissance, ni contrôle des informations transmises ou stockées.
Or, en l'espèce, la Cour a considéré que le défendeur, éditeur de presse qui publie sur ses sites internet la version électronique d'un journal a, en principe, connaissance des informations qu'il publie et exerce un contrôle sur celles-ci. Il ne saurait donc être considéré comme un simple prestataire ou intermédiaire technique, et endosser à ce titre la responsabilité atténuée de l'hébergeur. Dès lors, en qualité d'éditeur des contenus litigieux, la défenderesse peut voir sa responsabilité engagée pour diffamation. (*CJUE, 7e ch., 11 septembre 2014, Sotiris P. / O Filelefθheros Dimosia Etaireia Ltd, Takis K. Giorgos S.)*

Site web communautaire – Condamnation d'un utilisateur pour non respect des conditions générales d'utilisation du site
Dans cette affaire, un particulier inscrit sur le site web Onvasortir.com, s'est vu interdire l'accès au site par son exploitant. Considérant cette décision abusive, le particulier a assigné l'exploitant du site litigieux devant le Tribunal d'instance de Nancy. Il demandait la condamnation de la défenderesse à réactiver son compte, sous astreinte de 1.000€ par jour de retard à compter de la signification du jugement, et le paiement de 5.000€ de dommages et intérêts. Le demandeur invoquait le fait que la suppression de son accès au site Onvasortir.com avait nuit à son image et à son intégrité, causant un préjudice à l'activité d'animation de soirées qu'il entendait développer, sous le statut d'auto-entrepreneur.
La société exploitant le site web litigieux considérait que ces demandes devaient être rejetées car la suppression de l'accès au compte du demandeur était justifiée par le fait que ce dernier n'avait pas

respecté les conditions générales d'utilisation (CGU) du site. En effet, le demandeur s'était inscrit sous plusieurs pseudonymes et avait ouvert plusieurs comptes, en tant que particulier alors qu'il les utilisait à titre professionnel. Enfin il organisait des événements avec plus d'une vingtaine de membres inscrits sur le site litigieux. Or, les CGU du site Onvasortir.com interdisaient de telles pratiques.
Le Tribunal a accueilli les arguments de l'exploitant du site et débouté le particulier de toutes ses demandes. Le Tribunal a considéré que le demandeur n'avait pas respecté les CGU du site Onvasortir.com. La suppression de son compte était donc justifiée. Le demandeur a été condamné à payer 200€ de dommages et intérêts pour mauvaise foi et intention de nuire. *(Trib. d'Instance de Nancy, 5 septembre 2014, Monsieur C. / Netuneed)*

PROTECTION DES DONNÉES PERSONNELLES

1. RÉGLEMENTATION

Recommandation – Le G29 propose un pack de conformité à la société Google
A la suite des sanctions prononcées par différentes autorités européennes de protection des données à l'encontre de la société Google, le G29 (groupe des autorités de protection européennes), a adressé, fin septembre 2014, à la société Google une lettre comportant des mesures pratiques visant à mettre sa politique de confidentialité et ses pratiques en conformité avec la loi. La liste des mesures, annexée à la lettre du G29, constitue avant tout un guide de bonnes pratiques et de recommandations. Ces mesures ne sont que des suggestions et la société Google aura la possibilité de mettre en œuvre d'autres mesures pour se mettre en conformité. Le G29 préconise notamment à Google : (i) de rendre plus accessible sa politique de confidentialité sur sa page d'accueil ; (ii) d'utiliser un langage clair et compréhensible ; (iii) d'informer les internautes sur l'identité de ses « partenaires » autorisés à traiter les données collectées ; (iv) de mettre en œuvre une « politique de rétention des données » qui informe et explique aux utilisateurs la durée de conservation pour chaque catégorie de données ; (v) de créer une "politique de vie privée personnalisée", composée en fonction des services effectivement utilisés par chaque utilisateur ; et (vi) d'obtenir le consentement exprès et éclairé des utilisateurs avant tout croisement de leurs données pour une finalité spécifique. *(Liste des mesures pratiques pour se mettre en conformité publiée par le G29 le 23 septembre 2014)*

Recommandation – Le G29 publie des lignes directrices sur le droit à l'oubli
Les autorités de protection européennes, réunies au sein du G29, ont adopté le 26 novembre 2014 des lignes directrices. Celles-ci contiennent une interprétation commune de l'arrêt de la CJUE du 13 mai 2014 sur le droit à l'oubli, et des critères communs pour l'instruction des plaintes adressées aux autorités, suite à un refus de déréférencement par les moteurs de recherche.

Interprétation commune de l'arrêt de la CJUE
Les lignes directrices rappellent et précisent les termes de l'arrêt de la CJUE du 13 mai 2014, et leurs conséquences, à savoir notamment : qui peut et comment exercer en pratique le droit au déréférencement, le rôle des autorités européennes de protection de la vie privée et les garanties pour la liberté d'expression et le droit à l'information. En pratique, les autorités seront amenées à instruire les demandes des personnes ayant clairement un lien avec l'Union européenne, c'est-à-dire les citoyens ou résidents d'un pays membre de l'Union.
Par ailleurs, les lignes directrices précisent la portée territoriale donnée à un déréférencement. A ce titre, le G29 considère que pour assurer l'effectivité du droit au déréférencement et ne pas permettre son contournement, celui-ci devra être effectif dans toutes les extensions pertinentes, y compris le .COM. Or, Google a déclaré s'opposer à une telle extension de ces demandes, compte tenu de la faible utilisation faite de google.com par les internautes européens. Selon Google, les internautes européens ne représenteraient que 5% des requêtes sur google.com, les utilisateurs étant généralement automatiquement redirigés vers la version locale de Google (.fr, .de, .it, etc.), sur la base de leur IP de connexion. Cependant, cette redirection peut être aisément contournée pour utiliser google.com.
Le G29 précise enfin que les moteurs de recherche n'ont pas à informer de manière systématique les sites à l'origine du contenu déréférencé, du fait que certaines de leurs pages ne sont plus accessibles sur Google, en raison d'un déréférencement à la demande d'une personne physique. Une telle communication systématique n'a pas de base légale dans la législation européenne de protection des données.

Liste des critères communs d'examen des demandes
Les lignes directrices du G29 contiennent une liste des critères communs que les autorités nationales

de protection des données appliqueront pour traiter les plaintes qu'elles reçoivent suite à des refus de déréférencement par les moteurs de recherche. Ces critères doivent être considérés comme des outils de travail flexibles qui aideront les autorités dans la prise de décision. Cette liste n'est pas exhaustive. Les critères seront appliqués au cas par cas et en accord avec les dispositions nationales applicables. Aucun de ces critères n'est déterminant à lui seul. Chacun d'entre eux doit être appliqué à la lumière des principes établis par la Cour et en particulier de celui de « l'intérêt général du public à avoir accès à l'information ». Treize critères sont définis par le G29, sous trois grandes catégories :
- *Critères propres au plaignant* : les résultats de recherche concernent-ils une personne physique ? Cette personne est-elle publique ou joue t-elle un rôle dans la vie publique ? Le plaignant est-il mineur?
- *Critères concernant les données et informations litigieuses relatives au plaignant* : les données et les informations sont-elles exactes, pertinentes et/ou excessives, sensibles, à jour ? Les informations ont-elles un impact négatif sur la vie privée du plaignant ou créent-elles un risque pour le plaignant ? Enfin, les informations sont-elles relatives à une infraction pénale ?
- *Critères concernant le contexte de la publication des informations litigieuses* : le contenu a-t-il été volontairement diffusé par le plaignant ? Le contenu doit-il être public ? Le plaignant pouvait-il raisonnablement savoir que le contenu serait public? Le contenu a-t-il été publié à des fins journalistiques ? La publication répond-elle à une obligation légale ? *(Lignes directrices publiées par le G29, le 26 novembre 2014)*

2. DÉCISIONS JUDICIAIRES ET DÉLIBÉRATIONS CNIL

Délibération de la CNIL sur l'enregistrement des conversations téléphoniques des salariés
Le 27 novembre 2014, la CNIL a adopté une nouvelle norme simplifiée relative aux traitements automatisés de données à caractère personnel destinés à l'écoute et à l'enregistrement des conversations téléphoniques sur le lieu de travail. Les enregistrements doivent avoir pour finalité la formation ou l'évaluation des employés et/ou l'amélioration du service. Les données collectées peuvent comprendre les données d'identification de l'employé et de l'évaluateur, la date, l'heure et la durée de l'appel et l'évaluation professionnelle de l'employé.
Certains traitements sont exclus du champ de cette nouvelle norme : les traitements réalisés par des organismes collectant des données sensibles ; les enregistrements audiovisuels ; les écoutes et enregistrements couplés avec des données provenant d'une capture d'écran de l'ordinateur de l'employé ; et les enregistrements permanents ou systématiques des appels sur le lieu de travail, y compris à des fins probatoires. *(Délibération n°2014-474 du 27 novembre 2014 portant adoption d'une norme simplifiée relative aux traitements automatisés de données à caractère personnel mis en œuvre par les organismes publics et privés destinés à l'écoute et à l'enregistrement des conversations téléphoniques sur le lieu de travail (NS 057)*

Droit à l'oubli - Condamnation de Google en référé par le TGI de Paris
Par une ordonnance de référé du 19 décembre 2014, le Président du Tribunal de grande instance de Paris a donné effet, pour la seconde fois, aux principes relatifs au droit à l'oubli posés par la CJUE en mai 2014. La juridiction saisie devait se prononcer sur la demande d'une personne physique de déréférencement du moteur de recherche Google, d'un article du journal Le Parisien relatant sa condamnation pour escroquerie en 2006.
La plaignante ne contestait pas le caractère licite de l'article litigieux, mais elle souhaitait qu'il soit déréférencé dans les résultats de recherche associés à son nom. Ayant formulé, en vain, plusieurs demandes de déréférencement auprès de la société Google inc., la plaignante a décidé d'assigner Google France en justice, Google inc. étant intervenue volontairement à l'action. La société Google avait rejeté ses demandes au motif que le maintien du lien litigieux se fondait sur l'intérêt du public.
Le Président du Tribunal de grande instance de Paris a fait droit à la demande de la plaignante, considérant que cette dernière justifiait « de raisons prépondérantes et légitimes prévalant sur le droit à l'information ». Selon la juridiction saisie, le maintien des liens hypertexte litigieux n'était pas justifié car la plaignante avait purgé sa peine. La condamnation datait de plus de huit ans et elle ne figurait pas sur le bulletin n°3 du casier judiciaire de la plaignante. Enfin, ces liens nuisaient à sa recherche d'emploi. La société Google inc. a donc été enjointe de supprimer les liens litigieux. *(TGI Paris, Ordonnances de référé, 24 novembre et 19 décembre 2014, Marie-France M. c/ Google France et Google Inc.)*

Cybersurveillance – Un système de cybersurveillance non déclaré à la CNIL ne peut être utilisé comme moyen de preuve
Dans un arrêt du 8 octobre 2014, la Cour de cassation a considéré que les informations collectées par

un système de traitement automatisé de données personnelles avant sa déclaration à la CNIL, constituent un moyen de preuve illicite. Dans cette affaire, une société avait licencié une salariée sur la base d'une utilisation excessive de sa messagerie électronique professionnelle à des fins personnelles (plus de 600 emails privés envoyés et reçus par mois), en se fondant sur des éléments de preuve obtenus grâce à un dispositif de contrôle individuel de l'importance et des flux de messagerie électronique. La salariée a contesté son licenciement et réclamé des dommages et intérêts, au motif que ce dispositif n'avait pas été déclaré à la CNIL par son employeur, comme la loi l'y oblige. L'employeur n'avait procédé à cette formalité qu'après le licenciement. La Cour de cassation, dans une décision du 8 octobre dernier, a accueilli l'argumentaire du demandeur, jugeant que le dispositif automatisé de contrôle individuel de la messagerie des salariés était illicite, à défaut d'avoir été déclaré préalablement à son installation et à son licenciement. Les éléments de preuve du licenciement obtenus par ce dispositif sont donc illicites. En effet, le dispositif doit être conforme au moment de la collecte des informations qui sont utilisées comme moyen de preuve. *(Cour cass., ch. soc. 8 oct. 2014, Mme X. c/ Crédits finance conseils, devenue Finapole)*

Vidéosurveillance – Mise en demeure de la société Apple Retail France par la CNIL
La société Apple Retail France avait été mise en demeure en décembre 2013, dans le cadre du dispositif de vidéosurveillance des salariés, installé au sein d'un magasin Apple Store parisien. La société Apple avait notamment été enjointe de réorienter certaines de ses caméras qui filmaient en permanence des salariés, et de délivrer à ces salariés une information complète.
En février 2014, la société Apple a justifié auprès de la CNIL s'être mise en conformité à la loi. Toutefois, des contrôles supplémentaires menés par les agents de la CNIL au sein d'autres magasins Apple ont révélé des manquements à la loi. La CNIL a notamment constaté que des caméras filmaient des salariés en permanence à leur poste de travail, sans justification particulière. En outre, l'information des salariés relative à la mise en place d'un tel dispositif de surveillance s'avérait insuffisante. Dès lors, la surveillance des salariés a été considérée comme disproportionnée au regard de la finalité de prévention des atteintes aux personnes et aux biens. Ce constat a conduit la Présidente de la CNIL à mettre en demeure la société Apple de modifier, dans un délai de deux mois, l'intégralité des dispositifs de vidéosurveillance de l'ensemble de ses 16 magasins français. (*Décision de la Présidente de la CNIL n°2014-051 du 14 octobre 2014 mettant en demeure la société Apple Retail France exploitant les magasins Apple Store).*

PROPRIÉTÉ INTELLECTUELLE

1. RÉGLEMENTATION

Ordonnance du 12 novembre 2014 modifiant les dispositions du code de la propriété intellectuelle sur le contrat d'édition
Une ordonnance vient de modifier le code de la propriété intellectuelle concernant le contrat d'édition, afin de prendre en compte l'édition numérique (e-books notamment). La notion de contrat d'édition comprend désormais l'édition de l'œuvre au format papier et l'édition au format numérique. Les conditions de cession de l'œuvre devront, le cas échéant, distinguer clairement entre la cession des droits sous forme papier, et la cession des droits sous forme numérique. L'auteur devra percevoir une juste rémunération en cas d'exploitation de l'œuvre sous forme numérique. Ces dispositions sont entrées en vigueur le 1er décembre 2014. *(Ordonnance n°2014-1348 du 12 novembre 2014 modifiant les dispositions du code de la propriété intellectuelle relatives au contrat d'édition)*

2. JURISPRUDENCE

Cybersquatting – Vente-privée.com obtient la condamnation du transfert du nom de domaine Venteprivees.fr
La société Vente-privée.com avait constaté qu'un particulier était titulaire du nom de domaine "venteprivees.fr". Ce nom de domaine permettait l'accès à un site internet constitué de liens hypertextes publicitaires et proposant des services identiques ou similaires aux produits et services désignés par la marque Vente privée. La société Vente-privée.com avait également relevé que ce particulier percevait une rémunération à chaque fois qu'un internaute se re-dirigeait vers un site internet commercial lié. La société Vente-privée.com a décidé d'assigner le particulier pour contrefaçon de ses marques notoires, demander sa condamnation à cesser toute exploitation du nom de domaine litigieux et réaliser le transfert de ce nom de domaine à son profit. Dans une décision du 23 juillet 2014, le Tribunal de grande instance de Lyon a fait droit aux demandes de la société Vente-privée.com. Le Tribunal a jugé que le nom de domaine litigieux constituait une imitation quasi

identique des marques de la demanderesse et qu'il y avait en conséquence, un risque d'association évident entre ce nom de domaine et les marques notoires antérieures de la société Vente-privée.com. Les faits de contrefaçon sont donc établis. Par ailleurs, le Tribunal a constaté que le défendeur était coutumier de ce genre de pratiques et qu'il avait fait l'objet de plusieurs condamnations par l'OMPI pour enregistrement frauduleux de noms de domaines. Sa mauvaise foi était donc caractérisée. *(TGI Lyon, 23 juillet 2014, Vente-privée.com / M. W)*

Marques – L'usage d'une marque sur Facebook à titre d'enseigne ne constitue pas une contrefaçon

Une société exploite des discothèques sous l'enseigne Vip Room à Paris, Saint-Tropez et Cannes et est titulaire de la marque VIP ROOM. Ayant appris qu'un DJ utilisait cette marque sur sa page Facebook pour faire la promotion de son activité, l'exploitant des discothèques a assigné le DJ devant le Tribunal de grande instance de Paris. La demanderesse fondait son action sur la contrefaçon de la marque VIP ROOM et sollicitait, outre des mesures d'interdiction, la condamnation du défendeur au paiement de 50.000 € en réparation des atteintes portées à sa marque et de la somme de 30.000€ en réparation de l'atteinte portée à son nom commercial et à son enseigne. Cependant, dans un jugement en date du 25 septembre 2014, le Tribunal n'a pas fait droit à ces demandes.

En effet, les juges ont constaté que le défendeur rendait compte de son activité de DJ sur une page Facebook "fan", où les visiteurs ont la possibilité de poser des questions ou de faire des commentaires, ce qui permettait à son titulaire d'animer une discussion sur ses réalisations. Le Tribunal en a déduit que la page Facebook du DJ constituait un instrument de promotion de son activité professionnelle de DJ et que la dénomination VIP ROOM était donc utilisée dans le contexte de la vie des affaires.

Cette dénomination était par ailleurs toujours suivie des lieux "St-Tropez" et "Cannes", d'où on pouvait en déduire qu'elle ne visait pas des services mais l'établissement où le DJ avait exercé son activité. Cet usage de la dénomination Vip Room ne saurait être considéré comme étant fait à titre de marque, mais à titre d'enseigne. Enfin, le Tribunal n'a relevé aucune confusion sur l'origine des services puisque la mention "VIP ROOM" désigne effectivement les établissements de la société propriétaire de la marque. *(TGI Paris 3e ch., 4e section, 25 septembre 2014, JR Connect et Night Management Production / M. Eliott S. alias DJ El'S).*

Marques – Annulation des marques descriptives Seloger

Les sociétés Se loger.com et Pressimo on Line éditent et exploitent le site internet Seloger.com, proposant des annonces immobilières. Ces sociétés sont titulaires de six marques verbales et semi-figuratives, dont Se Loger et SeLoger.com. Ces sociétés reprochaient à un mandataire immobilier indépendant, spécialisé dans la vente de biens immobiliers, l'usage des termes « se loger pas cher », « se loger moins cher » et « se loger immo » comme noms de domaine et enseignes pour son activité. Après une mise en demeure restée infructueuse, les sociétés ont décidé d'assigner cet indépendant devant le Tribunal de grande instance de Paris, en contrefaçon des marques sus-mentionnées et en concurrence déloyale et parasitaire. Pour sa défense, l'indépendant a invoqué la nullité des marques enregistrées par les demanderesses, au motif que celles-ci ne seraient pas distinctives, mais auraient un caractère usuel et descriptif des services proposés par les demanderesses (relatifs au domaine de l'immobilier). La Cour d'appel a accueilli en partie les arguments du défendeur en prononçant la nullité de deux marques Seloger sur six, jugées effectivement descriptives. La Cour rappelle à ce titre que l'article L.712-2 du Code de la propriété intellectuelle dispose qu'un signe ne peut être valablement enregistré en tant que marque s'il est dans le langage courant la désignation nécessaire, générique ou usuelle du produit ou service ou s'il peut servir à désigner une caractéristique du service. En outre, la Cour a rejeté les demandes des deux sociétés au titre de la contrefaçon et de la concurrence déloyale et parasitaire. *(CA Paris, pôle 5, ch.1, 14 octobre 2014, Janny B. / Pressimmo On Line et Sa Se Loger.com)*

CYBERCRIMINALITÉ ET PÉNAL DU NUMÉRIQUE

1. RÉGLEMENTATION

OIV – L'Anssi réunit les premiers groupes de travail dédiés à la préparation des règles de sécurité

La loi de programmation militaire du 18 décembre 2013 comporte des dispositions spécifiques à la protection des infrastructures vitales contre la cybermenace. Parmi ces dispositions, l'article 22 de la Loi prévoit notamment que le Premier ministre fixe des référentiels de sécurité nécessaires à la protection des systèmes d'information des opérateurs (OIV).

Dans un communiqué du 28 octobre 2014, l'Agence nationale de la sécurité des systèmes d'information (Anssi) a annoncé que les premiers groupes de travail avaient commencé leur concertation. Ces travaux concernent les secteurs de l'énergie et des communications électroniques. Concernant les autres secteurs d'activité (eau, finances, transports, etc.), les groupes de travail doivent être mis en place début 2015. L'Anssi précise dans son communiqué que l'objectif de ce « *travail collectif est de définir les systèmes d'information concernés et des règles efficaces, soutenables et adaptées aux métiers et spécificités des opérateurs, et de garantir la bonne articulation de ce nouveau dispositif avec les réglementations préexistantes* ». *(Loi n°2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et Communiqué Anssi « Cybersécurité et loi de programmation militaire : préparation des règles de sécurité », 28 octobre 2014).*

Décret – Publication du décret fixant les conditions de l'accès administratif aux données de connexion

Le décret d'application de l'article 20 de la loi de programmation militaire, portant sur l'accès administratif aux données de connexion, a été publié le 24 décembre 2014. Cet article consacrant la possibilité pour les services de l'Etat d'accéder aux données, sans décision judiciaire, avait fait l'an passé l'objet d'une vive polémique. Il concerne précisément l'accès aux données de connexion détenues par les opérateurs de télécommunications électroniques, au titre de la sécurité nationale, de la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France ou de la prévention du terrorisme, de la criminalité et de la délinquance organisées.

Le décret crée un nouveau chapitre dans le Code de la sécurité intérieure. Il définit notamment les données de connexion pouvant être recueillies (identité de l'utilisateur ; date, heure et durée de la communication ; identité de son destinataire). Il dresse la liste des services relevant des ministres chargés de la sécurité intérieure, de la défense, de l'économie et du budget, dont les agents individuellement désignés et dûment habilités peuvent demander à accéder aux données de connexion (la DGSI, la DGSE, la direction générale de la police nationale, la direction centrale de la police judiciaire, la direction du renseignement militaire).

Le décret prévoit, en outre, les conditions de désignation et d'habilitation de ces agents. Il précise également les modalités de présentation des demandes d'accès en temps différé comme en temps réel, de conservation de ces demandes ainsi que de décision. En cas de décision favorable, il prévoit les conditions de transmission et de conservation des données recueillies.

Enfin, des dispositions prévoient l'indemnisation des coûts supportés par les opérateurs de communications électroniques, les fournisseurs d'accès à internet et les hébergeurs lors de la mise en œuvre de la procédure. Ce décret est entré en vigueur le 1er janvier 2015. *(Décret n°2014-1576 du 24 décembre 2014 relatif à l'accès administratif aux données de connexion)*

Contenus illicites sur internet – La DGSI a désormais accès aux contenus signalés via la plateforme Pharos

Dans le cadre de la lutte contre la cybercriminalité, le gouvernement a lancé en 2009 le portail internet Pharos (Plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements). L'objectif de cette plateforme est de fournir aux internautes et acteurs de l'internet un moyen simple de signaler tout contenu ou comportement illicite, accessible via internet. Tout type de contenu contraire à la loi peut être notifié (atteinte aux droits d'auteur, injure, diffamation, incitation à la haine raciale, apologie du terrorisme, etc.). Ces signalements sont traités par les policiers et gendarmes de l'OCLCTIC (Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication), qui ont pour mission de recueillir les notifications, d'effectuer des rapprochements entre les signalements et, si les contenus et comportements dénoncés s'avèrent effectivement illicites, de les orienter vers les services enquêteurs compétents.

Parmi les enquêteurs autorisés à accéder aux signalements et aux informations y afférentes, figurent les agents des directions générales de la police nationale, de la gendarmerie nationale, des douanes, de la concurrence et la répression des fraudes ainsi que ceux attachés aux finances publiques.

Un arrêté du 4 novembre 2014 vient compléter cette liste et offre désormais la possibilité aux agents de la direction générale de la sécurité intérieure (DGSI, ex-DCRI) de consulter les informations traitées par le système Pharos. La DGSI, dont les trois missions principales sont le contre-espionnage, la lutte contre le terrorisme et la protection du patrimoine économique, pourra ainsi utiliser les informations liées aux différents signalements à des fins d'enquête. *(Arrêté 4 nov. 2014 modifiant l'arrêté du 16 juin 2009 portant création d'un système dénommé « Pharos » et Portail Pharos : https://www.internet-signalement.gouv.fr/)*

2. JURISPRUDENCE

Usurpation d'identité – Première condamnation pour usurpation d'identité numérique

Dans cette affaire, un informaticien avait créé un faux "site officiel" de la députée-maire Rachida Dati, qui reprenait sa photo et la charte graphique du site officiel et permettait aux tiers de publier des commentaires sous la forme de communiqués de presse parodiques, soi-disant rédigés par la députée-maire. Ces communiqués étaient diffusés avec la mention « groupe Pipe » au lieu de « groupe PPE ». L'internaute se trouvait en fait sur le site officiel, très similaire au faux site. L'auteur de cette usurpation avait utilisé une faille de sécurité du site de la députée-maire, permettant d'y injecter du code indirect (opération dite "XSS" ou cross-site scripting).

Le directeur du Cabinet de Madame Dati a déposé plainte contre X pour usurpation d'identité sur support numérique et atteinte aux systèmes de traitement automatisé de données. L'enquête, menée par la BEFTI (Brigade d'enquête sur les fraudes aux technologies de l'information), a permis d'identifier l'auteur des agissements.

Dans un jugement du 18 décembre 2014, le Tribunal de grande instance de Paris a retenu les deux chefs d'accusation à l'encontre du prévenu. Le Tribunal considère en effet, que l'identité de Madame Rachida Dati avait été numériquement usurpée, dans la mesure où *« ces mentions* [« je vous offre un communiqué... » ou « merci pour ce geste citoyen »], *aux côtés du nom de Madame Rachida Dati et sur un site reprenant la photographie officielle de la député-maire, sa mise en page et sa charte graphique, ne peut que conduire l'internaute à opérer une confusion avec le site officiel de celle-ci »*. Par ailleurs, le Tribunal a retenu que l'auteur du faux site avait mis en place un dispositif permettant la mise en ligne par les internautes de faux communiqués au contenu sexiste et dégradant. Or, en sa qualité de modérateur du site, il avait la possibilité de fermer son site ou de désapprouver les termes des commentaires mis en ligne par les internautes. Le prévenu a également été considéré coupable d'introduction frauduleuse de données dans un système de traitement de données, du fait d'avoir exploité la faille de sécurité du site officiel pour y introduire des instructions dans le but d'en modifier son comportement. Condamné à une amende de 3.000€, l'auteur du faux site a fait appel de la décision. *(TGI Paris, 13e ch. correctionnel, 18 décembre 2014, MP c/ X.)*

Abus de confiance – Détournement de fichiers informatiques professionnels par un salarié

Un salarié a informé son employeur, un cabinet de courtage d'assurances, de son intention de démissionner de son emploi de chargé de clientèle en vue de rejoindre un cabinet de courtage concurrent. Alors que celui-ci effectuait son préavis, l'employeur a effectué un contrôle interne, permettant d'établir que le salarié avait utilisé sa messagerie électronique professionnelle pour transférer sur sa boîte mail personnelle un grand nombre de fichiers confidentiels à usage interne de la société. L'employeur a donc décidé de poursuivre le salarié pour détournement de plus de trois cents fichiers informatiques qui lui avaient été remis dans le cadre d'un usage professionnel déterminé, conformément à la charte informatique de l'entreprise.

Dans un arrêt du 5 février 2013, la Cour d'appel de Bordeaux avait retenu la culpabilité du salarié. La Cour avait notamment soulevé que le salarié « *s'était délibérément abstenu de solliciter des responsables de la société l'autorisation d'extraire ces données et de les conserver à des fins privées, sans doute conscient du refus qui lui serait opposé en raison de la date programmée de son départ et du risque de leur exploitation au bénéfice d'un concurrent ; que ces pratiques de captation clandestine déployées en violation de l'engagement de confidentialité qu'il avait signé, comme tous les salariés de l'entreprise, suffisaient à caractériser l'abus de confiance* ».

Le salarié s'est pourvu en cassation. Dans un arrêt du 22 octobre 2014, la Cour de cassation a rejeté le pourvoi du salarié aux motifs que "*le prévenu a, en connaissance de cause, détourné en les dupliquant, pour son usage personnel, au préjudice de son employeur, des fichiers informatiques contenant des informations confidentielles et mis à disposition pour un usage professionnel, la cour d'appel, qui a caractérisé en tous ses éléments, tant matériel qu'intentionnel, le délit d'abus de confiance, a justifié sa décision*". L'auteur des faits a été condamné à payer 2.500€ de dommages et intérêts à son ancien employeur. *(Cour cass., ch. crim., 22 octobre 2014, Thierry X.)*

VIE DU CABINET

1. PARTENARIAT

Depuis quelques mois, le Cabinet a développé un **partenariat avec le Cabinet Adven**. Ce partenariat nous permet de proposer un éventail de compétences élargi à nos clients. En sus des domaines relevant des nouvelles technologies, les avocats du Cabinet Adven apportent des compétences complémentaires dans les domaines du droit privé et public des affaires : droit des sociétés et des

fusions/acquisitions, droit fiscal des affaires, droit public, droit du travail et droit de la santé. (http://www.advenlegal.com/fr/)

2. ASSOCIATION

Dans le cadre du développement de notre activité vers l'Asie du Sud-est, le Cabinet est membre de la Chambre de Commerce Française de Singapour (French Chamber of Commerce in Singapore : http://www.fccsingapore.com)

3. PUBLICATIONS

Betty Sfez a été interviewée par Isabelle Duriez, journaliste, pour l'article "*Drones : ça arrive près de chez vous*", publié dans Elle magazine du 12 décembre 2014.

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

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