LA LETTRE DU CABINET
TECHNOLOGIES DE L'INFORMATION

EDITO

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

Cette Newsletter est organisée autour des thématiques suivantes : Informatique, Internet, Protection des données personnelles, Propriété intellectuelle, Cybersécurité, 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.

Nous vous souhaitons une bonne lecture !

SOMMAIRE

INFORMATIQUE

1. PROGICIEL DE GESTION INTÉGRÉE

Jurisprudence – Résolution d'un contrat d'installation d'un ERP pour manquement à l'obligation d'information incombant au professionnel

Un cabinet d'avocat avait signé un contrat d'installation d'un progiciel de gestion intégrée avec la société Secib, prestataire informatique. Le progiciel devait comporter une interface entre le logiciel d'agenda du cabinet et l'agenda électronique Ical de l'iPhone d'Apple, permettant de synchroniser les deux systèmes. Or, la fonctionnalité de synchronisation n'a pas été opérationnelle lors de l'installation de l'ERP. Le cabinet a assigné le prestataire afin de réclamer la résolution judiciaire du contrat et l'indemnisation du préjudice subi du fait du dysfonctionnement partiel du progiciel (période de formation inutile et perte de temps pour essayer de travailler avec un système non synchronisé). Le cabinet invoquait le non-respect par le prestataire de son obligation d'information et de conseil et l'absence de délivrance conforme du progiciel au contrat, la compatibilité du logiciel avec l'application iCal constituant une fonctionnalité essentielle pour le client.

Dans une décision du 13 mai 2014, le Tribunal de grande instance de Paris a prononcé la résolution judiciaire du contrat, ordonné la restitution, par le prestataire, des sommes versées (13.600€) et accordé au client des dommages et intérêts (1.500€). Selon le tribunal, le prestataire devait, en sa qualité de professionnel, s'enquérir des spécificités de son client. Le prestataire ne pouvait valablement soutenir qu'il appartenait à son client de préciser que la fonctionnalité litigieuse de synchronisation d'agendas était essentielle, sachant que cette fonctionnalité était effectivement essentielle, en l'espèce, au regard de l'activité professionnelle du client. *(TGI Paris, 5ème ch., 1ère section, 13 mai 2014, Cabinet d'avocats Dufour Iosca c/ Secib)*

2. CLOUD COMPUTING

Référentiel de sécurité – Publication par l'Anssi d'un projet de RGS pour la qualification des prestataires de services en Cloud

L'Agence Nationale de la Sécurité des Systèmes d'Information (Anssi) a publié un projet de référentiel général de sécurité (RGS) auquel les prestataires Cloud devront se conformer s'ils souhaitent obtenir une « qualification ». Ce document concerne les prestataires fournisseurs de services Cloud - en mode SaaS, PaaS ou IaaS, et ce quelque soit le profil de leurs clients (administrations, collectivités territoriales, OIV, entreprises privées, etc.). Le projet de RGS définit les exigences de sécurité ainsi que les recommandations (ou bonnes pratiques) que les prestataires Cloud devront respecter pour obtenir la qualification. Ces exigences seront vérifiées dans le cadre d'un audit des lieux liés à la prestation visée par la qualification. Ce document vise à donner aux clients, utilisateurs de services Cloud, des garanties quant à la compétence du prestataire, à la qualité de ses services et à la sécurité du traitement des données qui lui sont confiées. Le référentiel a ainsi pour objectif de favoriser l'émergence et la promotion d'offres de services sécurisées qualifiées et ainsi, garantir un niveau de confiance envers les prestataires qualifiés - même si le RGS est avant tout destiné aux administrations. L'Anssi a lancé un appel public à participation sur ce projet et invite les prestataires Cloud à lui adresser des commentaires et remarques sur ce projet de référentiel avant le 3 novembre 2014. *(Référentiel de qualification de prestataires de services sécurisés d'informatique en nuage (cloud computing) - référentiel d'exigences », Anssi, version du 30.07.2014).*

3. OPEN DATA

Réglementation - Publication du décret instituant le Chief data officer de l'Etat

Le décret instituant un administrateur général des données a été publié le 16 septembre 2014. L'administrateur général des données (ou "Chief data officer") sera en charge de plusieurs missions pour le compte de l'Etat : la coordination de l'action des administrations en matière d'inventaire, de

gouvernance, de production, de circulation et d'exploitation des données par les administrations, et l'amélioration de leur exploitation et leur circulation, dans le respect des règles applicables aux données personnelles et des secrets protégés par la loi (tel que le secret défense). Placé sous l'autorité du Premier ministre, l'administrateur général des données aura pour rôle de proposer des stratégies d'exploitation des données publiques, y compris en s'appuyant sur des entreprises innovantes ; il sera en charge de l'élaboration d'outils, de référentiels et de méthodologies permettant d'améliorer l'exploitation des données et le développement des sciences des données au sein des administrations ; il adressera à la direction interministérielle des systèmes d'information et de la communication de l'Etat ses recommandations en matière de cadres techniques de référence pour accroître l'interopérabilité des systèmes d'information et des données, y compris en travaillant à leur sémantisation. Henri Verdier a été nommé à cette fonction, en parallèle de la direction d'Etalab (en charge la politique open data en France). *(Décret n°2014-1050 du 16 septembre 2014 instituant un administrateur général des données)*

INTERNET

1. RÉGLEMENTATION

Dématérialisation – Adoption d'un règlement européen sur l'identification électronique et les services de confiance pour les transactions électroniques

Le 23 juillet 2014, le Conseil de l'Union européenne a adopté un règlement en matière d'identification électronique (« règlement eIDAS »). Ce texte établit le socle du marché européen de la "confiance numérique" pour les transactions sécurisées entre les citoyens, les entreprises et les autorités administratives. Il fixe les règles relatives d'une part, à l'identification électronique et d'autre part, aux services de confiance (signature électronique, cachet, horodatage, services d'envoi recommandé électronique, authentification de site internet et documents électroniques) et au régime juridique des prestataires de services de confiance.

- *Concernant l'identification électronique*, ce règlement vise à garantir un niveau adéquat de sécurité des moyens d'identification électronique et des services de confiance dans l'Union européenne afin d'assurer la reconnaissance mutuelle de ces moyens d'identification par les Etats membres. Les démarches administratives seront ainsi possibles dans toute l'Union avec le développement des téléservices et l'obligation pour les Etats membres de reconnaître les moyens d'identification électroniques des usagers venant d'autres Etats membres.
- *Concernant les Prestataires de Services de Confiance européens* (PSCO), le règlement pose des exigences de sécurité et une obligation de contrôle régulier ; il crée également un label de confiance de l'Union pour les services de confiance qualifiés.
- Ce texte est entré en vigueur le 17 septembre 2014. Toutefois, la plupart des dispositions ne seront pas applicables avant le 1er juillet 2016. *(Règlement (UE) n°910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE)*

Crowdfunding - Nouveau régime juridique du financement participatif, entré en vigueur le 1er octobre 2014

- Le cadre juridique du financement participatif a été défini par une ordonnance du 30 mai 2014. Cette ordonnance vient combler l'absence de règles adaptées au crowdfunding en créant deux nouveaux statuts juridiques : le Conseiller en Investissement Participatif (CIP) et l'Intermédiaire en Financement Participatif (IFP). La mise en œuvre de ce nouveau régime vient d'être précisée par l'adoption d'un décret et de plusieurs arrêtés publiés en septembre dernier. Ces textes, entrés en vigueur le 1er octobre 2014, apportent de nombreuses précisions sur les modalités du prêt et les compétences et obligations des conseillers et intermédiaires en financement participatif.
- Le CIP désigne les plateformes qui permettent, via la fourniture d'un conseil en investissement, la collecte de fonds en vue de la souscription de titres pour les SAS. Le CIP est soumis à une obligation d'immatriculation auprès de l'ORIAS (registre unique des intermédiaires en assurance, banque et finance), à des règles de bonne conduite dans la présentation des risques aux utilisateurs, s'apparentant à un devoir de mise en garde, à des conditions d'accès et d'exercice, à une obligation d'adhésion à une association chargée du suivi de ses membres ainsi que, plus globalement, au contrôle de l'AMF.
- L'IFP consiste à mettre en relation, au moyen d'un site internet, les porteurs d'un projet déterminé et les personnes finançant ce projet. La délivrance du statut d'IFP est soumise à l'immatriculation auprès de l'ORIAS, au respect de règles de transparence, de bonne conduite et d'organisation ainsi que

d'information aux prêteurs des risques encourus.
Les CIP et IFP devront également souscrire un contrat d'assurance couvrant les conséquences pécuniaires de leur responsabilité civile professionnelle avant le 1er juillet 2016.
- L'ordonnance introduit également une dérogation au monopole bancaire en permettant aux particuliers de consentir des prêts rémunérés aux porteurs de projets, à la seule condition d'avoir été mis en relation avec ce porteur par le biais de l'IFP. Concernant les *modalités du prêt* : pour les prêteurs, le montant des prêts rémunérés est plafonné à 1.000 euros par prêteur et par projet, et le montant des prêts sans intérêt est plafonné à 4.000 euros ; Pour les porteurs de projets, le montant d'emprunt est plafonné à 1 million d'euros. La durée d'un prêt rémunéré ne pourra aller au-delà de 7 ans. Enfin, plusieurs informations complémentaires doivent être intégrées aux sites internet des IFP. *(Ordonnance n°2014-559 du 30 mai 2014 relative au financement participatif, Décret d'application n°2014-1053 du 16 septembre 2014 et les arrêtés associés des 22, 24 et 30 septembre 2014)*

E-commerce – Publication du décret d'application de la Loi Hamon relatif à l'obligation d'information précontractuelle des consommateurs
La loi du 17 mars 2014 relative à la consommation (dite « Loi Hamon »), transposant la directive du 25 octobre 2011 relative aux droits des consommateurs, a redéfini l'obligation générale d'information précontractuelle des consommateurs. Toutefois, la loi renvoyait à un décret d'application en ce qui concerne le contenu précis des informations que le professionnel doit communiquer aux consommateurs avant la conclusion de tout contrat. Ce décret d'application a été publié le 17 septembre 2014 ; Il détaille les informations générales à communiquer, *d'une part*, sur les lieux de vente avant la conclusion d'un contrat ou un acte d'achat et, *d'autre part*, préalablement à la conclusion d'un contrat à distance. Les informations portent notamment sur l'identité des professionnels, leurs activités, les garanties légales et commerciales, les fonctionnalités et interopérabilité des contenus numériques et certaines conditions contractuelles. Pour les contrats conclus à distance, le décret précise les informations supplémentaires devant être communiquées. Par ailleurs, tout professionnel de la vente à distance doit désormais mettre à disposition des consommateurs un formulaire de rétractation. Le décret d'application comprend en annexe un modèle de formulaire de rétractation pouvant être utilisé par les e-commerçants ainsi que les informations à fournir aux consommateurs en matière d'exercice du droit de rétractation (modalités de la rétractation, montant et modalités de remboursement, etc.). (*Décret n°2014-1061 du 17 septembre 2014 relatif aux obligations d'information précontractuelle des consommateurs et au droit de rétractation)*

Jeux en ligne – Publication du rapport d'activité 2013 de l'Autorité de régulation des jeux en ligne (Arjel)
Dans son rapport annuel 2013, rendu public en septembre dernier, l'Arjel fait le constat que le marché des jeux d'argent et de hasard en ligne, bien qu'il continue à évoluer, et que chacun de ses trois segments (paris sportifs, hippiques et poker) fasse preuve d'une dynamique propre, a aujourd'hui atteint une certaine maturité.
- *L'évolution du marché* : « *si l'offre légale est désormais bien installée sur le marché français, elle n'en subit pas moins certains à-coups, liés en particulier aux variations de son périmètre et au calendrier des événements supports de paris (calendrier des compétitions sportives en premier lieu, calendrier et format des tournois de poker, calendrier des courses hippiques)* ». Le nombre de comptes joueurs actifs, qui reflète l'activité de chaque secteur, évolue de manière contrastée d'une année sur l'autre : + 14% pour les paris sportifs, - 1% pour les paris hippiques, et - 9% pour le poker, par rapport à l'année 2012. Enfin, le nombre d'acteurs actifs sur le marché français est en baisse : au 31 décembre 2013, 18 opérateurs restent titulaires de 30 agréments (9 agréments sportifs, 13 agréments poker et 8 agréments hippiques), 1 agrément a été délivré (paris sportifs), 3 ont été abrogés et 1 a été retiré à l'issue d'une procédure de sanction.
- *Contrôle et conformité des sites des opérateurs* : « *le respect des contraintes légales et réglementaires relatives à la présence de messages de mise en garde et de mécanismes de protection des personnes vulnérables fait l'objet d'une surveillance continue* ». Ainsi, sur les 30 sites d'opérateurs en activité, 1067 contrôles ont été réalisés. Deux types de manquements ont été constatés: une typographie non conforme ou une absence d'alternance des messages de mise en garde des risques liés au jeu, et une exemption de saisie de la date de naissance à chacune des connexions sur le compte joueur.
- *Lutte contre les sites illégaux* : il ressort du rapport qu'après 3 ans de lutte contre les sites illégaux, le nombre de nouveaux sites de jeu répertoriés en 2013 est moindre qu'au cours des années précédentes. Au 31 décembre 2013, l'Arjel recensait un peu plus de 2400 sites proposant des offres de paris sportifs, de paris hippiques, de poker ou de jeux de casinos en ligne. Sur ce total, un peu plus

de 2100 sites étaient en conformité avec la législation française. *(Rapport d'activité 2013, Arjel, communiqué du 10 septembre 2014)*

Blocage de sites - projet de loi sur la lutte contre le terrorisme : mesures concernant internet
Après son adoption par l'Assemblée nationale, le projet de loi renforçant les dispositions relatives à la lutte contre le terrorisme est actuellement en cours d'examen au Sénat. Porté par le ministre de l'Intérieur, Bernard Cazeneuve, le projet de loi antiterroriste comporte des dispositions relatives à internet. Ainsi, le projet de loi prévoit à l'article 5, que constitue un acte de terrorisme le fait de préparer la commission d'un des actes de terrorisme mentionnés au code pénal et que cette préparation est caractérisée notamment par le fait de consulter habituellement des sites internet provoquant à la commission d'actes de terrorisme ou en faisant l'apologie. L'article 9 prévoit que, *"lorsque les nécessités de la lutte contre la provocation à des actes terroristes ou l'apologie de tels actes le justifient*", le blocage administratif des sites internet concernés pourra être décidé. Enfin, les forces de l'ordre pourront accéder aux données stockées dans un système informatique tiers dans le cadre de leurs enquêtes en cours. Les réactions à ce projet de loi, qui est examiné en procédure accélérée (une seule lecture par chambre) sont très contrastées : d'une part, ses promoteurs mettent en avant la nécessaire lutte contre le terrorisme et les départs au "jihad" ; d'autre part, plusieurs organismes, dont la Commission nationale consultative des droits de l'Homme (CNCDH) estiment que ce texte porte atteinte aux libertés individuelles. Le texte devrait être adopté dans les prochaines semaines. (*Projet de loi renforçant les dispositions relatives à la lutte contre le terrorisme, enregistré le 2 juillet 2014)*

2. JURISPRUDENCE

Vente en ligne de médicaments – Condamnation de l'exploitant d'un site internet à suspendre la commercialisation de ses produits
- La société Enova Santé, qui exploite le site internet 1001pharmacies.com, site de vente en ligne de médicaments a été assignée par le Conseil national de l'ordre des pharmaciens. Le Conseil lui reprochait de procurer aux internautes des médicaments soumis à ordonnance, alors que d'une part, la société Enova Santé n'était pas une officine de pharmacie et que d'autre part, la vente sur internet de médicaments soumis à ordonnance n'est pas autorisée en France.
- Pour sa défense, la société Enova Santé prétendait exercer une activité d'exploitation d'une plateforme internet de mise en relation entre les utilisateurs et les pharmaciens, et la gestion d'un service de livraison de médicaments, vendus par les pharmacies partenaires de la société.
- Par jugement en date du 8 août 2014, le TGI de Paris, statuant en référé, s'est prononcé en faveur du Conseil de l'Ordre. Le Tribunal a considéré que la société Enova Santé jouait un rôle actif dans le commerce électronique de médicaments, alors même que 1001pharmacies.com n'est pas un site de pharmacien inscrit à l'ordre des pharmaciens, ne dispose pas de l'autorisation de l'Agence Régionale de Santé et qu'aucun responsable du site ne disposait de cette double qualité. En outre, la vente en ligne de médicaments sans ordonnance étant réservée aux pharmaciens titulaires d'une officine, le Tribunal a considéré que le trouble manifestement illicite était caractérisé. Le Tribunal a donc enjoint la société de cesser d'offrir à la vente des médicaments (soumis ou non à ordonnance) sur son site 1001pharmacies.com, sous astreinte de 1.000€ par jour de retard. (*TGI Paris, Ordonnance de référé, 8 août 2014, CNOP c/ Enova Santé)*

Obligation d'information – Condamnation de l'éditeur d'un site web pour défaut de mentions légales
Une société avait découvert des commentaires la concernant sur un site internet offrant aux salariés la possibilité de noter anonymement leur employeur (Notetonentreprise). Celle-ci avait, dans un premier temps, réclamé un droit de réponse, puis sollicité en justice l'identification de l'auteur du message ; en vain puisque les coordonnées de la société exploitant le site litigieux ne figuraient pas sur le site web. Or, en application de l'article 6 de la loi pour la confiance dans l'économie numérique (LCEN), il incombe à tout éditeur de site internet de faire apparaître sur le site les informations permettant de l'identifier (mentions légales). La société concernée par les commentaires a donc décidé de porter plainte sur ce fondement.
Les éditeurs du site litigieux ont été identifiés après enquête de la Brigade de Répression de la Délinquance contre la Personne (BRDP). Dans un jugement en date du 11 juillet 2014, le TGI de Paris a condamné chacun des éditeurs à une amende de 6.000€. *(TGI Paris, 11 juillet 2014, MP c/ M.X et M.Y)*

PROTECTION DES DONNÉES PERSONNELLES

1. RÉGLEMENTATION

Systèmes RFID – Adoption de normes techniques par la Commission européenne

La Commission européenne a présenté, le 30 juillet dernier, de nouvelles normes techniques européennes pour aider les utilisateurs de puces intelligentes et de systèmes d'identification par radiofréquence (« RFID ») à respecter les règles et recommandations sur la mise en oeuvre des principes de respect de la vie privée et de protection des données dans les applications reposant sur l'identification par radiofréquence. Ces normes visent à fournir aux entreprises un cadre accessible commun pour la conception et l'affichage de signes de notification d'identification RFID. Un logo européen est également créé, permettant aux consommateurs d'identifier rapidement que les produits qu'ils envisagent d'acheter sont équipés de puces intelligentes. Ce cadre prévoit par ailleurs que les entreprises ou les pouvoirs publics qui utilisent des puces : (i) informent clairement et simplement les consommateurs sur l'utilisation des données personnelles recueillies, (ii) veillent à un étiquetage clair des dispositifs, et (iii) procèdent à des évaluations de l'impact sur la vie privée et la protection des données, contrôlées par les autorités nationales de protection des données, avant d'utiliser des puces intelligentes. *(Normes 16570:2014 « Notification d'identification par radiofréquence (RFID) - Signe informationnel et informations complémentaires devant être délivrées par les exploitants de systèmes d'application d'identification RFID »)*

Objets connectés – Publication d'un avis par le G29

Le G29, organisme regroupant toutes les autorités européennes de la protection des données personnelles, vient de publier un avis sur l'internet des objets (ou objets connectés). Le G29 rappelle que les objets connectés collectent et traitent des données à caractère personnel, au sens de la directive européenne 95/46/CE et qu'à ce titre, le droit européen de la protection des données personnelles leur est applicable. Cet avis comporte des recommandations pratiques à l'attention des différents acteurs impliqués (fabricants d'appareils connectés, développeurs d'applications, plateformes sociales, destinataires ultérieurs des données, etc.), leur permettant de se conformer à la réglementation. L'avis rappelle notamment les droits et obligations incombant aux professionnels et aux utilisateurs des objets connectés, ainsi que les mesures de sécurité à mettre en œuvre par les responsables de traitement. (*Opinion 8/2014 on the Recent Developments on the Internet of Things, Article 29 Data Protection Working Party, 16 September 2014)*

Contrôles CNIL – Précisions sur le nouveau pouvoir de contrôle en ligne de la Commission

La loi Hamon du 17 mars 2014 a notamment modifié la loi Informatique et Libertés et prévoit la possibilité pour les agents de la CNIL d'effectuer, à distance, des contrôles de conformité à la loi Informatique et Libertés. Dans un récent communiqué, la CNIL est venue donner quelques précisions sur la mise en œuvre pratique de ces contrôles de conformité.

- Les étapes du contrôle : la décision de contrôle revient au Président de la CNIL, qui dans un ordre de mission désigne les agents en charge du contrôle. Un procès-verbal décrivant la méthodologie appliquée (environnement technique et vérifications) est rédigé puis envoyé à l'entreprise concernée par le contrôle, qui doit faire part de ses observations dans un délai imparti. A la suite du contrôle, la Commission a la possibilité de poursuivre ses investigations et de prononcer des sanctions.
- Les vérifications : les agents de la CNIL désignés auront pour mission de contrôler la conformité à la loi des traitements mis en œuvre par les entreprises contrôlées, à savoir notamment : la réalisation des formalités préalables, la pertinence des données collectées, l'existence des mentions d'information, la sécurité des données et la bonne gestion des cookies. (*Loi n°2014-344 du 17 mars 2014 relative à la consommation, nouvel article 44 Loi Informatique et Libertés et Communiqué CNIL « Contrôles en ligne : mode d'emploi » du 7 octobre 2014*)

2. DÉCISIONS JUDICIAIRES ET DÉLIBÉRATIONS CNIL

Droit à l'oubli - Condamnation de Google en référé par le TGI de Paris

Par une ordonnance de référé du 16 septembre 2014, le Président du Tribunal de grande instance de Paris a donné effet, pour la première fois, aux principes relatifs au droit à l'oubli posés par la CJUE en mai dernier. Le Président du TGI devait se prononcer sur les demandes de trois personnes physiques qui avaient été victimes de diffamation (reconnue par la justice), qui se plaignaient du fait que les propos jugés diffamatoires étaient toujours en ligne. Les demandeurs avaient vainement sollicité de Google qu'elle supprime les liens de la liste des résultats de son moteur de recherche. Les demandes des trois plaignants étaient expressément fondées sur l'arrêt de la CJUE du 13 mai 2014. Le juge des

référés devait donc dire si le principe posé par la Cour pouvait concrètement trouver application en droit interne. La réponse est positive. Le Juge a relevé que les propos litigieux avaient effectivement été jugés diffamatoires, qu'ils étaient reproduits dans le moteur de recherche de Google et que les sites qui les diffusaient étaient accessibles depuis les résultats du moteur par lien hypertexte. La société Google France a donc été enjointe de supprimer les liens concernés sous astreinte de 1.000€ par jour de retard. *(TGI Paris, Ordonnance de référé, 16 septembre 2014, M. et Mme X et M.Y c/ Google France)*

Failles de sécurité – Avertissement public prononcé par la CNIL à l'encontre de la société Orange

Conformément à son obligation légale de notification des failles de sécurité (violation des données personnelles), la société Orange avait notifié, en avril dernier, à la CNIL une violation de données personnelles, liée à une défaillance technique du serveur de l'un de ses prestataires chargé de réaliser des campagnes de marketing direct. Cette faille de sécurité a eu pour conséquence une fuite de données de près de 1,3 million de clients (nom, prénom, date de naissance, adresse électronique et numéro de téléphone fixe ou mobile). Suite à la notification, la CNIL a réalisé des investigations auprès de la société Orange mais également de ses sous-traitants. Ces contrôles ont révélé plusieurs manquements à l'obligation de sécurité prévue par la loi Informatique et Libertés, à savoir notamment : (i) le fait de ne pas avoir audité, avant sa mise en service, la sécurité d'une application technique permettant la réalisation des campagnes et spécialement adaptée aux besoins d'Orange « *alors que cette mesure lui aurait permis d'identifier la faille de sécurité* », (ii) le fait d'avoir « *envoyé de manière non sécurisée à ses prestataires les mises à jour de ses fichiers clients* » et, enfin, (iii) le fait de ne pas avoir « *veillé à ce que les obligations en matière de sécurité et de confidentialité des données soient répercutées au prestataire secondaire alors même qu'elle connaissait le périmètre d'intervention de ce dernier* ». La CNIL a donc décidé de prononcer un avertissement public, sans sanction pécuniaire. *(Délibération de la formation restreinte n°2014-298 du 7 août 2014 prononçant un avertissement à l'encontre de la société Orange)*

Géolocalisation – Condamnation d'une société par la CNIL pour la mise en œuvre d'un dispositif non conforme à la loi

La CNIL avait reçu une plainte d'un client de la société Loc Car Dream, société de location de véhicules de luxe. La plainte portait sur le système de géolocalisation mis en place par la société de location. Le client dénonçait le caractère excessif des données recueillies et traitées par ce dispositif, mis en œuvre sans déclaration, ni information préalable. Après avoir adressé plusieurs courriers à cette société, restés sans réponse, la CNIL a décidé d'effectuer un contrôle dans les locaux de la société. Ce contrôle ayant révélé de nombreux manquements à la loi, la Commission a mis en demeure la société de : (i) procéder aux formalités préalables pour les traitements relatifs à la géolocalisation et à la gestion des clients, (ii) limiter la collecte des données de géolocalisation aux situations de non restitution et de vols, (iii) d'informer les clients de la mise en œuvre des deux traitements précités, et (iv) de définir une politique sécurisée de gestion des mots de passe. Cette mise en demeure n'ayant pas été suivie d'effet, une procédure de sanction a été engagée et la CNIL a décidé de prononcer une sanction pécuniaire de 5.000€ à l'encontre de la société de location. *(Délibération n°2014-294 du 22 juillet 2014 prononçant une sanction pécuniaire publique à l'encontre de la société Loc Car Dream)*

Vidéosurveillance – Condamnation d'une société par la CNIL pour la mise en œuvre d'un dispositif de non conforme à la loi

La CNIL avait reçu une plainte de l'Inspection du travail de la région Rhône-Alpes, concernant les conditions de mise en œuvre de dispositifs de vidéosurveillance de la société Providis Logistique. A la suite de plusieurs contrôles ayant révélé de nombreux manquements à la loi, la Commission a décidé de mettre en demeure la société. Cette dernière a fait part de ses observations à la CNIL, et a indiqué avoir corrigé certaines défaillances. Toutefois, de nouveaux contrôles sur place dans les locaux de la société concernée ont révélé la persistance des manquements, notamment relatifs à la proportionnalité des dispositifs de vidéosurveillance. La Commission a relevé que : (i) la société continuait à filmer de manière continue certaines zones réservées aux salariés (accès aux vestiaires et aux locaux affectés au repos des salariés), sans qu'aucune justification particulière ne puisse légitimer une telle atteinte à la vie privée des salariés concernés, (ii) l'information relative à ces dispositifs était incomplète et (iii) les mesures de sécurité permettant de garantir la confidentialité des données issues des traitements déployés étaient insuffisantes. La CNIL a donc prononcé une sanction pécuniaire de 5.000€ à l'encontre de la société Providis Logistique. (*Délibération n°2014-307 du 17*

juillet 2014 prononçant une sanction pécuniaire à l'encontre de la société Providis Logistique)

3. Safe Harbor

Etats-Unis - Saisine de la FTC pour non-respect des principes du Safe Harbor par 30 sociétés
Le Center for Digital Democracy (CDD), organisme américain de défense de la vie privée, a déposé plainte et fait une demande d'enquête auprès de la Federal Trade Commission (FTC) concernant 30 sociétés américaines qu'elle soupçonne de ne pas respecter les principes du Safe Harbor.
Pour rappel, le Safe Harbor comporte les règles relatives à la protection des données personnelles. Ce système, négocié entre les autorités américaines et la Commission européenne en 2001, permet aux entreprises européennes d'exporter des données personnelles vers les sociétés américaines qui déclarent adhérer aux principes du Safe Harbor. La plainte du CDD, déposée le 14 août 2014, demande à la FTC d'engager des procédures à l'encontre des sociétés en cause, dont les sociétés Adobe Systems, AOL, Criteo et Salesforce et plusieurs sociétés de marketing en ligne, pour violation des règles du Safe Harbor. Les irrégularités constatées porteraient notamment sur : i) la complexité de leurs politiques sur la protection des données personnelles, difficilement compréhensibles pour un consommateur moyen, ii) la non-conformité des pratiques de ces sociétés concernant la qualification de sous-traitant (data processor) alors que, compte tenu de leur niveau de contrôle des procédés mis en place, ces sociétés sont en réalités des responsables de traitement (data controller), iii) des procédures de désinscription (opt-out) ineffectives, iv) des données personnelles non réellement anonymisées, et v) des informations incomplètes concernant les traitements de données, particulièrement dans le cadre des activités de marketing en ligne et de traitements de données dans un contexte de Big Data. *("CDD urges FTC to investigate 30 companies for alleged Safe Harbor violations", Michael Young, Alton & Bird LLP – Privacy & Data Security Blog, 18 août 2014 ; Safe Harbor principles : http://www.export.gov/safeharbor/ ; site du CDD : www.democraticmedia.org)*

Propriété Intellectuelle

Jurisprudence – Annulation d'une marque non exploitée, similaire à une marque notoire
- La société Free, titulaire de plusieurs noms de domaine et de marques sous cette dénomination, a découvert qu'un particulier avait enregistré une marque verbale « Free-Sport TV » et le nom de domaine associé. Après une mise en demeure restée sans réponse, la société Free a assigné le particulier pour demander la nullité de la marque, le transfert du nom de domaine et des dommages et intérêts en réparation des atteintes aux marques, dénomination sociale, nom commercial et noms de domaine dont la société Free est titulaire. La société Free a été déboutée en première instance au motif qu'il ne pouvait exister de contrefaçon ni d'atteinte quelconque en présence d'une marque et d'un nom de domaine non exploités.
- Toutefois, la société Free a obtenu gain de cause en appel. En effet, par un arrêt du 9 septembre 2014, la Cour d'appel de Paris a estimé que la reprise sans nécessité du terme Free, connu pour identifier le FAI, afin de procéder au dépôt d'une marque désignant des services quasiment similaires aux activités notoirement exercées par la société Free, constituait une négligence fautive. Selon la Cour, le défendeur ne pouvait ignorer que le signe choisi, comprenant les mots free et TV, évoquerait nécessairement les activités du FAI, car pour un consommateur moyen normalement attentif, le terme free est associé au FAI. L'usage de ce terme dans une marque constitue ainsi une atteinte préjudiciable aux droits antérieurs détenus par la société Free. La Cour a donc annulé la marque litigieuse, et condamné le défendeur à verser 2.000€ de dommages et intérêts à la société Free. *(CA Paris, Pôle 5, ch. 1, 9 septembre 2014, Sas Free c/ Vanessa M.)*

Jurisprudence – Condamnation du titulaire d'un nom de domaine non exploité, similaire à une marque renommée
- La société Red Bull GmbH avait refusé d'accorder une licence d'importation et de distribution de sa boisson sur le territoire de la Réunion à un particulier. Ce dernier avait néanmoins enregistré le nom de domaine « redbull.re ». Considérant que ce nom de domaine portait atteinte à ses marques et à ses noms de domaine, la société Red Bull a mis en demeure le particulier. Sans réponse de celui-ci, la société Red Bull a déposé une demande de transfert de nom de domaine auprès de l'Afnic. Cette demande a été rejetée, l'Afnic estimant que la mauvaise foi du titulaire du nom de domaine n'était pas établie. Ensuite, la société RedBull a adressé un courrier au particulier afin de trouver une solution amiable ; en réponse ce dernier a donné son accord pour le transfert contre le versement d'une somme de 130.000€.

- La société Red Bull a donc assigné ce dernier et obtenu gain de cause, par jugement du TGI de Paris en date du 23 mai 2014. Le Tribunal a considéré qu'en réservant le nom de domaine litigieux, son titulaire avait porté atteinte à la marque verbale renommée Red Bull. Selon le Tribunal *« le consommateur est en effet amené à penser que le site accessible par ce nom de domaine émane de la société Red Bull ou à tout le moins est économiquement lié à lui, de sorte que son contenu lui sera attribué. Il importe peu que le site ne soit pas exploité comme c'est le cas du site* (litigieux) *car l'absence d'exploitation peut être considérée par le consommateur comme un signe de désaffection qui sera là encore imputé à la société Red Bull. Enfin, le nom de domaine en cause se trouve de fait indisponible pour celle-ci qui se trouve dès lors empêchée d'exploiter un nom de domaine pourtant construit identiquement à d'autres sites qu'elle exploite, notamment www.redbull.fr ».* Le Tribunal a donc ordonné le transfert du nom de domaine litigieux, sous astreinte de 500€ par jour de retard et a condamné le particulier à verser 5.000€ de dommages-intérêts à la société Red Bull GmbH. *(TGI Paris 3e ch., 2e section, 23 mai 2014, Red Bull GmbH c/ Mohamed B.)*

CYBERSÉCURITÉ

Bitcoins – Publication du rapport Tracfin sur l'encadrement des monnaies virtuelles
La cellule Tracfin du ministère des Finances a publié, le 11 juillet dernier, le rapport de son groupe de travail sur l'encadrement des monnaies virtuelles. Dans un premier temps, le rapport souligne les trois caractéristiques de ce type de monnaie, sources de risques : l'intervention d'acteurs non régulés, le manque de transparence et l'extraterritorialité. Le rapport liste ensuite les risques d'utilisations illicites ou frauduleuses liés au développement des monnaies virtuelles : l'opacité des transactions, l'absence de garantie de la volatilité du cours, l'absence de dispositif de protection du consommateur ainsi que la fraude et le blanchiment des capitaux. Enfin, le rapport propose des pistes de réglementation avec notamment l'adoption de plusieurs mesures: 1) limiter l'anonymat des utilisateurs de monnaie virtuelle ; 2) clarifier le régime fiscal des monnaies virtuelles ; 3) limiter et plafonner l'utilisation des monnaies virtuelles en tant que moyen de paiement ; 4) adopter le dispositif de lutte contre le blanchiment d'argent et le financement du terrorisme aux risques posés par les monnaies virtuelles ; 5) harmoniser, aux niveaux européen et international, la régulation des plateformes qui échangent des monnaies virtuelles contre des devises officielles et 6) améliorer la connaissance du secteur et le suivi des risques. *(Rapport sur l'encadrement des monnaies virtuelles, Recommandation visant à prévenir leurs usages à des fins frauduleuses ou de blanchiment, publié le 11 juillet 2014)*

Europol – Création du J-CAT, groupe de travail de lutte contre la cybercriminalité
Le 1er septembre dernier, Europol, organisme inter-gouvernemental permettant aux services de police des différents Etats membres de collaborer et coordonner leurs actions dans certains domaines (tels que stupéfiants, terrorisme, pédophilie), a annoncé la création du J-CAT (Joint Cybercrime Action Taskforce), groupe de coordination dédié à la lutte contre la cybercriminalité dans l'Union européenne et à l'international. Les principaux contributeurs à ce groupe de travail, hébergé au centre de cybercriminalité européen (EC3) d'Europol seront, dans un premier temps, une partie des Etats membres, auxquels s'ajouteront les Etats-Unis et le Canada. La cybercriminalité ne connaissant pas les frontières terrestres, l'objectif du J-CAT sera de coordonner les enquêtes sur les principaux réseaux cybercriminels. Le J-CAT fonctionnera pendant une période d'essai de six mois. *(Communiqué de presse Europol du 1er septembre 2014 "Expert international cybercrime taskforce is launched to tackle online crime")*

VIE DU CABINET

1. PUBLICATIONS

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

2. ASSOCIATION, FORMATION ET CONFÉRENCE

Le Cabinet participe aux travaux de la Commission « Financement » de l'association EuroCloud. Dans le cadre de ces travaux, nous avons publié un document intitulé « *Grands principes relatifs à la*

réglementation française sur le prix » (http://www.eurocloud.fr/grands-principes-relatifs-reglementation-francaise-prix/)

Par ailleurs, le Cabinet a animé, les 6 et 9 octobre derniers :

- une formation intitulée « *Gérer la qualité dans les contrats de prestations* », organisée par l'organisme de formation Comundi ;
- une conférence intitulée « *La création d'une entreprise technologique : les bons reflexes juridiques à avoir* », en partenariat avec le Cabinet Adven, au Salon des Nouvelles Technologies et des Entrepreneurs de Strasbourg.

Enfin, Betty Sfez a été interviewée par Caroline Piquet, journaliste, pour l'article "*Comment policiers et gendarmes pourraient bientôt utiliser des drones*", publié le 7 octobre 2014 dans Le Figaro

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