LA LETTRE DU CABINET
TECHNOLOGIES DE L'INFORMATION

EDITO

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

Cette Newsletter est organisée autour des thématiques suivantes : un flash spécial sur le projet de règlement européen sur la protection des données et sur la loi pour la République Numérique, puis des points sur la réglementation ou la jurisprudence dans les domaines du le droit de l'internet, de la protection des données personnelles, de la propriété intellectuelle, la santé numérique, la banque et finance, le droit des affaires, la cybercriminalité et le droit pénal et enfin la vie du Cabinet. Nous souhaitons par ce moyen vous informer des derniers développements du droit des technologies de l'information.

Si vous le souhaitez, merci de nous faire part de vos impressions, critiques ou suggestions.

Nous vous souhaitons une bonne lecture.

SOMMAIRE

ⓘ FLASH – ACCORD DE PRINCIPE SUR LE PROJET DE RÈGLEMENT EUROPÉEN SUR LA PROTECTION DES DONNÉES PERSONNELLES

Près de quatre ans après la première publication du projet de règlement européen sur la protection des données personnelles, ayant pour objet d'unifier le droit de la protection des données dans l'Union européenne, un accord de principe a enfin été trouvé le 15 décembre 2015 à l'issue d'un dernier trilogue. Cet accord est l'aboutissement des discussions menées par les trois institutions européennes (le Parlement européen, le Conseil et la Commission européenne) débutées en juin 2015.

Ces discussions se sont accélérées depuis l'été 2015 avec dix réunions du trilogue. Ces réunions ont permis d'avancer, étape par étape vers un accord global sur une version définitive du règlement. Parmi les nouvelles dispositions de ce règlement, il convient de rappeler les principes suivants :
- le droit à la portabilité des données depuis un service numérique vers une autre plateforme ;
- la consécration du droit à l'oubli numérique ;
- la possibilité pour les internautes de contester la publicité ciblée ;
- le principe de la mise en place de responsables de la protection des données dans les entreprises ;
- la simplification des procédures en cas de litige, avec la saisine de l'autorité de régulation (CNIL par exemple) du pays du siège de l'entreprise.

En outre, deux points majeurs sont à relever :
- Le montant des sanctions applicables aux responsables de traitement sont fortement relevés : les sociétés, responsables de traitement, qui violeraient le droit européen de la protection des données personnelles seront passibles de sanctions pouvant atteindre 20 millions d'euros, ou une sanction pécuniaire maximale de 4% du chiffre d'affaires mondial de la société en cause.
- L'accord parental requis pour l'inscription des mineurs sur des services en ligne : jusqu'à présent, le projet de règlement ne comportait que quelques dispositions, figurant dans les considérants, relatives aux mineurs. L'article 8 du projet de règlement vient d'être modifié afin de renforcer la protection des mineurs sur internet. A compter de l'entrée en vigueur du règlement, les jeunes de moins de 16 ans ne pourront plus s'inscrire sur un service en ligne sans l'accord parental. Cette disposition vise tous les services en ligne collectant des données personnelles et notamment la messagerie, les réseaux sociaux et les plateformes de téléchargement.

Le règlement doit encore être validé par le Parlement européen début 2016 et par les Etats membres. Il entrera en vigueur deux ans après son adoption, soit courant 2018. *(Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data - Analysis of the final compromise text with a view to agreement - Interinstitutional File: 2012/0011 (COD) – Brussels – 15 December 2015)*

ⓘ FLASH – ADOPTION EN PREMIÈRE LECTURE DU PROJET DE LOI SUR LA RÉPUBLIQUE NUMÉRIQUE PAR L'ASSEMBLÉE NATIONALE

Le projet de loi pour une République numérique a été déposé à l'Assemblée nationale le 9 décembre 2015. Le 26 janvier 2016, l'Assemblée a adopté en première lecture un texte qui vient notamment modifier et compléter la loi Informatique et Libertés. Les principaux points à retenir concernant la protection des données personnelles sont les suivants :

- Principe fondamental : l'article 1er de la loi Informatique et Libertés serait complété comme suit : « *Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi* ». Ce principe, mentionné dans le premier article de la loi (projet), illustre la volonté du gouvernement de faire de la protection de la vie privée un droit fondamental.

- Information des personnes concernées : la loi Informatique et Libertés oblige le responsable de traitement à informer les personnes concernées par la collecte et le traitement de leurs données sur l'identité du responsable du traitement, la finalité du traitement, le caractère obligatoire ou facultatif des réponses au formulaire de collecte, le cas échéant l'identité des destinataires des données et des éventuels transferts de données hors Union européenne. Le projet de loi a ajouté une sixième mention sur la durée de conservation des catégories de données traitées.

- Effacement des données relatives aux mineurs : le projet de loi prévoit qu'à la demande de la personne concernée, le responsable de traitement serait tenu d'effacer - dans les meilleurs délais - les données collectées lorsque la personne concernée était mineure au moment de la collecte. A défaut d'effacement dans un délai d'un mois à compter de la demande, la CNIL pourra être saisie.

- "Mort numérique" : le projet de loi intègre de nouvelles dispositions permettant aux personnes concernées d'organiser le traitement de leurs données après leur mort. Des directives d'ordre général peuvent ainsi être enregistrées auprès d'un tiers de confiance numérique, certifié par la CNIL. Des directives plus précises peuvent aussi être enregistrées directement auprès des responsables de traitement.

- Action collective : le projet de loi ouvre le droit à une action collective permettant à certaines personnes d'obtenir la cessation d'une violation des données personnelles devant une juridiction civile. L'exercice de ce type d'action est subordonné à l'accomplissement de démarches préalables auprès du responsable de traitement concerné. Les personnes ayant qualité à agir comprennent les associations de protection de la vie privée, les associations de défense des consommateurs, les organisations syndicales de salariés, etc.

- Sanctions : actuellement, la CNIL peut prononcer une sanction pécuniaire d'un montant maximum de 300.000€ en cas de manquement à la loi Informatique et Libertés. Le projet de loi prévoit une augmentation sensible des sanctions pouvant atteindre 20 millions d'euros ou, dans le cas d'une entreprise, 4% du chiffre d'affaires total au niveau mondial. Ces montants correspondent à ceux figurant dans le projet de règlement européen. Certains manquements, tels le défaut de formalités préalables, le manquement à la sécurité des données ou la défaillance du sous-traitant, sont soumis à des sanctions « moins lourdes », pouvant atteindre 10 millions d'euros ou 2% du chiffre d'affaires annuel total au niveau mondial.

Le projet de loi pour une République numérique a été transmis au Sénat, dans le cadre d'une procédure accélérée (une seule lecture par chambre). Le texte définitif devrait donc être adopté dans les prochains mois. *(Projet de loi pour une République numérique, adopté en 1ère lecture par l'Assemblée nationale le 26 janvier 2016, TA n° 663.)*

INTERNET

1. JURISPRUDENCE

Responsabilité – Le directeur de la publication est responsable des contenus modérés par un sous-traitant

Dans cette affaire, un internaute avait posté un commentaire suite à un article concernant un parti politique, publié sur le site Lefigaro.fr. Considérant les allégations de l'internaute diffamatoires, l'un des représentants du parti politique concerné en a demandé la suppression au moyen de la fonctionnalité de modération proposée sur le site. La modération du site Lefigaro.fr est effectuée par

un prestataire externe. Bien que le service de modération ait répondu avoir fait le nécessaire pour supprimer le commentaire litigieux, celui-ci est cependant resté accessible en ligne.
Après avoir renouvelé sa demande de retrait, le représentant du parti politique concerné a déposé plainte contre le directeur de la publication du site Lefigaro.fr pour diffamation publique.
Pour sa défense, le directeur de la publication affirmait que du fait de l'externalisation des tâches de modération à un prestataire, il n'avait pas été personnellement alerté du contenu litigieux et il ne pouvait de ce fait voir sa responsabilité pénale engagée.
Toutefois, le directeur de la publication a été reconnu responsable par la chambre criminelle de la Cour de cassation. Dans un arrêt du 3 novembre 2015, la Cour a considéré que le prévenu ne pouvait se prévaloir de l'externalisation du service de modération pour échapper à son « devoir de surveillance » du contenu qu'il publie. *(Cass., ch. criminelle, 3 novembre 2015, n° de pourvoi 13-82645)*

Responsabilité - La société exploitant le site Leboncoin.fr condamnée pour pratique commerciale trompeuse
La société Goyard St-Honoré, fabricant d'articles de bagagerie de luxe, avait découvert la présence d'annonces proposant la vente de produits contrefaits de la collection Goyard sur le site Leboncoin.fr. Ces annonces faisaient état, sans équivoque, de la nature contrefaisante des produits, à savoir : « pochette Goyard fausse », « porte passeport imité parfaitement » ou « portefeuille inspiré Goyard ».
Après plusieurs signalements en ligne de contenus illicites et mises en demeure restés sans réponse, la société Goyard St-Honoré a assigné la société LBC France, exploitant le site Leboncoin.fr, devant le Tribunal de grande instance de Paris sur les fondements suivants :

- pour pratiques commerciales trompeuses, du fait de ne pas avoir respecté ses engagements contractuels. En effet, la défenderesse indiquait expressément dans ses CGU qu'elle relit et modère les contenus mis en ligne, et refuse ou supprime les annonces contraires aux dispositions légales ;
- pour contrefaçon par reproduction des marques Goyard, du fait de la diffusion d'annonces sur le site Leboncoin.fr de produits de maroquinerie sous la dénomination Goyard ;
- pour atteinte à sa dénomination sociale, à son nom commercial, à son enseigne et négligence fautive.

A ce titre, la société Goyard demandait l'interdiction pour la défenderesse de reproduire ou faire usage sur son site de toute dénomination reproduisant les marques Goyard. La demanderesse réclamait également la condamnation de la société LBC France à 80.000€ de dommages et intérêts.
Pour sa défense, la société LBC France soutenait qu'elle n'intervenait que comme intermédiaire dont l'activité est purement technique et passive, et qu'elle endossait à ce titre la qualité d'hébergeur de contenu. Or, à défaut d'avoir été notifiée, dans les formes prévues par la loi, de la présence de contenus illicites sur son site web, les actes de contrefaçon invoqués à son encontre ne pouvaient lui être imputés.
Dans sa décision du 4 décembre 2015, le Tribunal de grande instance de Paris a condamné la société LBC France pour pratique commerciale trompeuse de nature à induire le consommateur en erreur sur la portée de son engagement. Les juges ont ainsi retenu que le site Leboncoin.fr mentionnait expressément dans ses CGU que "(…) *toutes les annonces sont relues avant mise en ligne afin de s'assurer de leur qualité et du respect des règles de diffusion* (…)", et que "(…) *toute annonce contenant des éléments du texte* (…) *qui sembleraient contraires aux dispositions légales* (…) *sera refusée par le Leboncoin.fr*".
Le Tribunal a par ailleurs débouté la société Goyard de ses demandes en contrefaçon et sur l'atteinte aux signes distinctifs de son entreprise. La société LBC France a été condamnée à la publication du jugement dans plusieurs journaux, magazines et sur son propre sites web. *(TGI Paris, 3ème ch., 2ème section, 4 décembre 2015, Goyard St-Honoré c/ LBC France)*

Parasitisme économique – Condamnation pour reproduction des pages d'un site web et de ses CGV
La société Sound Strategy, proposant notamment des services de messagerie destinés à l'accueil téléphonique des PME, via le site www.studio-loxcost.com, a découvert que l'un de ses anciens actionnaires, gérant de la société Concepson, proposait des services concurrents via son site www.myphonestudio.com. La société Sound Strategy a décidé d'assigner son concurrent sur le fondement de la concurrence déloyale parasitaire, la société Concepson ayant lancé un site web dont l'agencement et les conditions générales de vente étaient similaires à ceux de Sound Strategy. La demanderesse soutenait que son concurrent avait indûment tiré profit des importants investissements

qu'elle avait réalisés pour la création de son site web et réclamait ainsi près de 55.000€ de dommages et intérêts.
Pour sa défense, la société Concepson a tenté de démontrer la banalité du site internet litigieux, comme de ses CGV.
Dans son jugement du 28 septembre 2015, le Tribunal de commerce de Paris a condamné la société Concepson. Après avoir rappelé que la concurrence parasitaire *« requiert la circonstance selon laquelle, à titre lucratif et de façon injustifiée, une personne morale ou physique s'inspire ou copie une valeur économique d'autrui, individualisée et procurant un avantage concurrentiel, fruit d'un savoir-faire, d'un travail intellectuel et d'investissement »*, les juges ont relevé de nombreuses similitudes entre les deux sites et leurs CGV, l'absence d'investissement spécifique de la défenderesse pour le développement de son propre site et l'infériorité des tarifs qu'elle propose.
En outre, les juges ont considéré que la banalité du concept du site internet développé par la société Sound Strategy n'est pas *« de nature à démontrer l'absence de parasitisme »*, le seul fait de s'inspirer de la valeur économique d'une autre société qui a réalisé des investissements étant suffisant à qualifier un agissement parasitaire. Il convient de noter que l'acte de concurrence déloyale était d'autant plus caractérisé en l'espèce que le dirigeant de Conception avait participé à la création du site web de Sound Strategy, à l'époque où il était encore actionnaire de cette société.
En conséquence, le Tribunal de commerce a condamné la société Conception au paiement de 5.000€ de dommages et intérêts au bénéfice de Sound Strategy, montant bien inférieur à celui réclamé, la société Sound Strategy n'ayant pu démontrer une quelconque diminution de son chiffre d'affaires ou de profit du fait de ces actes de parasitisme. *(Tribunal de commerce de Paris, 15ème chambre, 28 septembre 2015, Sound Strategy c/ Concepson)*

PROTECTION DES DONNÉES PERSONNELLES

1. RÉGLEMENTATION

Transfert de données vers les Etats-Unis - Accord « EU-US Privacy Shield » en remplacement des règles du Safe Harbor

Le 6 octobre 2015, la Cour de justice de l'Union européenne (CJUE) invalidait les règles de Safe Harbor de transfert des données vers les Etats-Unis. Les règles du Safe Harbor (ou Sphère de sécurité) permettaient aux entreprises situées dans l'Union européenne de transférer des données personnelles vers des entreprises américaines adhérentes au Safe Harbor. Considérant que les Etats-Unis, depuis les révélations de 2013 concernant leurs activités de renseignement (affaires Snowden), ne garantissaient plus une confidentialité suffisante des données, la CJUE a invalidé le dispositif existant, bloquant ainsi les transferts vers les Etats-Unis réalisés sous ce système. Les membres du G29 (regroupant les autorités européennes de protection des données personnelles) ont alors enjoint les institutions européennes et les autorités américaines de trouver des solutions juridiques et techniques visant à pallier cette insécurité juridique, au plus tard pour le 31 janvier 2016.
Le 2 février, la Commission européenne a annoncé qu'un accord avait été trouvé avec ses homologues américains. Le texte de l'accord, dénommé « EU-US Privacy Shield » (bouclier vie privée), a été rendu public le 29 février. Les principales dispositions du dispositif Privacy Shield sont les suivantes : (1) les entreprises américaines devront publier leurs engagements, dont le respect sera contrôlé par le ministère américain du commerce et la Federal Trade Commission (FTC) ; (2) l'accès aux données par les autorités américaines à des fins d'ordre public et de sécurité nationale sera strictement encadré, limité, et contrôlé, excluant ainsi toute surveillance de masse ; (3) les droits des citoyens européens seront renforcés en offrant notamment plusieurs recours à toute personne estimant que ses données sont utilisées de manière abusive (dépôt de plaintes, procédure extrajudiciaire gratuite et accès à un médiateur).
Toutefois, l'accord Privacy Shield n'est pas encore applicable. La Commission européenne doit donner son avis sur la décision d'adéquation de cet accord au regard du droit européen. En attendant, les entreprises peuvent continuer à utiliser les outils juridiques existants pour encadrer leurs transferts de données personnelles vers les Etats-Unis : règles internes d'entreprise (BCR) pour les multinationales, clauses contractuelles types (CCT) préconisées par la Commission européenne ou contrats privés de transferts de données. *(Commission européenne, communiqué de presse du 29 février 2016, « la Commission européenne présente le paquet «bouclier de protection des données UE-États-Unis»: des garanties solides pour restaurer la confiance dans les transferts transatlantiques de données »)*

2. JURISPRUDENCE

Délibération CNIL – La société Facebook mise en demeure pour manquement à la loi

En novembre 2014, Facebook avait annoncé une révision de ses conditions générales d'utilisation et de sa politique de confidentialité. Cinq autorités de protection (France, Belgique, Pays-Bas, Espagne et le Land de Hambourg en Allemagne) au sein du G29 (groupe des "CNIL" européennes) ont formé un groupe de travail, et décidé de mener des investigations.

Pour les besoins de son enquête, ce groupe de travail ("Groupe de contact") s'est notamment appuyé sur un jugement du Tribunal de première instance de Bruxelles, du 9 novembre 2015. Ce jugement a enjoint à Facebook de cesser l'enregistrement, via des cookies et plug-ins (boutons sociaux), de la navigation des internautes résidant en Belgique et ne disposant pas de compte Facebook, sans information préalable. A défaut, le Tribunal a prévu une astreinte de 250.000 euros par jour.

Facebook dépose un cookie sur le terminal de tout internaute qui se rend sur une page du site facebook.com (pour visiter la page publique d'un événement, par exemple), même si cette personne n'est pas inscrite sur Facebook. Une fois ce cookie déposé, à chaque fois que l'internaute visite une page contenant un plug-in Facebook (un site d'actualités, par exemple), le réseau social procède à la lecture du cookie et est ainsi informé de la visite de cet internaute sur ce site. Alors que Facebook indique que ce cookie est utilisé pour assurer la sécurité de son service et de ses utilisateurs, il lui permet également de suivre la navigation, hors de son site, d'internautes non inscrits.

Aussi, dans une déclaration commune du 4 décembre 2015, le Groupe de contact a demandé à Facebook de prendre les mesures nécessaires pour respecter la décision du Tribunal belge, et ainsi se mettre en conformité avec la législation européenne sur tout le territoire européen.

C'est dans ce contexte que la CNIL a effectué des contrôles sur place et en ligne pour vérifier la conformité du réseau social Facebook à la loi Informatique et Libertés. Ces vérifications ont permis de relever de nombreux manquements à la loi.

Outre la collecte d'informations concernant les non-membres, il apparaît que le réseau social ne recueille pas le consentement exprès des internautes lors de la collecte et du traitement des données relatives à leurs opinions politiques, ou religieuses, et à leur orientation sexuelle. De même, aucune information n'est délivrée aux internautes sur leurs droits et sur l'utilisation qui sera faite de leurs données sur le formulaire d'inscription au service.

La Commission relève ensuite que le site dépose sur l'ordinateur des internautes des cookies à finalité publicitaire, sans les en avoir informés au préalable, ni avoir recueilli leur consentement.

Enfin, Facebook transfère les données personnelles de ses membres vers les Etats-Unis en vertu des règles du Safe Harbor, invalidées par la Cour de Justice de l'Union Européenne le 6 octobre 2015.

La CNIL a donc décidé de mettre en demeure les sociétés Facebook Inc. et Facebook Ireland de se conformer à la loi dans un délai de 3 mois. A défaut, la CNIL pourrait prononcer une sanction à l'égard de ces sociétés. *(Déclaration commune des autorités de protection des données personnelles membres du Groupe de contact, du 4 décembre 2015 et Délibération n°2016-007 du 26 janvier 2016 mettant en demeure les sociétés Facebook Inc. et Facebook Ireland)*

Délibération CNIL - Condamnation d'Optical Center pour défaut de sécurité des données clients

En 2014, la CNIL a reçu une plainte d'une cliente de la société Optical Center, dénonçant la communication par téléphone de son mot de passe par la société, laissant ainsi supposer que les mots de passe des comptes clients étaient stockés en clair dans la base de données. La CNIL a donc procédé à une mission de contrôle, au cours de laquelle elle a constaté des manquements à la loi. Optical Center a fait l'objet d'une mise en demeure de se conformer à la loi dans un délai d'un mois.

En raison de la persistance de certains manquements, la CNIL a lancé une instruction et prononcé une sanction pécuniaire de 50.000€ à l'encontre de la société pour manquements à la loi concernant la sécurité des données. La société n'avait pas mis en place les mesures adaptées pour assurer la sécurité et la confidentialité des données de ses clients (170.000 comptes utilisateurs sur le site Optical Center).

A ce titre, la CNIL a notamment relevé une absence de sécurisation de la page d'accueil permettant à l'utilisateur de se connecter à son compte et de la page lui permettant de modifier son mot de passe, ainsi que l'absence de politique de gestion des mots de passe pour l'accès aux postes informatiques des salariés.

La CNIL exige en l'espèce la mise en oeuvre d'un chiffrement du canal de communication, une authentification du site distant lors de l'accès au site web, et l'amélioration de la robustesse des mots de passe de ses clients et salariés.

Le second manquement concerne la sécurité et la confidentialité des données, gérées par un sous-traitant de la société. La CNIL a relevé que le contrat conclu entre Optical Center et son sous-traitant

ne comportait aucune clause relative à la sécurité et à la confidentialité des données. La société a donc été enjointe d'insérer une clause de ce type, définissant de manière claire les obligations de son prestataire vis-à-vis des données personnelles. *(Délibération de la formation restreinte de la CNIL n°2015-379 du 5 novembre 2015 prononçant une sanction pécuniaire à l'encontre de la société Optical Center)*

Décision du Conseil d'Etat - Un loueur de véhicule considéré comme responsable du traitement de géolocalisation

Dans une délibération du 22 juillet 2014, la CNIL avait prononcé une sanction pécuniaire, rendue publique, d'un montant de 5.000€ à l'encontre de la société Loc Car Dream, société de location de voitures de luxe. La Commission reprochait à cette dernière le non-respect de son obligation légale d'accomplir des formalités de déclaration préalable, nécessaires à la mise en oeuvre du traitement des données personnelles relatif à la géolocalisation des véhicules. La CNIL reprochait également à la société Loc Car Dream de ne pas avoir informé les utilisateurs des véhicules de la présence d'un dispositif de géolocalisation, ni d'avoir assuré la sécurité des données collectées, et enfin de ne pas avoir veillé à l'adéquation, à la pertinence, et au caractère non excessif des données collectées et traitées.

Contestant cette décision, la société Loc Car Dream a déposé une requête devant le Conseil d'Etat et a demandé l'annulation de la délibération CNIL. Elle soutient en effet que son rôle consiste simplement à mettre à la disposition de tiers des véhicules et qu'elle ne peut, à ce titre, être considérée comme responsable du traitement des données relatif à la géolocalisation. De ce fait, il ne lui incombe pas de respecter les obligations légales issues de la loi Informatique et Libertés dont les manquements lui sont reprochés par la CNIL.

Dans une décision du 18 décembre 2015, le Conseil d'Etat a rejeté cet argumentaire et débouté la société Loc Car Dream. Le Conseil a relevé que l'ensemble des données collectées via le dispositif de géolocalisation des véhicules était accessible depuis un seul poste de travail, dont le mot de passe était détenu par l'épouse du gérant de la société Loc Car Dream, situé à l'accueil commun à l'ensemble des sociétés des propriétaires des véhicules. En outre, le Conseil a constaté que la société Loc Car Dream avait déclaré à la CNIL un traitement destiné à « *géolocaliser les véhicules utilisés par les employés* ».

En conséquence, le Conseil d'Etat a considéré que la société Loc Car Dream déterminait les finalités et les moyens du traitement des données, et devait à ce titre être qualifiée de responsable de traitement. La sanction prononcée par la CNIL est donc justifiée. *(Conseil d'Etat, 10ème / 9ème SSR, 18 décembre 2015, Loc Car Dream)*

Décision du Conseil d'Etat - Confirmation des sanctions prononcées à l'encontre d'une société pour mise en œuvre disproportionnée d'un système de vidéosurveillance

Dans cette affaire, un salarié de la société PS Consulting avait déposé plainte auprès de la CNIL, du fait de la mise en œuvre au sein de son entreprise d'un système de vidéosurveillance qu'il jugeait particulièrement intrusif. Dans un premier temps, la CNIL a adressé plusieurs courriers à l'employeur, rappelant les obligations légales qui lui incombaient. Ensuite, la Commission a procédé, en moins d'un an, à trois contrôles successifs dans les locaux de la société PS Consulting et y a systématiquement relevé plusieurs manquements à la loi. La Commission a notamment constaté que : (i) les caméras fixaient les postes de salariés, (ii) les salariés et les visiteurs n'avaient pas été informés de la mise en œuvre de ce dispositif dans les formes prévues par la loi, et (iii) le poste de travail permettant d'avoir accès aux images enregistrées était accessible au moyen d'un mot de passe faiblement sécurisé. La CNIL a alors décidé d'appliquer à cette société une sanction pécuniaire de 10.000€, rendue publique.

Contestant cette décision, la société PS Consulting a déposé une requête devant le Conseil d'Etat demandant l'annulation de la délibération CNIL. Dans sa décision du 18 décembre 2015, le Conseil a confirmé l'argumentaire et la sanction prononcée par la CNIL. *(Conseil d'Etat, 10ème / 9ème SSR, 18 novembre 2015, PS Consulting)*.

PROPRIÉTÉ INTELLECTUELLE

1. DROIT D'AUTEUR

Téléchargement illégal - L'administrateur du forum Wawa-Mania condamné à payer plus de 15 millions de dommages et intérêts à plusieurs ayants droit

Wawa-Mania est un forum internet permettant le téléchargement illégal de divers fichiers, notamment des films. Le 2 avril 2015, le tribunal correctionnel de Paris a reconnu le fondateur et administrateur de

la société, coupable de contrefaçon par mise à disposition de liens vers des fichiers de téléchargement illicites, et de travail dissimulé. Il encourt ainsi une peine d'un an de prison ferme et 20.000€ d'amende.
Le 2 juillet 2015, le tribunal correctionnel a rendu sa décision sur le volet civil de l'affaire et a condamné le prévenu au versement d'une somme de plus de 15 millions d'euros aux différents plaignants. Le tribunal a procédé à l'évaluation du préjudice matériel et moral des plaignants sur la base d'éléments objectifs, tels que le nombre de liens de redirection vers les oeuvres, le nombre d'intervenants sur le site, et le nombre de vues. Les montants alloués aux plaignants se répartissent comme suit :

- supérieur à 2.500.000 € : Twentieth Century Fox Film Corporation, Sacem
- entre 2.000.000€ et 1.500.000€ : Disney Enterprise, Inc., Columbia Pictures Industries, Inc., Universal City Studios LLC, Paramount Pictures Corporation
- entre 1.500.000€ et 1.000.000€ : Warner Bros. Inc.
- entre 1.000.000€ et 500.000€ : Microsoft, Société Civile des Producteurs Phonographiques (SCPP)
- entre 500.000€ et 100.000€ : Tristar Pictures Inc.
- inférieur à 100.000€ : Marc Dorcel, Syndicat de l'Edition Vidéo Numérique (SEVN), Fédération Nationale des Distributeurs de Films (FNDF) et l'Agence pour la Protection des Programmes (APP)

(TGI Paris, 31ème ch. correctionnelle n°2, 2 juillet 2015, APP, Sacem, Microsoft et autres c/ D.M.)

2. Base de données

Producteur de base de données – La délicate preuve des « investissements spécifiques »
Le producteur d'une base de données bénéficie d'une protection *sui generis* lorsqu'il rapporte la preuve d'investissements (financiers, matériels ou humains) spécifiques. Dans un arrêt du 12 novembre 2015, la Cour de cassation vient rappeler l'importance de ce critère d'investissement.
En l'espèce, la société Pressimmo On Line, qui édite et exploite le site internet Seloger.com, prétendait que la société Yakaz, spécialisée dans le référencement de petites annonces, procédait à l'extraction, sans son autorisation, de la totalité de sa base de données d'annonces immobilières pour alimenter sa propre base. La société Pressimmo On Line a alors assigné la société Yakaz notamment en réparation de l'atteinte portée à ses droits de producteur de base de données.
Cette demande avait été rejetée par la Cour d'appel de Paris dans un arrêt rendu le 15 novembre 2013. Les juges ont ainsi relevé que la société Pressimmo On Line « *se doit de rapporter la preuve d'investissements spécifiques qui ne se confondent pas avec ceux qu'elle consacre à la création des éléments constitutifs de sa base de données et à des opérations de vérification, purement formelle, pendant cette phase de création consistant à les collecter auprès de professionnels et à les diffuser tels que recueillis de ses clients* ».
Toutefois, la Cour de cassation a censuré les juges du fond pour ne pas avoir suffisamment précisé dans leur décision les investissements qui satisfaisaient ou non aux critères précédemment énoncés. La Cour souligne que « *…le bénéfice de la protection sui generis conférée par les articles L.341-1 du Code de la propriété intellectuelle n'est pas nécessairement subordonnée à la démonstration d'un « apport substantiel » sur les données collectées* » et précise qu'il suffit de rapporter la preuve d'investissements substantiels consacrés à la recherche d'éléments existants et à leur rassemblement dans ladite base. *(Cass., civ. 1ère, 12 novembre 2015, Pressimmo c/ Yakaz)*

Santé Numérique

Réglementation

Loi de modernisation de notre système de santé – Nouvelles dispositions légales relatives au domaine numérique dans la santé
La loi de modernisation du système de santé a été promulguée le 26 janvier 2016. Cette loi comporte plusieurs dispositions relatives au domaine numérique dans la santé :

- Mise en place d'un système national des données de santé : la loi prévoit que les établissements de santé et les mutuelles auront la possibilité de mettre gratuitement à disposition des données de santé ou des données relatives au remboursement des soins. Ces données seront anonymisées à des fins de recherche, d'étude ou d'évaluation, dans un système centralisé. L'objectif de cet « open data de données de santé » est de contribuer à l'information sur la santé, l'offre de soin, les dépenses de santé et enfin permettre une veille sanitaire. La Caisse nationale de l'assurance maladie des travailleurs salariés est nommée responsable du traitement. En outre, l'Institut national des données

de santé, groupement d'intérêt public, sera chargé de veiller à la qualité des données mises à disposition et à leur sécurité.

- Création du dossier médical partagé : les nouvelles dispositions portent création du dossier médical numérique. Ce dossier permettra aux professionnels de santé d'y inscrire toutes les informations relatives à la prise en charge du patient (du diagnostic aux soins), sous réserve du consentement exprès de celui-ci. Le patient pourra également accéder à son dossier médical numérique, rendre certaines informations inaccessibles aux professionnels de santé, et restreindre l'accès de tout ou partie du dossier à certains médecins. Les informations relatives au don d'organes y seront également inscrites. *(Loi n°2016-41 du 26 janvier 2016 de modernisation de notre système de santé)*

E-santé - Nouveau groupe de travail européen en matière de santé connectée

La Commission européenne vient de constituer un groupe de travail sur la santé connectée ou santé mobile (mHealth), dont la tâche sera de rédiger des lignes de conduite visant à améliorer la qualité des données collectées par les applications mobiles de santé. Ce groupe de travail comprend 20 membres, issus de la société civile, de la recherche et de l'industrie. Les lignes de conduite doivent être publiées d'ici la fin de l'année 2016.

Cette initiative fait suite à la publication du livre vert de la Commission sur la santé mobile datant d'avril 2014. L'un des principaux problèmes identifié dans le domaine de la santé connectée concerne la sécurité et la transparence de l'information. La multiplication des applications de bien être et de santé, sans garantie de qualité ni de fiabilité, fait naître des doutes quant à leur réelle utilité.

Les lignes de conduite devant être développées par ce groupe de travail doivent s'appuyer sur des initiatives et bonnes pratiques existantes en Europe, la recherche de critères de qualité et de méthodologies d'évaluation communs devant permettre aux parties prenantes d'évaluer les applications de santé mobile.

Les applications de santé mobile collectent des données personnelles de santé. A l'avenir, ces applications pourront transmettre ces données directement vers les dossiers médicaux électroniques de la personne concernée/patient, le dossier pouvant ensuite être consulté par le professionnel de santé. Il est donc impératif que ces données soient non seulement de qualité, mais également fiables afin que les professionnels de santé puissent prendre des décisions en matière de traitement et/ou de suivi médical. *(European Commission – Digital Single market – Digital Economy and Society « New EU working group aims to draft guidelines to improve mHealth apps data quality » 15/01/2016)*

BANQUE ET FINANCE

1. RÉGLEMENTATION

Règlementation UE - Entrée en vigueur de la nouvelle directive portant sur les services de paiement dite « DSP2 »

Le 25 novembre 2015 le Parlement européen et le Conseil ont adopté la nouvelle directive sur les services de paiement (DSP2), venant réviser la première directive dite « DSP1 », adoptée en 2007. L'objectif de ce texte, qui fait suite à la proposition de la Commission européenne de juillet 2013, renforce la protection des consommateurs, favorise l'innovation et améliore la sécurité des services de paiements.

La DSP2 vise également à lever les obstacles à l'entrée sur le marché pour les nouveaux fournisseurs de services de paiement, tels que les opérateurs de télécommunication, afin notamment de soutenir la croissance du commerce électronique.

Ainsi la DSP2 introduit des évolutions majeures : (a) de nouveaux services d'initiation de paiement entrent dans le champ de la réglementation ; (b) les prestataires fournissant ces services ou « tiers prestataires de paiement » (TPP) devront adopter le statut d'établissement de paiement, et (c) les banques et aux autres PSP gestionnaires de comptes auront l'obligation de donner accès aux comptes à ces fournisseurs tiers pour initier des paiements.

D'autres dispositions sont prévues, à savoir : (i) l'accès non discriminatoire aux systèmes de paiement pour tout prestataire de services de paiement, (ii) l'ouverture non discriminatoire de comptes bancaires pour tout prestataire de services de paiement, (iii) la révision des règles de surfacturation, et (iv) le droit du client à un remboursement sans condition en cas de contestation d'un prélèvement.

Cette directive, entrée en vigueur le 12 janvier 2016, devra être transposée en droit interne par chaque Etat membre avant le 13 janvier 2018. *(Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur)*

DROIT DES AFFAIRES

1. RÉGLEMENTATION

Règlementation UE - Avancée importante de la réforme européenne de la protection du secret des affaires

Le 15 décembre 2015, à la suite d'un « trilogue » entre le Conseil, la Commission et le Parlement européen, un accord a été trouvé sur le texte de la proposition de Directive européenne pour la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires). L'objectif de la future directive est d'assurer une protection améliorée et harmonisée des secrets d'affaires des entreprises. Il s'agit des informations secrètes qui présentent une valeur commerciale et qui ont fait l'objet de mesures destinées à les garder secrètes, telles que les informations d'ordre stratégique (business plan), les informations commerciales (fichiers clients), les informations techniques (savoir-faire) ou les informations marketing (plans de communication).

La proposition de directive prévoit notamment :

- la possibilité de prévenir et de réprimer l'obtention, la divulgation et l'usage illicites d'un secret d'affaires appartenant à autrui. Ainsi, engageront leur responsabilité, non seulement les personnes qui ont obtenu ou capté le secret de façon illicite, mais aussi les personnes qui en feront un simple usage dès lors qu'elles savaient ou ne pouvaient pas ignorer l'origine illicite de l'information ;
- la possibilité d'obtenir - sous certaines conditions - des mesures provisoires et rapides (interdiction, saisie des produits litigieux) dans le cas d'atteinte avérée ou imminente à un secret ;
- l'aménagement des règles de procédure habituelles afin d'éviter la divulgation du secret dans le cadre de la procédure elle-même (huis clos, etc.).

Le texte prévoit néanmoins des limites à cette protection. Ainsi, l'obtention, l'utilisation ou la divulgation d'informations sont considérées comme licites si cela résulte d'une découverte ou d'une création indépendante, d'une opération d'ingéniérie inverse (reverse engineering) ou encore si cela procède de l'exercice du droit des représentants des salariés ou d'autres usages commerciaux honnêtes.

Le texte final devrait être adopté courant 2016. Les Etats membres devront ensuite transposer le texte en droit interne dans un délai de deux ans à compter de l'entrée en vigueur de la directive. *(Proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure - Analysis of the final compromise text with a view to agreement, Interinstitutional File: 2013/0402 (COD), Brussels, 18 December 2015.)*

CYBERCRIMINALITÉ ET DROIT PÉNAL

1. JURISPRUDENCE

Piratage de fichiers clients - Plainte de l'association de consommateurs UFC-Que choisir contre la société Vtech

La société Vtech commercialise des jouets éducatifs destinés aux enfants, certaines gammes de jouets étant connectés. Certains jouets proposent des fonctionnalités permettant l'enregistrement de la voix, la prise de photos ou sont connectés grâce à diverses applications, telles que "Learning lodge", plateforme permettant le téléchargement d'applications proposées par Vtech, ou "Kid Connect", application permettant l'envoi et la réception de messages et photos entre les parents et les enfants.

Un piratage de comptes clients a eu lieu courant novembre 2015 à travers ces deux applications. La France est le deuxième pays le plus touché par ce piratage, après les États- Unis, avec plus de deux millions de comptes piratés en France, et plus de 6 millions de profils d'enfants touchés à travers le monde. Il s'agit d'un des cas de piratage informatique les plus importants de l'année 2015. Les données contenues dans ces deux applications comprennent les adresses email et postales des parents, les adresses IP, l'historique des téléchargements, les photos de profils des enfants ainsi que les dates de naissance. La société Vtech a suspendu les deux applications en cause et a invité les parents à modifier leurs mots de passe. A des fins de prévention, Vtech a étendu la suspension à d'autres services. L'enquête visant à identifier le ou les auteurs de cette attaque informatique et ses motivations est en cours. L'association UFC-Que Choisir a déposé plainte contre la société Vtech. Elle fonde son action sur l'article 226-17 du Code pénal, qui condamne le fait de procéder ou de faire procéder à un traitement de données personnelles, sans mettre en oeuvre les mesures de sécurité prescrites par la loi. UFC-Que Choisir considère en effet que la société Vtech n'a pas mis en oeuvre des moyens suffisants pour sécuriser l'accès aux données de ses clients et jeunes utilisateurs.

(Communiqué UFC-Que Choisir du 21 décembre 2015 accessible sur le site http://www.quechoisir.org/)

Atteinte à un STAD – Condamnation d'un administrateur réseau de la société Tefal

Dans cette affaire, des documents confidentiels appartenant au Directeur des ressources humaines de la société Tefal et emails émis et reçus par ce dernier (portant notamment sur des futurs licenciements) avaient été publié sur le site web de la Confédération Nationale du Travail et dans plusieurs journaux. La société Tefal a porté plainte contre X auprès du procureur de la République du Tribunal de grande instance de Nancy, pour délit d'atteinte au secret des correspondances électroniques, délit d'accès et de maintien dans un système de traitement automatisé de données et recel de ces infractions. Parallèlement à l'enquête menée par la gendarmerie, les disques durs des administrateurs réseaux de la société Tefal ont été saisis et une expertise informatique a été réalisée visant à auditer certains postes de travail et à rechercher des traces numériques de la fraude informatique.

L'enquête et l'expertise informatique ont permis de relever qu'un administrateur réseau, en conflit avec son employeur pour le paiement d'heures supplémentaires, et une inspectrice du travail, également en litige avec la société Tefal, étaient à l'origine de la fuite des documents confidentiels.

Dans une décision du 4 décembre 2015, le Tribunal de grande instance d'Annecy a déclaré l'administrateur réseau coupable d'atteinte à un STAD, au motif qu'il s'est introduit intentionnellement et frauduleusement dans le système informatique de son employeur, dans un cadre extérieur à l'exercice de ses fonctions. Il est en outre reconnu coupable d'interception, d'utilisation et de détournement de correspondances électroniques, et ce même s'il n'a pas accédé directement à la messagerie privée du directeur des ressources humaines de la société Tefal.

L'inspectrice du travail a été déclarée coupable de recel de détournement de correspondances électroniques, et de violation du secret professionnel.

Le Tribunal ne les a cependant condamnés qu'à une peine d'amende de 3.500€ chacun avec sursis, et au paiement de dommages et intérêts d'un montant symbolique de 1€ au profit de la société Tefal.

(TGI Annecy, ch. correctionnelle, 4 décembre 2015, Tefal et autres c. M.M.C. et Mme J.L.)

VIE DU CABINET

PUBLICATIONS ET PRÉSENTATIONS

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

- Transferts de données personnelles vers les Etats-Unis : un bouclier de protection des données pour remplacer la sphère de sécurité
- Drones et concurrence déloyale : illustration d'un conflit entre un nom commercial, des noms de domaine et une marque
- Un accord de confidentialité aux termes trop généraux peut être privé d'effet
- Quelles mesures pour le transfert de données personnelles vers les Etats-Unis après l'invalidation des règles du Safe Harbor par la CJUE ?

Nous avons également commencé à publier un Blog en anglais à destination de nos clients à l'international, accessible à http://dwavocatit.blogspot.com/

- Software license audits challenged in French court
- Personal data transfers from the EU to the US after the cancellation of Safe Harbor by the CJEU
- Drone use regulation: legal perspectives from France and Singapore

Le 28 janvier, le Cabinet a fait une présentation, conjointement avec Singapore Post, à la French Chamber of Commerce in Singapore (FCCS) sur le thème « *Launching and expanding your e-commerce business in SE Asia : legal, operational and other logistic considerations* »

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