Veille juridique d'octobre 2018 de Claire Sambuc

publié le **20/11/2018**, vu **2951 fois**, Auteur : Claire Sambuc

La juriste en droit des nouvelles technologies de l'information et de la communication (NTIC) Claire Sambuc, partage avec vous toutes les actualités juridiques liées à Internet.

Droit des données personnelles

Sanction de la CNIL pour manquement à l'obligation d'assurer la sécurité et la confidentialité des données

CNIL 6 septembre 2018

Une association française s'est vue infligée par la CNIL une amende de 30 000 euros pour avoir manqué à son obligation « *de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès* ». Il lui était reproché un incident de sécurité qui avait permis l'accès à des documents contenant des données à caractère personnel de personnes suivant les cours de français qu'elle dispensait.

Sanction de la CNIL d'une société ayant mis en œuvre un système biométrique destiné à contrôler les horaires de salariés

6 septembre 2018

La CNIL a condamné une société spécialisée dans la télésurveillance d'ascenseurs et de parkings s'est vue condamnée par la CNIL à la somme de 10 000 euros pour avoir eu recours à un "*dispositif de pointage biométrique à des fins de contrôle des horaires de salariés*" sans autorisation. Pour la CNIL la société a considéré que la société avait procédé à « *une collecte de données excessives au regard des finalités pour lesquelles elles étaient collectées* » en rappelant que les données biométriques bénéficient d'un régime particulièrement protecteur.

La particule d'un patronyme en majuscule n'entache pas d'inexactitude les données personnelles de son titulaire

La CNIL avait clôturé la plainte d'un particulier qui reprochait à une société éditrice d'un magazine de ne pas avoir donné suite à sa demande de rectification qui consistait à faire apparaitre la particule de son patronyme en minuscule et non en majuscule dans les fichiers.

Le Conseil d'Etat a considéré que la CNIL n'avait pas méconnu les dispositions sur lesquelles était fondée la plainte et : *"que la graphie en lettres majuscules de la particule du patronyme [du demandeur] n'entachait pas d'inexactitude ses données personnelles et n'entrainait aucun risque de confusion ou d'erreur sur la personne".*

Conseil d'Etat 3 octobre 2018

Accès aux données de connexion justifié même en l'absence d'infractions pénales graves

CJUE 2 octobre 2018

Un homme avait déposé une plainte auprès de la police pour vol de son téléphone. Pour son enquête, la police avait saisi le juge d'instruction afin qu'il ordonne à divers fournisseurs de services de communications électroniques la transmission des numéros de téléphone activés pendant les douze jours suivant le vol avec le code relatif à l'identité internationale d'équipement mobile (code IMEI) du téléphone volé ainsi que les données à caractère personnel relatives à l'identité civile des titulaires ou des utilisateurs des numéros de téléphone correspondant aux cartes SIM activées avec ce code.

Le juge d'instruction a rejeté cette demande au motif que la loi espagnole limitait cette communication de données aux infractions graves.

Une question préjudicielle a donc été posée à la CJUE.

La Cour rappelle que la directive « vie privée et communications électroniques » de 2002 avait énuméré de manière exhaustive des objectifs justifiant un tel accès aux données, dont celui de prévention, de recherche et de poursuites d'infractions pénales. Elle avait toutefois précisé que cet objectif visé pour cet accès devait être en relation avec la gravité de l'ingérence dans les droits fondamentaux que cette opération entraîne.

Pour la Cour, qui applique le principe de proportionnalité, les données visées par la demande d'accès en cause permettaient uniquement de mettre en relation, pendant une période déterminée, la ou les cartes SIM activées avec le téléphone mobile volé avec l'identité civile des titulaires de ces cartes SIM. Il n'y a donc pas d'ingérence « grave » dans les droits fondamentaux des personnes dont les données sont concernées.

Hameçonnage : absence de négligence grave du client nécessaire

Cour de cassation, 3 octobre 2018

Dans cet arrêt, la Cour de cassation rappelle qu'une banque doit rembourser son client qui conteste un achat sur internet, à condition que l'opération ne résulte pas d'une négligence ou manquement grave de ce client.

La Cour a reproché à la décision de proximité d'avoir condamné l'établissement financier à rembourser les sommes contestées sans avoir recherché si le client avait répondu à un courriel d'hameçonnage.

La Cour rappelle qu'un établissement financier, afin de ne pas procéder au remboursement d'une

opération litigieuse, doit apporter la preuve que le client qui nie avoir effectué un achat, a agi frauduleusement ou a communiqué à un tiers ses données personnelles ou identifiants par sa négligence.

2 groupes intervenant dans le domaine de la protection sociale mises en demeure par la CNIL pour détournement des finalités des données des assurés

Lors d'un contrôle auprès des groupes Humanis et Malakoff-Médéric, la CNIL a pu constater que ces entreprises "*utilisent les données personnelles qu'elles détiennent dans le cadre de leur mission d'intérêt général de mise en œuvre des régimes de retraite complémentaire afin de faire de la prospection commerciale pour des produits et services de ces groupes ».*

Pour rappel, un traitement de données personnelles est toujours limité aux finalités prévues et annoncées aux personnes

Les groupes intervenant dans tous les domaines de la protection sociale, pour les entreprises et les particuliers, le détournement des données couvre potentiellement plus de 16 millions de personnes.

Compte tenu du grand nombre de personnes concernées et de la gravité du manquement relevé, la CNIL a décidé de rendre publique cette mise en demeure, laquelle n'est pas une sanction. Aucune suite ne sera donnée si les sociétés des groupes Humanis et Malakoff-Médéric se conforment à la loi dans un délai d'un mois.

DROIT DES MARQUES

Rejet d'enregistrement de la marque verbale « IMESSAGE » pour défaut de caractère distinctif non compensé par l'usage

CA Paris 25 septembre 2018

La société Apple avait formé un recours contre la décision du directeur général de l'INPI qui avait refusé l'enregistrement du signe « IMESSAGE » comme marque verbale. La Cour d'appel a approuvé ce dernier en considérant que le signe « imessage » était identique phonétiquement à « e-message » et que le consommateur pertinent le comprendrait comme un « *message transmis par voie électronique* », de sorte que le signe était dépourvu de caractère distinctif.

Par ailleurs, son usage à la date du dépôt n'étant « *pas suffisamment établi pour compenser l'absence de distinctivité intrinsèque de ce terme* ».

Similitude de noms de domaine : pas de faute en l'absence de distinctivité

TGI Rennes 1 er octobre 2018

Dans cette affaire, une entreprise de déménagement avait créé un site internet Lesartisansdemenageurs.com, et reprochait à une société d'utiliser le nom de domaine Artisans-demenageurs.com.

Déboutée de sa demande sur le terrain de la propriété intellectuelle et du droit des marques, la société avait également agi sur le fondement de la concurrence déloyale, considérant que la quasi similitude des deux noms de domaine était de nature à entraîner un risque de confusion lié au caractère original ou distinctif des éléments reproduits. Pour le tribunal, le caractère distinctif

duquel découlerait le risque de confusion, faisait défaut. En effet, le nom de domaine utilisant les termes d'artisans déménageurs très usités par la profession doit être considéré comme purement descriptif.

Pour le TGI de Rennes, *« les activités sont bien les mêmes, tout du moins en partie, mais les sites réellement différents, et l'absence totale de distinctivité des termes utilisés pour les noms de domaine ainsi que les différences d'apparence, excluent qu'il puisse y avoir le moindre risque de confusion ».*

Le tribunal rappelle que *« les termes nécessaires ou utiles à la désignation ou à la description des produits, services ou activités proposés, appartiennent au domaine public et doivent rester à la disposition de tous si bien que nul ne peut être considéré comme fautif de l'avoir utilisé. »*

DROIT DES CONTRATS

Indivisibilité de contrats de licence de logiciel et de contrat d'intégration

CA Paris 3 octobre 2018

Une société avait fait appel à un prestataire informatique pour la fourniture d'un logiciel avec une prestation d'intégration. Le contrat d'intégration comportait une clause de résiliation pour faute. La société, invoquant des anomalies, des délais non respectés, avait notifié à son prestataire la résiliation du contrat pour faute et demandait le remboursement des sommes réglées pour la licence.

Le client qui avait assigné son fournisseur soutenait en effet qu'il y avait une indivisibilité entre les deux contrats, l'un portant sur la fourniture des licences de logiciel, l'autre sur des prestations d'intégration dudit logiciel. En prononçant la résiliation du contrat d'intégration il devait à son sens obtenir le remboursement du prix des licences.

Il a été débouté de ses demandes, la cour ayant jugé qu'il existait une contestation sérieuse, à savoir que le remboursement des licences était conditionné par la capacité de démontrer au fond une faute du prestataire dans l'exécution du contrat d'intégration.

E-signature : preuve de la validité du contrat

Tribunal d'instance de Nîmes, 18 septembre 2018

Dans cette affaire, une femme ne réglait plus, depuis plusieurs mois, les échéances qu'elle devait à l'établissement de crédit qui lui avait accordé un emprunt.

La question présentée aux juges était de savoir si le contrat était valide. Le juge a rappelé qu'une signature électronique simple était suffisante pour apporter la preuve de la validité d'un contrat, à condition de satisfaire aux conditions de l'article 1367 du code civil (ancien article 1316-4 al.2). Celui-ci dispose que lorsqu'elle est électronique, la signature consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel il s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve du contraire.

ACTUALITES JURIDIQUES

Faille de sécurité Google +

Google va fermer Google + après la découverte d'une faille de sécurité ayant affecté les données d'au moins 500 000 utilisateurs.

Les informations personnelles des comptes étaient accessibles de manière non prévue via l'API. Ce bug inscrit dans le code de Google + est resté en ligne durant 3 ans entre 2015 et 2018. Google l'a découvert en mars lors d'un audit interne et a pris la décision de le corriger sans prévenir ses utilisateurs ou les autorités de régulation. A quelques semaines près, Google n'aurait pas eu le choix de garder ce secret : en Europe, le règlement général sur la protection des données (RGPD) impose de communiquer aux régulateurs de la vie privée la découverte d'une telle faille et d'en informer les utilisateurs en cas de fuite de données.

Google assure cependant n'avoir constaté aucun cas de collecte ou de mauvaise utilisation de ces accès.

Faille de sécurité Facebook

50 millions de comptes Facebook dont moins de 5 millions de comptes européens seraient touchés par la faille de sécurité de Facebook, révélée le 28 septembre 2018 selon l'autorité de protection des données irlandaises. Cette faille ayant permis à des pirates de récupérer les clés d'accès.

Un peu moins de 50 millions de tokens (clé générée lors de la connexion qui permet de ne pas entrer à chaque fois son mot de passe) ont été dérobés en utilisant un défaut dans le code du réseau social. Avec ces éléments, il est possible de récupérer le contrôle total des comptes (y compris de s'identifier sur des sites qui utilisent Facebook comme moyen de s'y connecter). Facebook ne sait pas (encore) si ces tokens ont été effectivement utilisés.

Les données concernées par la faille sont nombreuses car le token permet de prendre le contrôle total du compte : messages privés échangés, photos postées (même celles dont la diffusion a été restreinte par des paramètres de confidentialité), pages aimées, liste d'amis,…

Données personnelles : 33 millions de données compromises entre mai 2018 et octobre 2018 selon la CNIL

Dans un communiqué publié le 16 octobre, La CNIL a dressé le bilan après avoir reçu de nombreux signalements sur des violations de données personnelles : 33 millions de personnes ont vu leurs données personnelles violées entre le 25 mai, date d'entrée en vigueur du RGPD, et le 1er octobre.

La presque totalité de ces signalements sont relatifs à des atteintes à la confidentialité de ces données.

La plupart des violations de données ont pour origine un acte de malveillance, du piratage via un logiciel malveillant ou du hameçonnage.

Facebook déploie de nouveaux outils pour lutter contre le harcèlement

Facebook a annoncé mardi 2 octobre de nouvelles mesures pour lutter contre harcèlement sur sa plateforme.

Voici les mesures qui ont été annoncées :

- Les utilisateurs du réseau auront la possibilité de masquer ou supprimer plusieurs commentaires à la fois sous un post
- Les victimes ne seront plus les seules à pouvoir signaler les personnes qui les harcèlent : les amis pourront le faire anonymement
- La personne ayant vu son message supprimé pourra faire appel de la décision de Facebook et demander une révision supplémentaire.

Instagram ajoute des fonctionnalités pour lutter contre le cyber-harcèlement

Le réseau social a ajouté mardi 9 octobre des fonctionnalités pour combattre le harcèlement. Il est question d'utiliser une intelligence artificielle qui permettrait de scanner les photos afin d'identifier et détecter les contenus problématiques. Le contenu pourra être signalé automatiquement et sera ensuite examiné par une équipe chargée des opérations du réseau social.

Un filtre permet également aux utilisateurs d'Instagram de repérer et de cacher des commentaires considérés comme du harcèlement, sur les vidéos diffusées en direct.