Veille juridique de septembre 2019 de Claire Sambuc

Actualité législative publié le **05/11/2019**, vu **1686 fois**, Auteur : Claire Sambuc

Claire Sambuc décrypte pour vous toute l'actualité juridique liée au droit des nouvelles technologies.

DEREFERENCEMENT

Le droit au déréférencement n'a pas une portée mondiale

CJUE 24 Septembre 2019

Portée du déréférencement

La CJUE a tranché la question qui planait depuis la consécration du droit au déréférencement qui permet depuis 2014 à chaque internaute européen de faire supprimer sous conditions certains résultats le concernant des moteurs de recherche lorsqu'on y saisit ses noms et prénoms : ce droit ne s'applique qu'à l'intérieur des frontières de l'Union européenne, il ne s'applique pas à une échelle mondiale.

Bien que déréférencé sur une extension européenne, la CNIL avait constaté qu'il suffisait de se rendre sur une autre extension type google.com pour retrouver le contenu retiré. La CNIL avait ordonné au moteur de recherche de procéder au déréférencement dans le monde entier, internet n'ayant pas de frontières.

Face au refus de Google, la CNIL l'avait sanctionné. Le moteur de recherche avait porté l'affaire devant le Conseil d'Etat. La CJUE a estimé ce 24 septembre que cette solution souhaitée par la CNIL n'était pas satisfaisante car elle conduirait à l'application mondiale d'un droit européen. *« L'équilibre entre la protection de la vie privée et la liberté d'expression des internautes est susceptible de varier à travers le monde »*, remarque ainsi la Cour.

La CJUE précise que les moteurs de recherches doivent prendre des mesures suffisamment efficaces pour que le déréférencement soit bien effectif dans toute l'UE.

La CJUE a également laissé la possibilité de procéder à un déréférencement mondial, dans certains cas. En précisant que les autorités nationales de protection des données (comme la CNIL en France) devraient alors déterminer, le cas échéant et au cas par cas, si Google devait supprimer de ses résultats de recherche mondiaux certaines pages.

Données sensibles

Les juges ont également précisé comment les moteurs de recherches devaient appréhender une demande de déréférencement visant des données « sensibles ».

Les données sensibles peuvent être par exemple l'appartenance sexuelle, l'origine ethnique, l'orientation politique, …

Pour Google, ces données bien que sensibles étaient d'intérêt public et ne devaient pas être déréférencées. Il s'agissait par exemple d'un homme condamné pour pédophilie désireux de ne plus voir sa condamnation apparaitre, ou une ancienne responsable politique locale voulant supprimer un photomontage suggérant une relation sexuelle.

Saisie par les particuliers suite au refus de Google, la CNIL s'était alignée sur la position de Google.

L'affaire a été portée devant le Conseil d'Etat. La CJUE a confirmé que les moteurs de recherche ne devaient pas vérifier a priori qu'une donnée sensible était présente dans les pages indexées.

La Cour a aussi jugé que, dans la plupart des cas, le moteur de recherche devait obéir à la demande de déréférencement des pages contenant ce type de données, en raison de la menace qu'elles font peser sur la vie privée des internautes. La Cour indique que dans certains cas, lorsque l'intérêt des internautes à accéder à ces informations est plus important que la vie privée des demandeurs, le moteur pouvait refuser le déréférencement.

Dans le cas des données obsolètes liées à une procédure judiciaire (par exemple, l'annonce d'une mise en examen alors que l'internaute a été relaxé quelques mois plus tard), la CJUE a indiqué que le moteur de recherche devait prendre en compte la gravité des faits, le rôle public de la personne concernée ou encore l'intérêt du public à connaître cette information pour décider si la page Web devait disparaître des résultats de recherche.

VIE PRIVEE

Le site du Figaro Madame condamné pour atteinte à la vie privée

TGI Nanterre, 12 septembre 2019

Le site Figaro Madame avait diffusé un article portant sur des "suppositions illicites sur la relation sentimentale" prêtée à un journaliste. L'article renvoyait vers un site du dailymail.co.uk donnant accès à une dizaine de clichés le représentant avec sa prétendue petite amie.

Les juges sanctionnent cette pratique de la presse people en ligne consistant à rediriger les internautes vers un contenu attentatoire à la vie privée des personnes.

« La société défenderesse participe à la diffusion de ces clichés manifestement fixés à la dérobée et sans le consentement des intéressés et violant de ce fait le droit au respect de la vie privée du requérant, quand bien même ces images auraient été fixées dans un lieu ne marquant pas les bornes de la vie privée mais n'emportant pour autant nulle autorisation tacite de captation. ».

Le tribunal a par ailleurs relevé que le journaliste, bien que présent sur les réseaux sociaux, n'y évoque pas sa vie sentimentale.

Les juges minimisent cependant le préjudice subi du fait de l'absence de caractère exclusif, de l'information et des clichés, déjà diffusés sept jours plus tôt sur le site du Daily Mail. De plus, Madame.lefigaro.fr avait retiré l'article sept jours après la mise en demeure.

Condamnation du site Voici.fr pour avoir relayé une information reprise d'un site américain

Le site Voici.fr a été condamné pour avoir révélé sa rupture avec son mari. Le fait que l'information ait été préalablement diffusée sur un site américain n'empêche pas Voici.fr d'être sanctionné pour atteinte à la vie privée.

DROIT DES CONTRATS

Condamnation d'Amazon à 4 millions d'euros d'amende

Tribunal de commerce de Paris, 2 septembre 2019

Amazon France Services et Amazon Services Europe ont été condamnées par le tribunal de commerce de Paris à 4 millions d'euros d'amende.

Suite à une enquête de la DGCCRF sur les contrats d'ASE et AFS avec les vendeurs tiers, l'existence d'un déséquilibre significatif a été jugée.

Le tribunal constate l'absence de négociation dans un contexte de déséquilibre de puissance entre les acteurs, Amazon étant le premier site marchand de produits finis en France.

Le tribunal a considéré que la clause « modifications » du contrat permettant à Amazon d'amender toutes les dispositions contractuelles à tout moment à son entière discrétion, sans aucun préavis, est de nature à créer un déséquilibre manifeste au détriment des vendeurs. Idem pour la clause relative à la suspension ou la résiliation du contrat, en l'absence de préavis, discrétionnaire et imprécise elle est constitutive d'un déséquilibre significatif.

Condamnation pour rupture brutale des relations commerciales

Tribunal de commerce de Lille, 24 septembre 2019

La société commercialisant les produits Paul Marius avait confié la distribution au site mesbagages.com, référence en ligne dans le domaine de la maroquinerie.

Le maroquinier a interrompu brutalement et sans préavis les relations commerciales arguant que le site pratiquait des offres promotionnelles illicites. De plus, en l'absence de contrat, le maroquinier considérait que la marque avait été utilisée sans son autorisation.

Pour le tribunal, une relation commerciale existe entre les parties, bien qu'en l'absence de contrat, au regard du chiffre d'affaire réalisé.

Sur l'utilisation de la marque sans autorisation, le tribunal considère que les actes ne sont pas constitutifs de contrefaçon considérant que le maroquinier avait confié la distribution en ligne de ses produits au site internet et donc acquis la possibilité d'utiliser la marque sans l'autorisation du titulaire pour les besoins de la commercialisation.

Sur les offres promotionnelles, le tribunal constate « *que la pratique de remises est largement répandue dans le secteur de la vente en ligne d'articles de bagages/maroquinerie ».* De plus, la société était parfaitement informée des pratiques commerciales du site internet lequel ne trompait

pas le consommateur.

Les juges en concluent que le bagagiste a rompu brutalement la relation commerciale établie avec le distributeur en prenant en compte les deux ans pendant lesquels les produits ont été vendus et le chiffre d'affaires.

DONNEES PERSONNELLES

Google My Business : communication des données d'identification des auteurs des avis

Ordonnance de référé 11 juillet 2019

Une dentiste parisienne avait constaté l'existence d'une fiche GMB comportant ses coordonnées professionnelles et des avis qu'elle jugeait dénigrants ou insultants.

Elle a demandé à Google Ireland de supprimer sa fiche mais Google a refusé d'accéder favorablement à sa demande.

Cette affaire a été portée devant le tribunal. Le TGI de Paris a débouté la dentiste de sa demande de suppression de fiche GMB, fondée sur son droit d'opposition, car elle ne justifie pas de motif légitime au sens de l'article 21 du RGPD.

Pour le tribunal, les coordonnées professionnelles ne relèvent pas de la sphère privée. Les finalités du traitement sont légitimes, à savoir l'accès rapide pour le public à des informatiques pratiques sur les professionnels de santé. A l'instar du juge de Metz, le tribunal parisien a par ailleurs considéré que *« la suppression pure et simple de la fiche de la demanderesse contreviendrait au principe de la liberté d'expression, alors même qu'il est loisible à celle-ci d'agir spécifiquement contre les personnes à l'origine d'avis qu'elle estimerait contraires à ses droits ».*

Le TGI a cependant ordonné à Google de communiquer à la dentiste les éléments d'identification des internautes ayant commenté sa fiche de nature à lui avoir causé un préjudice afin que la demanderesse puisse engager une procédure d'indemnisation.

La professionnelle de santé avait également demandé la suppression d'avis négatifs sur sa fiche. Le tribunal a jugé qu'un seul était injurieux traitant la dentiste de « vraie perverse ». Celle-ci a obtenu 200 € d'indemnisation provisionnelle en raison de la diligence tardive de Google pour supprimer ce contenu injurieux notifié.

Une société d'intermédiation en assurance sanctionnée par la CNIL

Délibération de la CNIL 18 juillet 2019

Une sanction de 180 000 euros a été prononcée à l'encontre d'une société d'intermédiation en assurance pour atteinte à la sécurité des données de ses clients et absence de mesures techniques et organisationnelles appropriées afin de garantir la sécurité des données personnelles traitées conformément à l'article 32 du RGPD.

La CNIL a constaté un défaut de sécurité et une violation des données relatives aux clients de la société telles que des copies de permis de conduire, des RIB ou des données relatives à des infractions commises par les clients.

Violation du Children's Online Privacy Protection Act

Federal Trade Commission 4 septembre 2019 : Condamnation d'une plateforme de vidéos en ligne

La FTC a condamné la plateforme à une amende record de 170 millions de dollars pour avoir enfreint les dispositions de de la loi COPPA (Children's Online Privacy Protection Act, notamment en collectant les données personnelles des enfants dans un but de ciblage publicitaire, à l'insu des parents. Les enfants auraient été également exposés à des vidéos inappropriées.

ACTUALITES

Google VS droit voisin des éditeurs de presse

Alors que la directive européenne sur le droit voisin des éditeurs de presse a été adoptée en juillet, permettant à la presse à négocier avec Google, Facebook ou Twitter une rémunération pour l'utilisation d'extraits d'articles ou vidéos, Google a annoncé qu'il ne montrera plus par défaut les extraits d'article. En somme, Google refuse de payer les éditeurs de presse.

Google a annoncé le 25 septembre qu'il allait changer les règles d'affichage de ses services et ne montreraient plus les extraits d'articles ou photos miniatures mais seulement les titres et les liens. Cette mesure sera effective lorsque la loi entrera en vigueur.

« *Nous n'avons pas l'intention de payer une licence pour la reprise d'un extrait d'un contenu* » a annoncé le vice-président chargé des médias.

Les réactions ne se sont pas fait attendre. Du côté de l'Association européenne des éditeurs de presse (ENPA) : *« Le diktat de Google est inacceptable »,* écrit-elle, ajoutant : *« Google n'est pas au-dessus des lois ».*

Le ministre de la culture a également fait part de sa déception pour lequel « *l'unité et la détermination* » permettront de s'imposer face à cet acteur.

Découverte d'un virus capable de surveiller les iPhone

Des chercheurs en sécurité informatique de Google ont relevé l'existence jeudi 29 aout d'un logiciel malveillant permettant l'accès aux messages, photos, localisation de mobiles et tablettes Apple. Il suffisait de visiter, depuis son appareil iPhone, un site infecté pour que le virus prenne place, même sur les derniers modèles d'iPhone.

Le virus aurait été actif pendant plus de deux ans et s'intéressait aux archives de messages aux travers des applications comme Gmail, Whatsapp, iMessage mais aussi à la géolocalisation, aux photos stockées ainsi qu'au répertoire téléphonique.

Le nombre de victimes n'est pas précisé. Google a choisi de ne pas reproduire le nom des sites concernés. Concernant la cible, selon le chercheur « *Il suffit peut-être d'être né dans une certaine région ou de faire partie d'un certain groupe ethnique »*.

Au regard de l'envergure des moyens employés et des failles concernées, il semblerait qu'un Etat soit impliqué. L'entité qui a conçu ce virus dispose de moyens importants.

Facebook : des centaines de millions de numéros de téléphone d'utilisateurs librement accessibles

Des fichiers stockés sans protection sur un serveur n'appartenant pas à Facebook contenant des numéros d'utilisateurs étaient librement accessibles.

Ces bases de données contenant des centaines de millions de numéros de téléphone appartenant à des utilisateurs Facebook ont été découvertes par un chercheur en sécurité informatique. Sans protection, les fichiers étaient accessibles et lisibles par n'importe qui trouvant l'emplacement sur internet.

D'autres données telles que le nom d'utilisateur, genre ou pays étaient parfois disponibles.

Facebook assure n'avoir *« trouvé aucune preuve que des comptes Facebook aient été compromis »* et que ces données sont anciennes, récoltées à l'époque où il était possible de rechercher un numéro de téléphone dans le moteur de recherche Facebook et découvrir à quel compte il était relié, fonctionnalité désactivée l'an dernier.

Désormais hors ligne, on ignore toutefois si ces données ont été exploitées, vendues, dupliquées et quelles étaient les intentions de cette mise en ligne.

Nouvelles lignes directrices de la CNIL sur les cookies et traceurs

Délibération du 4 juillet 2019

La Cnil a adopté par une délibération du 4 juillet 2019 de nouvelles lignes directrices relatives aux cookies et autres traceurs.

La Cnil considère désormais que le consentement au dépôt de cookies "*ne peut être valable que si la personne concernée est en mesure d'exercer valablement son choix et ne subit pas d'inconvénients majeurs en cas d'absence ou de retrait du consentement*" et rappelle ainsi que la pratique consistant à bloquer l'accès à un site web pour qui ne consent pas à être suivi n'est pas conforme au RGPD.

La simple poursuite de la navigation sur un site ne peut plus être regardée comme une expression valide du consentement au dépôt de *cookies*. D'autre part, les opérateurs qui exploitent des traceurs doivent être en mesure de prouver qu'ils ont bien recueilli le consentement.

Faux avis sur TripAdvisor : ménage sur la plateforme

1.4 million de faux commentaires auraient été recensés et retirés sur la plateforme, destinés à promouvoir ou nuire à un établissement. En conséquence, 35 000 lieux ont été déclassés.

TripAdvisor explique que 4.7% des avis déposés en 2018 ont été rejetés automatiquement par un logiciel de pointe. Une équipe de modération est également mobilisée pour vérifier manuellement les commentaires.

Expérience de reconnaissance faciale menée à Nimes : doutes de la CNIL

A Nice, une étude a été menée sur quelques milliers de niçois : leurs visages captés par la vidéosurveillance ont été analysés en temps réel par un logiciel de reconnaissance faciale.

La CNIL a jugé le rapport de la mairie trop imprécis et manquant d'éléments techniques en particulier sur les conséquences d'un possible biais du logiciel et demande plus de précisions. Cette demande est en cours d'instruction par les services de la mairie.

La mairie estime que le cadre juridique est insatisfaisant. La CNIL réclame que le législateur se penche sur les nouvelles utilisations sécuritaires de la vidéosurveillance pour compléter le cadre légal existant.

Instagram : vulnérabilité relative à la confidentialité des comptes

Les comptes privés d'Instagram ne seraient pas si privés. La possibilité d'accéder au contenu de comptes privés est possible à la seule condition de se procurer leur URL.

Par une simple lecture du code source d'une publication privée à l'aide d'un navigateur web, il est possible de récupérer l'adresse web d'une publication et d'en partager l'URL.

A l'aide de l'URL, même un tiers non inscrit sur Instagram peut accéder au contenu.

La vulnérabilité toucherait aussi les contenus privés partagés sur Facebook.

« Cour suprême » de Facebook mise en place début 2020

Comme évoqué dans notre veille de juillet, ce projet avance et prend forme pour une mise en place début 2020. La structure sera composée d'une quarantaine de membres et sa mission sera de trancher les litiges liés aux retraits de publications sur le réseau social.

Les premiers membres seront nommés fin 2019 et les premières décisions seront rendues au premier semestre 2020 selon l'entreprise. A terme, la structure sera composée d'une quarantaine de membres *« par exemple des modérateurs de groupes de discussion Facebook, d'anciens juges ou avocats, ou d'anciens journalistes »,* a précisé Brent Harris, le directeur de la gouvernance de l'entreprise.

Le réseau social souhaite que ce comité soit « indépendant ». Ces membres seront payés par un trust crée pour l'occasion. Les membres auront un mandat de trois ans renouvelables deux fois et ne seront pas révocables par Facebook mais par le trust s'ils enfreignent le code de conduite.

Tous les pays ne seront pas représentés bien que le réseau social annonce vouloir que ce comité reflète la diversité. Les décisions seront prises en application de la charte de modération du réseau et non des lois des Etats.