SOMMAIRE

PARIS - NANTES
MONTPELLIER - LYON
FORT-DE-FRANCE

Bureaux intégrés

BORDEAUX - CAEN
CLERMONT-FERRAND
GRENOBLE - LE HAVRE
MARSEILLE - ROUEN
SAINT-ETIENNE
SAINT-DENIS (La Réunion)
STRASBOURG - TOULOUSE

Réseau SIMON Avocats

ALGÉRIE - ARGENTINE
ARMÉNIE - AZERBAÏDJAN
BAHAMAS - BAHREÏN
BELGIQUE - BOLIVIE - BRÉSIL
BULGARIE - CAMBODGE
CAMEROUN - CHILI - CHINE
CHYPRE - COLOMBIE
COREE DU SUD - COSTA RICA
CÔTE D'IVOIRE - ÉGYPTE
EL SALVADOR
ÉMIRATS ARABES UNIS
ESTONIE - ÉTATS-UNIS
GUATEMALA - HONDURAS
HONGRIE - ÎLE MAURICE
ÎLES VIERGES BRITANNIQUES
INDE - INDONÉSIE - IRAN
ITALIE - LUXEMBOURG
MAROC - NICARAGUA
OMAN - PARAGUAY - PÉROU
PORTUGAL - RD CONGO
RÉPUBLIQUE DOMINICAINE
SENEGAL - SINGAPOUR
THAÏLANDE - TUNISIE
URUGUAY - VENEZUELA

Conventions transnationales

www.simonassocies.com
www.lettredunumerique.com

DATA / DONNÉES PERSONNELLES

Publicités ciblées & performance des campagnes marketing : le SDK dans la ligne de mire de la CNIL !
Décision de la CNIL n°MED 2018-042 du 30 octobre 2018 mettant en demeure la société VECTAURY

Ce qu'il faut retenir :

La CNIL a saisi la société Vectaury, start-up spécialisée dans le ciblage publicitaire, lui reprochant d'exploiter des données d'utilisateurs de smartphones sans leur accord.

Pour approfondir :

Cette année la CNIL est particulièrement vigilante en matière de traitements de données réalisés via des logiciels dénommés SDK. Ces outils sont intégrés dans le code d'applications mobiles permettant de collecter les données des utilisateurs des smartphones dont notamment l'identifiant publicitaire des smartphones et les données de géolocalisation des personnes en vue d'envoyer des publicités ciblées.

Ces données sont ensuite croisées avec des points d'intérêts (généralement des points de vente physiques), ce qui permet d'évaluer la performance d'une campagne marketing.

Depuis cet été, la CNIL a procédé à plusieurs contrôles sur place de plusieurs entités qui ont recours à ces outils, qu'il s'agisse d'éditeurs d'applications mobiles ou de prestataires offrant des services d'affichage de publicités ciblées et d'évaluation de la performance des campagnes marketing aux éditeurs d'applications.

Après le contrôle des sociétés TEEMO et FIDZUP ayant abouti à une mise en demeure de chacune d'elle en juillet dernier, puis de la société SINGLESPOT mise en demeure le 8 octobre 2018, la société Vectaury a, à son tour, fait l'objet d'un contrôle de l'autorité de contrôle et d'une mise en demeure le 30 octobre dernier.

Retour sur les manquements constatés.

- **Les faits**

Vectaury est une société spécialisée dans la programmation informatique et notamment l'édition et la vente d'outils informatiques.

Elle affiche pour le compte de ses clients annonceurs des publicités sur les smartphones.

Elle a également pour activité de mesurer les visites des porteurs de smartphone dans les points de vente de ses clients.

A partir de données de géolocalisation, Vectaury détermine le profil de chaque utilisateur, déterminant ainsi les habitudes de leurs déplacements en vue de leur proposer de la publicité ciblée.

Le 23 mai 2017, la société a effectué auprès de la CNIL un engagement de conformité à la norme simplifiée n° 48 portant sur les traitements relatifs à la gestion de clients et de prospects.

En application d'une décision du 30 mars 2018 de la Présidente de la Commission, une délégation de la CNIL a procédé à des missions de contrôle sur place auprès de la société Vectaury.

La lettre de mission du contrôle prévoyait notamment la vérification de la conformité à la loi Informatique et Libertés de l'ensemble des traitements de données à caractère personnel mis en œuvre par la société.

Afin de réaliser ses activités de profilage, la société a indiqué avoir développé un logiciel SDK, intégré par ses partenaires dans leurs applications mobiles et qui permet de collecter les données de géolocalisation ainsi que l'identifiant publicitaire mobile, le nom et la version de l'application mobile et le système d'exploitation utilisé (ANDROID ou IOS).

Les données collectées grâce à ce logiciel SDK sont ensuite croisées avec des points d'intérêts « POIs » déterminés avec ses clients annonceurs et qui correspondent à des coordonnées géographiques de lieux permettant de révéler un profil de consommateur, tels que des points de vente physiques.

Enfin et dans un troisième temps, Vectaury réalise des campagnes marketing à travers l'achat d'espaces publicitaires sur les plateformes de ventes aux enchères de publicités en temps réel. Ce système permet à des applications mobiles de trouver un annonceur pour afficher des publicités sur les espaces publicitaires qu'elle comprend.

Afin d'estimer la valeur de l'espace publicitaire pour ses clients et placer une enchère, les diverses données reçues de l'application où s'affichera la publicité sont transmise à Vectaury et conservée par elle.

En outre, dans le but de mesurer l'impact et la performance des campagnes marketing (c'est-à-dire la société vérifier si et combien d'utilisateurs ciblé par les publicités se sont rendus dans un point de vente physique) Vectaury analyse et recoupe les données collectées *via* le SDK et le système de demande d'enchère en temps réel

Lors de ses opérations de contrôle, la délégation de la CNIL a constaté, sur plusieurs applications mobiles intégrant le SDK de la société Vectaury que, lorsque l'utilisateur d'un smartphone valide l'autorisation d'accès à ses données de géolocalisation pour le fonctionnement de l'application, ses données sont également transmises à la société Vectaury sans qu'il en soit spécifiquement informé et sans que son consentement ne soit recueilli pour cette transmission.

Ces données de géolocalisation ainsi que celles du système d'enchère sont ensuite conservées par la société Vectaury pendant douze mois à compter de la date de leur collecte.

Pour rendre sa décision, la CNIL s'est attachée dans un premier temps à qualifier le rôle de la société Vectaury, puis dans un second temps à vérifier la conformité des traitements mis en œuvre ou constater les manquements.

- **Sur la qualification de la société Vectaury**

La CNIL retient que dans la mesure où la société Vectaury détermine dans une large mesure les finalités et les moyens des traitements mis en œuvre dans le cadre de l'utilisation du SDK et des dispositifs d'enchères de publicités en temps réel et que la société traite pour son propre compte les données à caractère personnel collectées pour vendre des services d'analyse ou de profilage auprès de ses clients, elle doit être qualifiée de Responsable de traitement.

- **Sur les manquements constatés**

Le traitement des données de géolocalisation aux fins de marketing ciblé est fondé sur le consentement des personnes concernées.

La société Vectaury a indiqué à la Commission qu'elle propose aux éditeurs d'application une interface d'information visant à recueillir le consentement des utilisateurs.

La Société a également développé, en partenariat avec une association de professionnels du marché de la publicité sur internet, un outil destiné à uniformiser les modalités de recueil du consentement *via* les SDK dénommé *Consent Management Provider* (CMP).

Lorsque cet outil est implémenté dans une application, une première information au lancement de l'application est délivrée. Cette information s'accompagne d'un lien hypertexte renvoyant vers les politiques de confidentialité de l'application.

L'utilisateur a ensuite le choix entre accepter, refuser ou affiner ses préférences. Par défaut, si l'utilisateur choisi d'affiner ses préférences, la collecte des données est réputée acceptée par l'utilisateur. Pour refuser, l'utilisateur doit décocher l'ensemble des cases se rapportant aux différentes finalités de la collecte.

La CNIL a considéré que le mécanisme en place ne permet pas de répondre aux obligations en matière de consentement et notamment celles découlant du Règlement Général sur la Protection des Données Personnelles (RGPD).

En effet, il est apparu que ce consentement n'était pas informé dès lors que le texte de présentation adressé à l'utilisateur à la première ouverture de l'application ne présente pas la clarté requise en ce qu'il ne permet pas aux personnes concernées de comprendre précisément à quoi elles consentent. La CNIL relève que ce texte manque également de transparence et qu'il est rédigé dans des termes si flous qu'il peut induire en erreur les utilisateurs quant à la non-gratuité du service en cas de refus.

De plus, la CNIL a constaté que le consentement n'était pas spécifique puisque les personnes concernées sont amenées à valider l'autorisation de collecter leurs données de géolocalisation uniquement pour l'utilisation de l'application mobile téléchargée. De plus, lorsque dans un second temps, grâce à l'outil CMP la personne peut accepter ou refuser la collecte de ses données, ces actions ne sont pas différenciées selon que l'autorisation concerne l'affichage de publicités ciblées, ou l'élaboration d'un profil commercial à visée marketing.

Enfin, le fait que l'ensemble des finalités de collecte soient pré-acceptées par défaut lorsque l'utilisateur souhaite affiner ses préférences ne saurait aboutir à l'expression d'un consentement valide de la part de l'utilisateur dès lors que le RGPD impose que ce consentement doit être matérialisé par un acte positif.

En conséquence, la CNIL a mise en demeure la société Vectaury, sous un délai de trois (3) mois à compter de la notification de sa décision de :

- Rétablir la base légale de ses traitements et recueillir, de manière effective, le consentement préalable, dans des conditions conformes aux dispositions du RGPD, des utilisateurs des applications éditées par les partenaires de la société VECTAURY comme celles des utilisateurs des applications dont proviennent des offres d'enchère en temps réel, au traitement de leurs données par cette dernière ;
- Procéder à la purge des données obtenues sans consentement informé, spécifique et activement manifesté ;
- Justifier auprès de la CNIL que l'ensemble des demandes précitées a bien été respecté, et ce dans le délai imparti.

La CNIL indique être disposé à clore cette mise en demeure si la société Vectaury s'y conforme dans les délais impartis. Dans la négative, un rapporteur sera désigné par la CNIL en vue de prononcer une sanction à son encontre.

A rapprocher : Applications mobiles : mises en demeure pour absence de consentement au traitement de données de géolocalisation à des fins de ciblage publicitaire (CNIL, 19 juillet 2018)

La CNIL publie la liste des traitements de données personnelles soumis à analyse d'impact

Délibération n°2018-326 du 11 octobre 2018 portant adoption de lignes directrices sur les analyses d'impact relatives à la protection des données (AIPD) prévues par le règlement général sur la protection des données (RGPD)

Ce qu'il faut retenir :

La CNIL a fait la liste des traitements de données personnelles qui seront soumis à une analyse d'impact préalable en respect des dispositions du RGPD.

Pour approfondir :

Le Règlement Général sur la Protection des Données personnelles (RGPD) a introduit la notion d'analyse d'impact relative à la protection des données.

Cette analyse d'impact est un processus dont l'objet est de décrire le traitement, d'en évaluer la nécessité ainsi que la proportionnalité et d'aider le responsable du traitement à gérer les risques pour les droits et libertés des personnes concernées, en les évaluant et en déterminant les mesures de sécurité adéquates.

L'article 35 du RGPD prévoit l'obligation de réaliser une telle analyse d'impact lorsqu'un de traitement, en particulier par le recours à de nouvelles technologies, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques.

Depuis l'adoption du RGPD, de nombreux outils ont été publiés afin d'accompagner les responsables de traitement et les aider à faire face aux analyses d'impact.

Parmi ces outils, la CNIL a publié :
- un logiciel de réalisation d'analyse d'impact (PIA sous licence Open source) ;
- un guide présentant la méthodologie de l'analyse d'impact ;
- un modèle d'analyse.

De son côté, le G29 (groupe des autorités de contrôle européennes) a adopté des lignes directrices d'une grande utilité notamment parce qu'au travers d'un certain nombre de critères, ces lignes aident à identifier si un traitement nécessite ou non la réalisation d'une analyse d'impact.

En effet, pour donner une vision plus concrète des opérations de traitement qui nécessitent une analyse d'impact, le G29 a dégagé neuf critères. Selon la méthode présentée, si un traitement répond à au moins deux de ces critères, alors une analyse d'impact s'avère nécessaire.

En synthèse, les neuf critères ont été présentés comme suit :
- évaluation/*scoring* (y compris le profilage) ;
- décision automatique avec effet légal ou similaire ;
- surveillance systématique ;
- collecte de données sensibles ;
- collecte de données personnelles à large échelle ;
- croisement de données ;
- personnes vulnérables (patients, personnes âgées, enfants, *etc.*) ;
- usage innovant (utilisation d'une nouvelle technologie) ;
- exclusion du bénéfice d'un droit/contrat

Conformément à l'article 35-4 du RGPD, lequel prévoit qu'une autorité de contrôle doit établir et publier une liste des types d'opérations de traitement pour lesquelles une analyse d'impact est requise, La CNIL a publié le 6 novembre dernier, en tenant compte de ces neuf critères, sa liste des traitements qui par définition sont soumis à analyse d'impact.

A la lecture de cette liste, sont concernés les traitements des données de santé, de ressources humaines lorsqu'une surveillance individualisé des salariés est réalisée, de géolocalisation lorsque celle-ci est réalisé à grande échelle, des assurances et enfin des données recueillies dans le cadre de la gestion des logements sociaux.

Liste des traitements soumis à analyse d'impact :

- Traitements de données de santé mis en œuvre par les établissements de santé ou les établissements médicosociaux pour la prise en charge des personnes ;
- Traitements portant sur des données génétiques de personnes dites « vulnérables » (patients, employés, enfants, etc.) ;
- Traitements établissant des profils de personnes physiques à des fins de gestion des ressources humaines ;
- Traitements ayant pour finalité de surveiller de manière constante l'activité des employés concernés ;
- Traitements ayant pour finalité la gestion des alertes et des signalements en matière sociale et sanitaire ;
- Traitements ayant pour finalité la gestion des alertes et des signalements en matière professionnelle ;
- Traitements des données de santé nécessaires à la constitution d'un entrepôt de données ou d'un registre ;
- Traitements mutualisés de manquements contractuels constatés, susceptibles d'aboutir à une décision d'exclusion ou de suspension du bénéfice d'un contrat ;
- Traitements de profilage faisant appel à des données provenant de sources externes ;
- Traitements de données biométriques aux fins de reconnaissance des personnes parmi lesquelles figurent des personnes dites « vulnérables » (élèves, personnes âgées, patients, demandeurs d'asile, etc.) ;
- Traitements impliquant le profilage des personnes pouvant aboutir à leur exclusion du bénéfice d'un contrat ou à la suspension voire à la rupture de celui-ci ;
- Instruction des demandes et gestion des logements sociaux ;
- Traitements ayant pour finalité l'accompagnement social ou médico-social des personnes ;
- Traitements de données de localisation à large échelle.

A rapprocher : Délibération n°2018-326 du 11 octobre 2018

PROPRIÉTÉ INTELLECTUELLE

Action en contrefaçon de droit d'auteur et preuve de la qualité d'auteur

Ord. réf., Président TGI Paris, 24 septembre 2018, n°18/57276

Ce qu'il faut retenir :

La recevabilité de l'action en contrefaçon de droit d'auteur est subordonnée à la preuve de la qualité d'auteur et de la titularité des droits.

Pour approfondir :

Dans cette affaire, le juge des référés était saisi dans le cadre d'une action en contrefaçon de droit d'auteur pour de prétendues atteintes tant aux droits patrimoniaux qu'au droit moral. L'action était exercée par un célèbre artiste designer à l'encontre de la société avec laquelle il avait collaboré pendant plusieurs années une fois que celle-ci eut repris les actifs de la société qu'il avait fondée.

L'action en contrefaçon, en matière de droit d'auteur, suppose d'établir en premier lieu sa qualité pour agir comme pour toute action en justice. En matière de contrefaçon, cela signifie que la personne qui agit doit être titulaire des droits patrimoniaux si elle fait état d'une atteinte à ceux-ci, et établisse sa qualité d'auteur si elle fait état d'une atteinte au droit moral dès lors que ce droit appartient au seul auteur. Il s'agit là d'une condition de recevabilité de l'action.

Ajoutons que, dans le cadre d'une action en référé, cela doit ressortir avec l'évidence attendue dans ce type de procédure. Or, dans cette affaire, les pièces versées aux débats ne permettaient pas au demandeur de justifier, précisément de sa qualité d'auteur. En outre, il ne justifiait pas davantage de la date de création des œuvres revendiquées. Or, en l'espèce, ce point était d'autant plus essentiel que les parties avaient par le passé été en relations contractuelles et que le contrat organisait la cession des droits de propriété intellectuelle. Egalement, préalablement à la conclusion de ce contrat, elle avait repris l'intégralité des actifs, en ce compris la propriété intellectuelle, de la société dans laquelle l'artiste avait exercé ses activités professionnelles et à laquelle il avait cédé ses droits.

Reprenant des principes constants, le Juge des référés relève dans son ordonnance :

> « *Il importe donc de déterminer la date et les circonstances de création de chacune des œuvres opposées … Ce à quoi ne peut se livrer avec l'évidence requise, le juge des référés (…) En l'état, à défaut de date certaine de création des œuvres opposées et eu égard aux incertitudes relatives au périmètre des droits cédés, la titularité de Jean-Charles de Castelbajac sur les dessins qu'il revendique n'est pas établie. L'action en contrefaçon de droit d'auteur, tant patrimonial que moral, est irrecevable* ».

A rapprocher : Article 122 du code de procédure civile ; Article L.111-1 du code de la propriété intellectuelle ; Article L.113-1 du code de la propriété intellectuelle

Pas de marque sur l' « iMessage »
CA Paris, 25 septembre 2018, RG n°17/19211

Ce qu'il faut retenir :

L'obtention d'un droit à titre de marque implique que le signe présente un caractère distinctif, qualité refusée à la dénomination « iMessage ».

Pour approfondir :

Le caractère **distinctif** d'un signe est une condition de sa protection à titre de marque, le signe doit être apte à remplir la fonction de la marque d'identifier l'origine des produits et services qu'il désigne. L'article L.711-2 du code de la propriété intellectuelle prévoit que sont dépourvus de caractère distinctif les signes qui sont exclusivement la désignation nécessaire, générique ou usuelle du produit ou du service, ceux pouvant servir à désigner une caractéristique du produit ou du service, et notamment l'espèce, la qualité, la quantité, la destination, la valeur, la provenance géographique, l'époque de la production du bien ou de la prestation de service, le texte réservant la possibilité d'acquérir ce caractère par l'usage.

C'est précisément en raison de l'absence de caractère distinctif que le signe « iMessage » pour désigner les produits et services suivants : « *logiciels (programmes enregistrés) ; diffusion de matériel publicitaire (tracts, prospectus, imprimés, échantillons) ; Télécommunications ; informations en matière de télécommunications ; communications par terminaux d'ordinateurs ou par réseau de fibres optiques ; communications radiophoniques ou téléphoniques ; services de radiotéléphonie mobile ; services d'affichage électronique (télécommunications) ; agences de presse ou d'informations (nouvelles) ; émissions radiophoniques ; services de téléconférences ; services de messagerie électronique ; location de temps d'accès à des réseaux informatiques mondiaux ; Evaluations, estimations et recherches dans les domaines scientifique et technologiques rendues par des ingénieurs ; conception et développement de logiciels ; recherche et développement de nouveaux produits pour des tiers ; études de projets techniques ; élaboration (conception), installation, maintenance, mise à jour ou location de logiciels ; programmation pour ordinateur ; services scientifiques et technologiques ainsi que services de recherches et de conception y relatifs ; services d'analyses et de recherches industrielles* », a été refusé à l'enregistrement.

Le directeur général de l'INPI avait estimé que le signe « *phonétiquement identique à l'expression « e-message », sera compris par le consommateur pertinent comme désignant un message électronique, plus précisément l'objet ou la qualité des produits et services désignés et par là-même leur caractéristique, que le signe déposé ne permet pas de distinguer les produits et services du déposant de ceux d'une autre entreprise et ne remplit donc pas la fonction essentielle de la marque qui est de garantir l'identité d'origine du produit ou du service et qu'il est dépourvu de caractère distinctif* ».

En conséquence, la demande d'enregistrement de la marque avait été rejetée.

La société APPLE a donc formé un recours devant la Cour d'appel (compétente pour statuer sur les recours formés contre les décisions du directeur de l'INPI), à l'appui duquel elle formulait deux arguments :

- tout d'abord, elle avançait que le signe « iMessage » a un caractère intrinsèquement distinctif, faisant partie d'une famille de marques à préfixe « I » déposées et exploitées de manière intensive et jouissant d'une renommée pour les produits et services en cause et étant reconnu par le public pertinent comme faisant partie de cette famille de marques à préfixe « I » et comme identifiant des produits et des services multimédias informatiques et électroniques émanant d'APPLE ;
- ensuite, elle prétendait que le signe a acquis un caractère distinctif par l'usage, en raison de la publicité qui lui a été donnée juste avant et juste après le dépôt, ainsi que de l'intensité de l'usage qui en a été fait très rapidement après ce dépôt.

Par cet arrêt, la Cour approuve l'INPI qui a estimé que le signe sera ainsi aisément compris par le consommateur pertinent, soit le consommateur moyen de la catégorie des produits en cause, normalement informé et raisonnablement attentif et avisé, comme désignant un message transmis par voie électronique, c'est à dire un message envoyé au moyen de réseaux informatiques et notamment d'Internet, et que, de ce fait, le signe ne permet pas de distinguer les produits et les services proposés par la déposante en relation avec l'informatique et les télécommunications de ceux d'autres entreprises, au sens de l'article L.711-1 du code de la propriété intellectuelle. En outre, le signe « iMessage » peut servir à désigner une caractéristique d'une partie des produits et services visés à l'enregistrement, soit en décrivant l'objet des produits et services soit en définissant le moyen utilisé pour fournir les services et qu'ainsi il est dépourvu de caractère distinctif pour les produits et services en cause au sens de l'article L.711-2 du code de la propriété intellectuelle.

L'argument avancé par APPLE selon lequel le signe appartiendrait à une famille de marques à préfixe « I » ne va pas davantage prospérer. Elle faisait ainsi valoir que ces marques, déposées et exploitées de manière intensive et jouissant d'une renommée à l'échelle planétaire (iPad, iPod, iPhone, iMac, iBooks, iTunes...), de sorte que le public pertinent serait apte à reconnaître le signe « iMessage » comme faisant partie de cette famille de marques ajoutant que toute marque d'APPLE à préfixe « I » est automatiquement reconnaissable comme une indication de l'origine commerciale des produits et services et qu'une marque telle qu' « iMessage » remplit ainsi *ab initio* la fonction essentielle de la marque.

Or, selon la Cour, une partie des marques dont se prévaut la société requérante débutent par un « i » minuscule, différent du « I » majuscule entrant dans la composition du signe contesté, et que seuls quelques documents parmi ceux produits par la requérante font état de la lettre « i » (et non la lettre « I ») comme un signe de reconnaissance de la société APPLE. Aussi, il n'est pas démontré que la présence, au sein du signe « iMessage », de la lettre « I » en attaque amène le consommateur pertinent à identifier les produits et services couverts par la demande d'enregistrement comme provenant de la société APPLE.

La société APPLE tentait également de justifier de l'acquisition du caractère distinctif du signe litigieux par l'usage qui en avait été fait. Cela nécessite d'établir un usage continu, intense et de longue durée, à titre de marque - c'est à dire pour identifier les produits et services concernés comme provenant d'une entreprise déterminée auprès du public pertinent (en l'espèce le public français). Le caractère distinctif doit avoir été acquis par l'usage de la marque avant le dépôt de la demande d'enregistrement.

La Cour va considérer que les pièces produites à l'appui de cet argument ne démontrent pas l'usage du signe « iMessage » à titre de marque, ni la capacité d'une partie significative du public pertinent à identifier les produits et services concernés comme provenant de la société APPLE, et approuve la décision de refus d'enregistrement de la marque dès lors que l'usage du signe « iMessage » à la date du dépôt n'était pas suffisamment établi pour compenser l'absence de distinctivité intrinsèque de ce terme.

L'arrêt confirme ainsi que la dénomination « iMessage » ne pouvait constituer une marque valable.

A rapprocher : Article L.711-1 du code de la propriété intellectuelle ; Article L.711-2 du code de la propriété intellectuelle

SERVICES NUMÉRIQUES

Phishing : le seul fait de répondre à un email d'hameçonnage constituerait-il une négligence grave ?
Cass. com., 3 octobre 2018, n°17-21.395

Ce qu'il faut retenir :

La Cour de cassation, dans cet arrêt du 3 octobre 2018, a censuré les juges du fond qui s'étaient contentés de constater l'absence de négligence grave d'un client pour condamner la Banque à lui rembourser les sommes indument prélevées sur son compte. En effet, il ressortait des éléments versés aux débats, que le client lui-même avait reconnu, à l'occasion d'un courrier adressé à la Banque, avoir répondu à un email de type hameçonnage. La Cour a considéré qu'il appartenait aux juges du fond, compte tenu de l'existence d'un tel mail, de rechercher si dans les circonstances de l'espèce, le comportement du client de la Banque n'était pas constitutif d'une négligence grave.

Elle a jugé au visa des articles L.133-16 et L.133-19 du code monétaire et financier : « *Qu'en se déterminant ainsi, sans rechercher, au regard des circonstances de l'espèce, si le fait, qu'elle avait constaté, que M. X avait répondu à un courriel d'hameçonnage ne résultait pas d'un manquement de celui-ci, par négligence grave, à ses obligations mentionnées au premier des textes susvisés, la juridiction de proximité a privé sa décision de base légale.* »

Pour approfondir :

Selon **l'arrêt en date du 3 octobre 2018**, et poursuivant son œuvre de définition des contours de la négligence grave de la victime d'hameçonnage la privant de solliciter le remboursement des sommes indument prélevées sur son compte, la Cour de cassation a annulé le jugement de la juridiction de proximité de Béthune qui avait condamné l'établissement bancaire à rembourser le client victime.

Son préjudice matériel s'élevait alors à la somme de 1 568,56 € en principal, correspondant au montant des paiements frauduleux non autorisés.

La Cour de cassation a ainsi annulé la décision du juge du fond, au motif que ce dernier n'avait pas recherché si le comportement du client ne pouvait recevoir la qualification de négligence grave au sens de l'article L.133-19 du code monétaire financier qui dispose :

> *« IV. – Le payeur supporte toutes les pertes occasionnées par des opérations de paiement non autorisées si ces pertes résultent d'un agissement frauduleux de sa part ou s'il n'a pas satisfait intentionnellement ou par négligence grave aux obligations mentionnées aux articles **L.133-16** et **L.133-17** [du code monétaire et financier] ». »*

Les articles L.133-16 et L.133-17 précités imposent, en effet, à l'utilisateur de services de paiement une obligation de moyens, à notre sens désormais renforcée, d'assurer la sécurité des données liées à l'instrument de paiement mis à sa disposition.

Dans les faits, le titulaire d'un compte dans les livres d'une banque, constatant l'existence de prélèvements frauduleux sur son compte, a assigné l'établissement bancaire afin d'être remboursé des sommes indument débitées.

Le premier juge a écarté la négligence grave telle que soulevée par la banque afin d'échapper à son obligation de règlement, fondant son argumentation sur la combinaison des articles L.133-16 et L.133-19 du code monétaire et financier.

L'établissement bancaire, pour sa part, avait en effet, fait état de l'existence d'une correspondance émanant de la victime elle-même, à la faveur de laquelle elle reconnaissait expressément avoir répondu à un mail de phishing.

La juridiction de proximité a écarté tout manquement commis par le client, après avoir soulevé un moyen d'office (selon lequel « *le numéro de téléphone de M. X étant celui d'une ligne fixe, il ne pouvait recevoir le code de validation permettant de terminer l'achat sur internet* ») sans l'avoir au préalable soumis à la discussion contradictoire des parties.

La Cour de cassation a donc annulé le jugement, au motif qu'il appartenait à la juridiction de proximité de rechercher l'éventuel manquement, par négligence grave, de l'utilisateur de moyens de paiement compte tenu de l'existence établie d'un mail de phishing.

La Cour de cassation continue de façonner une jurisprudence sévère envers les clients des banques, en matière de phishing, et impose désormais aux juges du fond de procéder systématiquement à un examen minutieux des faits, face à une escroquerie menée sur internet par l'envoi de mails frauduleux, permettant de caractériser ou non la négligence grave de l'internaute.

Rappelons, par ailleurs, qu'il appartient à la banque de rapporter par tous moyens la preuve de la négligence fautive de l'utilisateur, qui pourrait malheureusement être constituée par le simple fait établi de répondre à un mail de type phishing.

Encore et à nouveau, nous ne pouvons qu'inviter les titulaires de compte en banque à redoubler de vigilance.

A rapprocher : Art. L.133-16 du code monétaire et financier ; Art. L.133-19 du code monétaire et financier ; Cass. com., 18 janv. 2017, n°15-18.466 ; Cass. com., 25 oct. 2017, n°16-11.644 ; Cass. com., 28 mars 2018, n°16-20.018

La signature électronique simple est suffisante pour apporter la preuve de la validité d'un contrat
TI Nîmes, 18 septembre 2018, CA Consumer Finance SA / Mme X

Ce qu'il faut retenir :

Une signature électronique simple est 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).

Pour approfondir :

La SA CA Consumer Finance a octroyé un prêt bancaire à l'une de ses clientes.

Cette dernière a cessé de rembourser ses échéances. La SA CA Consumer a alors saisi le Tribunal d'instance de Nîmes d'une demande en paiement contre cette cliente.

Au soutien de ses demandes, la SA CA Consumer a produit un contrat de prêt conclu par voie électronique avec la cliente.

Une réouverture des débats a été prononcée afin que l'établissement de crédit puisse présenter ses observations relatives à la validité du contrat dont il se prévalait.

La société a alors rapporté la preuve de la validité de son contrat en produisant des éléments permettant d'authentifier la signature électronique du contrat par la cliente.

Ont été produits, d'une part, une synthèse du fichier de preuve émanant de son prestataire, la société Open Trust et, d'autre part, une attestation de la fiabilité des pratiques de la société Open Trust, au sens du décret du 30 mars 2001 sur la signature électronique.

Il résulte de la synthèse du fichier de preuve un numéro de transaction identique au numéro d'indexation figurant sur le contrat de crédit. La société Open Trust, en sa qualité de Prestataire de Service de Certification Electronique, y atteste de la signature électronique le 13/04/2016 à 15:15:49 du contrat de crédit par Madame X dont elle précise l'adresse mail.

Le juge a rappelé le droit positif en matière de signature électronique et notamment du fait 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).

Cet article 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, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie dans les conditions fixées par décret en Conseil d'Etat*.

Dès lors, et compte tenu des justificatifs rapportés par l'établissement de crédit, le tribunal a reconnu et constaté la validité du contrat.

A rapprocher : Article 1367 du code civil

E-COMMERCE

Vente en ligne : validation de possibles restrictions à la vente sur marketplaces
ADLC, 24 octobre 2018, décision n°18-D-23

Ce qu'il faut retenir :

L'Autorité de la concurrence, tout en sanctionnant lourdement une entreprise pour avoir interdit la vente en ligne de ses produits par ses distributeurs, valide en revanche la possibilité de limiter la revente sur des plateformes tierces.

Pour approfondir :

Le 24 octobre dernier, l'Autorité de la concurrence a sanctionné d'une amende de 7 millions d'euros la pratique d'un fabricant de produits de motoculture consistant à interdire en pratique la vente de ses produits sur les sites internet des distributeurs.

Elle a en revanche pris une position plus souple s'agissant des restrictions imposées quant à la vente via des plateformes tierces (*marketplaces*).

- **Une condamnation de l'interdiction de vente en ligne imposée dans les faits aux distributeurs**

Si la distribution en ligne n'était pas expressément interdite en tant que telle par le fabricant, ce dernier imposait à ses distributeurs une remise des produits en main propre à l'acheteur, ce qui nécessitait dès lors soit un retrait en magasin, soit une livraison en personne au domicile de l'acheteur (alors que cette remise en main propre n'est imposée par aucune réglementation nationale ou européenne), une telle livraison à domicile ayant par ailleurs été freinée par le fabricant jusqu'en 2014.

L'Autorité de la concurrence a ainsi considéré qu'en imposant une telle condition de remise en main propre, le fabricant avait retiré tout intérêt à la vente en ligne pour ses distributeurs et pour les consommateurs, ces derniers n'ayant pas pu pleinement faire jouer la concurrence entre les distributeurs et bénéficier de prix plus intéressants. Certains distributeurs avaient d'ailleurs confirmé qu'ils avaient assimilé cette condition de remise en main propre à une interdiction pure et simple de toute vente à distance.

Selon l'Autorité de la concurrence, cette pratique de restriction de la vente en ligne était disproportionnée en ce qu'elle allait au-delà de ce qui était nécessaire pour préserver la santé du consommateur et constituait, de la part du fabricant, une entente illicite, contraire aux droits français et communautaire de la concurrence.

L'Autorité de la concurrence a considéré que cette interdiction de vente en ligne ne pouvait bénéficier d'aucune exemption. D'une part, le bénéfice du règlement d'exemption par catégorie applicable aux restrictions verticales n'était pas envisageable, dans la mesure où l'interdiction de vente en ligne s'apparentait à une restriction caractérisée des ventes passives (la présence d'une telle restriction caractérisée excluant automatiquement l'exemption prévue par le règlement communautaire). D'autre part, l'Autorité de la concurrence a considéré que la pratique en cause ne remplissait pas les conditions requises pour bénéficier d'une exemption individuelle.

Dans ces circonstances, le fabricant a été condamné à :
- une amende de 7 millions d'euros (qui, malgré son montant, demeure peu élevée au regard de l'amende encourue qui s'élevait à près de 380 millions d'euros) ;
- modifier dans un délai de 3 mois ses contrats de distribution sélective, afin d'y prévoir expressément et clairement la possibilité pour les distributeurs membres du réseau de distribution sélective de procéder à la vente en ligne de tous les produits du fabricant, sans exiger de quelconque remise en main propre ;
- adresser à l'ensemble des points de vente de son réseau, dans ce même délai de 3 mois, une lettre recommandée avec accusé de réception leur annonçant les modifications ainsi apportées à leurs contrats de distribution sélective ;
- procéder à la publication de la condamnation dans une publication nationale et deux publications spécialisées.

- **L'admission de l'interdiction de vente des produits objets d'une distribution sélective *via* des marketplaces**

A l'inverse, dans la lignée de l'arrêt « Coty » rendu par la Cour de justice de l'Union européenne le 6 décembre 2017 (CJUE, affaire n°C-230/16), l'Autorité de la concurrence se prononce en faveur de la possibilité pour un fournisseur d'imposer des restrictions à la vente en ligne par l'intermédiaire de plateformes tierces, s'agissant d'un réseau de distribution sélective.

Dans son communiqué de presse, l'Autorité de la concurrence a d'ailleurs pris le soin d'indiquer que la décision avait *« vocation à préciser le cadre applicable en France pour les différents secteurs et produits, au-delà du secteur de la motoculture »*.

En l'espèce, le fabricant a contractuellement exclu le recours aux ventes sur les places de marché principalement par l'effet de deux clauses insérées dans les accords conclus avec les distributeurs :

- D'une part, le fabricant impose au distributeur de lui communiquer le domaine de premier niveau de la page Internet sur laquelle il envisage de distribuer les produits (notamment lorsque le nom de domaine du site de vente en ligne ne contient pas le nom ou les marques du fabricant), le distributeur devant alors attendre l'autorisation du fabricant avant de débuter la commercialisation des produits par le biais du site concerné ;

- D'autre part, le distributeur s'engage *« à ne proposer, ni directement ni indirectement (par exemple au moyen de liens hypertextes) de produits (…) à la vente via des URL (adresses web ou Internet) de plateformes d'enchères et de vente ou des places de marché en ligne, telles qu'eBay ou Amazon »*.

L'Autorité de la concurrence a estimé que, s'agissant d'un réseau de distribution sélective, cette pratique permet au fabricant, qui n'a aucun lien contractuel avec les plateformes tierces, de s'assurer, de manière à la fois appropriée et proportionnée, que ses produits sont vendus dans des conditions qui préservent son image de marque et garantissent la sécurité du consommateur.

Ainsi, alors que certains s'interrogeaient sur la possibilité de circonscrire la décision « Coty » aux produits de luxe, l'Autorité de la concurrence pose un principe large d'autorisation des restrictions de vente par les *marketplaces* dans les réseaux de distribution sélective, quelle que soit la nature des produits (sous réserve bien entendu que la licéité du recours à un tel mode de distribution ait préalablement été validée, tous les types de produits n'ayant pas vocation à être distribués dans le cadre d'un tel système de distribution sélective) :

> *« À titre liminaire, il importe de préciser que l'analyse opérée par la Cour de justice dans l'arrêt Coty susvisé pour la commercialisation en ligne de produits de luxe paraît susceptible d'être étendue à d'autres types de produits. En effet, si la Cour a pris soin de rappeler que son raisonnement s'inscrivait dans le prolongement des principes dégagés par sa jurisprudence antérieure, et notamment l'arrêt Pierre Fabre précité, qui renvoie lui-même à l'arrêt Metro précité, aux termes de laquelle un système de distribution sélective ou une clause particulière d'un tel système peuvent être licites dès lors qu'ils sont nécessaires à la préservation de la qualité et au bon usage des produits concernés, elle n'a pas apporté davantage de précisions sur la nature desdits produits et n'en a donc pas circonscrit le champ d'application, renvoyant cette appréciation au cas par cas. »* (point 278 de la décision de l'Adlc).

Cette **décision** devrait ainsi renforcer l'engouement des têtes de réseau pour le système de la distribution sélective, lequel connait un essor depuis déjà plusieurs années du fait de l'encadrement qu'il permet quant aux ventes en ligne.

Il demeurera néanmoins nécessaire pour la mise en place d'un tel système, d'en vérifier préalablement la faisabilité juridique, puisque – comme cela a été précédemment rappelé – le recours à la distribution sélective n'est envisageable que s'il est justifié, notamment par le type de produits concernés.

En particulier, l'accord mettant en place un système de distribution sélective devra impérativement prévoir la sélection des distributeurs sur la base de critères objectifs qui seront à la fois :

- de caractère qualitatif, fixés de manière uniforme pour tous les revendeurs potentiels et appliqués de façon non discriminatoire.

  Comme le rappelle l'Autorité de la concurrence dans la décision commentée, *« l'appréciation de la nature qualitative des critères de sélection des revendeurs requiert nécessairement l'examen des propriétés du produit en cause, afin de vérifier, d'une part, que celles-ci nécessitent, pour préserver la qualité du produit et en assurer le bon usage, un système de distribution sélective et, d'autre part, qu'il n'est pas déjà satisfait à ces objectifs par la réglementation nationale »*.

- proportionnés, c'est-à-dire n'allant pas au-delà de ce qui est nécessaire pour l'objectif poursuivi (tel que les objectifs légitimes de préservation de la qualité des produits et de sécurisation de leur bon usage, ou encore de garantie de sécurité pour le consommateur).

A rapprocher : Décision n°18-D-23 du 24 octobre 2018 relative à des pratiques mises en œuvre dans le secteur de la distribution de matériel de motoculture

CONTENUS ILLICITES / E-RÉPUTATION

L'abonné titulaire d'une connexion internet reste responsable des atteintes aux droits de propriété intellectuelle en cas de téléchargement illicite
CJUE, 3ème ch., 18 octobre 2018, Bastei Lübbe GmbH & Co. KG / M. X.

Ce qu'il faut retenir :

L'utilisateur ne saurait s'exonérer de sa responsabilité en désignant un membre de sa famille comme étant celui qui aurait utilisé sa connexion internet pour porter atteinte à un droit d'auteur.

Pour approfondir :

Une personne de nationalité allemande a partagé un livre audio au moyen de sa connexion internet aux fins de son téléchargement, avec un nombre illimité d'utilisateurs d'une bourse d'échanges sur Internet (peer-to-peer).

Un expert a attribué avec exactitude l'adresse IP concernée à une personne (l'Utilisateur).

Bastei Lübbe, société allemande titulaire des droits d'auteur et des droits voisins sur la version audio du livre, a mis en demeure l'Utilisateur de mettre fin à l'atteinte du droit d'auteur constatée.

Sans retour de l'Utilisateur, le détendeur des droits a assigné l'Utilisateur en sa qualité de titulaire de cette adresse IP, afin d'obtenir une indemnisation pécuniaire.

L'Utilisateur a alors contesté avoir porté lui-même atteinte au droit d'auteur et a soutenu que sa connexion était suffisamment sécurisée. En outre, il fait valoir que ses parents, qui vivent sous le même toit que lui, avaient également accès à cette connexion. L'Utilisateur fait par ailleurs valoir que son ordinateur aurait été éteint au moment où l'atteinte au droit d'auteur a eu lieu.

L'Amtsgericht München, le Tribunal de district de Munich, a rejeté le recours indemnitaire de Bastei Lübbe au motif que l'Utilisateur ne pouvait être tenu pour responsable de l'atteinte au droit d'auteur invoquée, dès lors qu'il avait indiqué que l'adresse IP identifiée par l'expert n'était pas personnellement attribuée à l'Utilisateur dès lors que ses parents disposaient de la même adresse lors de leurs connexions et étaient en conséquence susceptibles d'être également les auteurs de l'atteinte.

Selon la loi allemande, le détenteur d'une connexion internet est présumé être l'auteur d'une atteinte commise via cette connexion dès lors qu'il est identifié par son adresse IP et que personne d'autre n'a la possibilité d'y accéder.

En revanche, s'il désigne un membre de sa famille qui comme lui peut utiliser sa connexion internet (donc avec la même adresse IP), il ne peut voir sa responsabilité engagée et ce, sans avoir à donner davantage d'explications en vertu du droit à la vie privée et des dispositions du droit constitutionnel allemand relatives à protection du mariage et de la famille.

En appel devant le Landgericht München I, le Tribunal régional de Munich a décidé de surseoir à statuer et de poser à la Cour de Justice de l'Union Européenne (CJUE) des questions préjudicielles tendant à savoir si les sanctions contre les atteintes au droit de mise à disposition du public d'une œuvre et les mesures pour assurer le respect des droits de propriété intellectuelle restent-elles toujours efficaces, dissuasives et effectives lorsque le titulaire d'une connexion à Internet par laquelle des atteintes au droit d'auteur ont été commises par un partage de fichiers ne verra pas sa responsabilité engagée quand il désigne à tout le moins un membre de la famille qui avait comme lui la possibilité d'accéder à cette connexion à Internet, sans donner davantage de précisions tirées de recherches faites sur le moment et la nature de l'utilisation d'Internet par ce membre de la famille ?

La Cour a considéré que la décision préjudicielle devait induire une conciliation des différents droits fondamentaux invoqués conduisant à un juste équilibre des droits.

En l'espèce, la protection induite par le droit national, quasi absolue aux membres de la famille du titulaire d'une connexion à Internet, par laquelle des atteintes au droit d'auteur ont été commises au moyen d'un partage de fichiers fait obstacle au respect des droits de propriété intellectuelle.

La CJUE indique néanmoins qu'il en irait autrement si, en vue d'éviter une ingérence jugée inadmissible dans la vie familiale, les titulaires de droits pouvaient disposer d'une autre forme de recours effectif, leur permettant notamment, dans ce cas, de faire reconnaître la responsabilité civile du titulaire de la connexion à Internet en cause.

Dès lors, la Cour a affirmé que « *l'article 8, paragraphes 1 et 2, de la directive 2001/29/CE du Parlement européen et du Conseil, du 22 mai 2001, sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information, lu en combinaison avec l'article 3, paragraphe 1, de celle-ci, d'une part, et l'article 3, paragraphe 2, de la directive 2004/48/CE du Parlement européen et du Conseil, du 29 avril 2004, relative au respect des droits de propriété intellectuelle, d'autre part, doivent être interprétés en ce sens qu'ils s'opposent à une législation nationale, telle que celle en cause au principal, interprétée par la juridiction nationale compétente, en vertu de laquelle le détenteur d'une connexion à Internet, par laquelle des atteintes au droit d'auteur ont été commises au moyen d'un partage de fichiers, ne peut voir sa responsabilité engagée, dès lors qu'il désigne à tout le moins un membre de sa famille qui avait la possibilité d'accéder à cette connexion, sans donner davantage de précisions quant au moment où ladite connexion a été utilisée par ce membre de sa famille et à la nature de l'utilisation qui a été faite de celle-ci par ce dernier* ».

Il en découle que l'Utilisateur ne saurait s'exonérer de sa responsabilité en désignant un membre de sa famille comme étant celui qui aurait utilisé sa connexion internet pour porter atteinte à un droit d'auteur.

A rapprocher : Directive 2001/29/CE du Parlement européen et du Conseil du 22 mai 2001

INTERNATIONAL

Première sanction financière depuis l'entrée en application du RGPD

Un hôpital condamné par la CNIL portugaise à une amende de 400 000 €

Ce qu'il faut retenir :

Le CNPD (Comissão Nacional de Proteção de Dados), homologue portugais de la CNIL, a prononcé à l'encontre de l'Hôpital Barreiro-Montijo une amende de 400 000 € pour non-respect du Règlement Européen (UE) 2016-679 sur la Protection des Données.

Il s'agit de la première sanction financière prise depuis l'entrée en application du RGPD contre un établissement de santé.

Pour approfondir :

Le CNPD a constaté que la politique d'accès aux bases de données des patients de l'hôpital ne respectait pas les exigences de la réglementation. En effet, en juin 2018, l'ordre des médecins avait alerté le CNPD sur de nombreuses non-conformités.

Les manquements relevés étaient divers : accès réservés en principe aux médecins utilisés par des personnels administratifs, comptes des médecins ayant quitté l'établissement toujours actifs (985 comptes versus 296 médecins en poste…), mauvaise gestion des habilitations, et faiblesses du système d'habilitation révélées à l'occasion de la création d'un compte test par les services du CNPD.

Les arguments avancés par l'établissement de soins pour tenter d'échapper à sa responsabilité n'étaient pas très convaincants. Il a d'abord tenté de se dédouaner en invoquant le fait que le ministère de la santé portugais fixait les règles relatives aux données de santé. Il a ensuite invoqué l'absence de transposition du RGPD dans la loi nationale, puis l'absence de moyens informatiques dont dispose l'hôpital pour gérer le système d'habilitation. Or, faut-il le rappeler, un règlement européen est d'application directe sur tout le territoire de l'Union européenne sans qu'il soit besoin de le transposer. Enfin, il est apparu, à l'occasion du contrôle, que l'outil informatique de l'établissement permettait une parfaite gestion des habilitations.

Le CNPD a donc retenu des manquements graves au RGPD : violation des principes d'intégrité et de confidentialité des données, violation du principe de minimisation de l'accès aux données et absence de garantie de l'intégrité des données. Pour ces infractions, l'autorité de contrôle a condamné le Centre Hospitalier, responsable de traitement, à deux amendes de 150 000 euros et une troisième de 100 000 euros, soit au total 400 000 €.

L'établissement de soins a annoncé avoir interjeté appel de la décision. Affaire à suivre…

A rapprocher : Guide pratique sur la protection des données à destination des médecins libéraux

***

ACTUALITÉ NUMÉRIQUE SIMON ASSOCIÉS

NOVEMBRE 2018

Le délégué à la protection des données : profil, missions et ressources
Petit-déjeuner organisé par SIMON ASSOCIES (intervenant : AMIRA BOUNEDJOUM) et ZIWIT
23 novembre 2018 – Montpellier
En savoir plus et s'inscrire

3ème Village de la LegalTech
Simon Associés animera une conférence sur le thème :
« *Legal tech : quel avenir pour les juristes dans l'évolution des métiers du droit ?* »
27-28 novembre 2018 – Paris
En savoir plus

DECEMBRE 2018

Quelle solution concrète pour piloter la conformité au RGPD ?
Conférence-débat organisée par Simon Associés et Visiativ
10 décembre 2018 – Paris
En savoir plus et s'inscrire

Constituer et protéger sa base de données : des contraintes du RGPD au dépôt APP
Webinar co-animé par AMIRA BOUNEDJOUM,
en partenariat avec l'APP (Agence pour la Protection des Programmes)
13 décembre 2018 – Live