SOMMAIRE

PARIS - NANTES
MONTPELLIER - LYON
PERPIGNAN

Bureaux intégrés

AIX-EN-PROVENCE BORDEAUX - CAEN CLERMONT-FERRAND LE HAVRE - LYON MARSEILLE - METZ - ROUEN SAINT-DENIS (La Réunion) SAINT-ETIENNE

Réseau SIMON Avocats

ALGÉRIE - ARGENTINE ARMÉNIE - AZERBAÏDJAN BAHAMAS - BAHREÏN BANGLADESH - BELGIQUE BIRMANIE - 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 MALTE - MADAGASCAR MAROC - MEXIQUE NICARAGUA - OMAN PANAMA - PARAGUAY - PÉROU PORTUGAL - RD CONGO RÉPUBLIQUE DOMINICAINE SENEGAL - SINGAPOUR THAÏLANDE - TUNISIE URUGUAY - VENEZUELA VIETNAM

Conventions transnationales

www.simonassocies.com
www.lettredunumerique.com

DATA / DONNÉES PERSONNELLES

Le cybercommerçant qui intègre un bouton « j'aime » de Facebook sur son site internet est un responsable conjoint de traitement

CJUE, 2ème ch., 29 juillet 2019, *Fashion ID GmbH & Co. KG / Verbraucherzentrale NRW eV, Facebook Ireland Ltd et autre*

Ce qu'il faut retenir :

Intégrer un bouton « j'aime » du réseau social Facebook sur son site internet entraîne la qualification de responsable conjoint de traitement de l'administrateur du site internet aux côtés de Facebook.

Pour approfondir :

Fashion ID est une entreprise de vente de vêtements de mode en ligne qui a inséré sur son site Internet le module social « j'aime » du réseau social Facebook.

En raison de la présence de ce module, lorsqu'un internaute navigue sur le site internet de Fashion ID, des données à caractère personnel le concernant sont transmises à Facebook Ireland et ce, même si l'internaute n'est pas membre du réseau social.

Les données de cet internaute sont également transmises à Facebook même s'il n'a pas cliqué sur le bouton « j'aime ».

Une association d'utilité publique de défense des intérêts des consommateurs – la Verbraucherzentrale NRW – reproche à Fashion ID d'avoir transmis à Facebook Ireland les données à caractère personnel des visiteurs de son site internet sans le consentement de ces derniers et en violation des obligations d'information prévues par la réglementation applicable en matière de protection des données personnelles.

L'association a alors intenté une action en cessation contre Fashion ID devant le tribunal régional de Düsseldorf, afin que la société mette fin à cette pratique.

Le tribunal allemand ayant partiellement fait droit aux demandes de l'association, Fashion ID a interjeté appel de la décision en soutenant notamment que le tribunal régional de Düsseldorf l'avait à tort jugé responsable du traitement issu du module social.

Fashion ID a notamment soutenu qu'en intégrant le bouton « j'aime » de Facebook, elle ne décide ni des données qui peuvent être collectées ni de la transmission de celles-ci à Facebook.

La juridiction de renvoi s'est alors interrogée sur la qualification de Fashion ID et son niveau de responsabilité, sur le fait de savoir si le traitement des données à caractère personnel en cause est licite et si les obligations d'information des personnes concernées pèsent sur Fashion ID ou sur Facebook Ireland.

Cette dernière question revêt un caractère particulièrement important dans la mesure où si une insertion de contenus externes sur un site internet donne lieu à un traitement de données, l'étendue et la finalité de ce traitement sont néanmoins inconnues de celui qui réalise cette insertion.

Dès lors, celui-ci n'est pas en mesure de fournir l'information à laquelle il est tenu.

Ainsi, la juridiction de renvoi considère que faire peser sur le gestionnaire d'un site internet l'obligation d'informer la personne concernée, alors que lui-même ne dispose pas de cette information, conduirait en pratique à interdire l'insertion de contenus externes.

Dans ces conditions, la juridiction de renvoi a décidé de surseoir à statuer et de poser à la Cour de Justice de l'Union Européenne plusieurs questions préjudicielles et notamment les deux questions suivantes :

- « *Dans un cas comme celui de l'espèce, où quelqu'un insère dans son site un code programme permettant au navigateur de l'utilisateur de solliciter des contenus d'un tiers et de transmettre à cet effet au tiers des données à caractère personnel, celui qui fait l'insertion est-il « responsable du traitement », au sens de l'article 2, sous d), de la directive [95/46], lorsqu'il ne peut avoir lui-même aucune influence sur ce processus de traitement des données ?* »

- « *L'obligation d'informer la personne concernée en vertu de l'article 10 de la directive [95/46] dans une situation telle que celle qui se présente en l'espèce pèse-t-elle également sur le gestionnaire du site qui a inséré le contenu d'un tiers et est ainsi à l'origine du traitement des données à caractère personnel fait par un tiers ?* »

Pour répondre à ces questions, la Cour a rappelé que la notion de « responsable du traitement » vise l'organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel.

Dès lors, cette notion implique qu'il est possible que plusieurs acteurs participent au même traitement.

La Cour a, par ailleurs, considéré qu'une personne physique ou morale qui exerce une influence sur le traitement de données à caractère personnel, participe de ce fait à la détermination des finalités et des moyens de ce traitement et peut donc être considérée comme responsable du traitement.

En poursuivant son analyse, la Cour a considéré que Fashion ID a offert la possibilité au réseau social de détenir des données personnelles des visiteurs de son site internet en insérant le bouton « j'aime » puisque l'insertion de ce bouton déclenche la transmission automatique des données concernant les internautes dès l'instant où ces derniers se rendent sur le site internet de Fashion ID.

En effet, Fashion ID a inséré sur son site internet le bouton « j'aime » de Facebook tout en étant consciente que ce module social sert d'outil de collecte et de transmission de données à caractère personnel des visiteurs de son site, que ceux-ci soient membres ou non du réseau social Facebook et même si les visiteurs ne cliquent pas sur ce bouton.

En conséquence, en insérant le bouton « j'aime » sur son site internet, Fashion ID exerce une influence déterminante sur la collecte et la transmission des données à caractère personnel des visiteurs au profit de Facebook Ireland.

En outre, la Cour précise que la circonstance que Fashion ID n'a pas accès aux données personnelles collectées et transmises Facebook ne fait pas obstacle à la qualité de responsable du traitement.

En conséquence, compte tenu de ces éléments, la Cour a considéré que « *le gestionnaire d'un site Internet, tel que Fashion ID, qui insère sur ledit site un module social permettant au navigateur du visiteur de ce site de solliciter des contenus du fournisseur dudit module et de transmettre à cet effet à ce fournisseur des données à caractère personnel du visiteur, peut être considéré comme étant responsable du traitement […] ; Cette responsabilité est cependant limitée à l'opération ou à l'ensemble des opérations de traitement des données à caractère personnel dont il détermine effectivement les finalités et les moyens, à savoir la collecte et la communication par transmission des données en cause* ».

S'agissant des obligations d'information, la Cour a considéré que lorsque le gestionnaire d'un site Internet insère sur son site un tel module social, les obligations en matière de recueil de consentement et d'information pèsent sur le gestionnaire du site en ce qui concerne les seules opérations de traitement des données dont ce dernier détermine les finalités et les moyens de traitement.

A rapprocher : Articles 4, 5, 12, 25 et 26 du RGPD

La CNIL publie de nouvelles lignes directrices en matière de cookies
Délibération n°2019-093 du 4 juillet 2019

Ce qu'il faut retenir :

Par une délibération en date du 4 juillet 2019, la CNIL publie de nouvelles lignes directrices relatives aux opérations de lecture ou écriture dans le terminal d'un abonné ou utilisateur, et notamment à l'utilisation de cookies et autres traceurs. La CNIL œuvre ainsi dans le sillage du Règlement européen sur la protection des données qui a renforcé le régime juridique relatif au consentement.

Pour approfondir :

Dans ce contexte, l'article 82 de la **loi Informatique et Libertés** modifiée impose de recueillir le consentement de la personne concernée (tout abonné ou utilisateur d'un service de communications électroniques) avant toute action qui viserait au stockage ou à l'accès à des informations stockées sur son terminal.

De cet article découlent deux actions distinctes imposées au responsable de traitement : une première se caractérisant par la délivrance d'une information claire et complète, la seconde se caractérisant par le recueil du consentement de l'abonné ou de l'utilisateur.

Dans ce contexte, les nouvelles lignes directrices précisent que l'abonné ou l'utilisateur doit avoir préalablement exprimer sa volonté de manière *« libre, spécifique, éclairée et univoque par une déclaration ou*

par un acte positif clair ». En outre, l'abonné ou l'utilisateur doit consentir indépendamment et spécifiquement pour chaque finalité. La Commission rappelle que la poursuite de la navigation, l'utilisation d'une application mobile, le fait de faire défier une page (*scrolling*), l'utilisation de cases pré-cochées ou encore l'acceptation globale de conditions générales d'utilisation ne constituent point un recueil de consentement valable.

Les responsables de traitement doivent ainsi recueillir un consentement valable, être en mesure de prouver ledit recueil et fournir une information claire et transparente.

En effet, les lignes directrices rappellent les caractéristiques de l'information délivrée aux personnes concernées. Celle-ci doit être *« complète, visible, et mise en évidence au moment du recueil du consentement ».* Quant au contenu de l'information, la CNIL priorise trois éléments principaux : l'identité du ou des responsable(s) de traitement, la finalité des opérations de lecture ou écriture des données, et l'existence du droit de retirer son consentement

Rappelons dans ce cadre que certains cookies et traceurs ne sont pas soumis au recueil du consentement. Il s'agit des cookies et traceurs ayant pour finalité *« exclusive de permettre ou faciliter la communication par voie électronique »* ou *« strictement nécessaires à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur ».* Les lignes directrices précisent que bien que le recueil du consentement soit exclu, une information complète doit être délivrée aux abonnées ou utilisateurs.

Ces nouvelles lignes directrices intègrent le plan d'action de la CNIL relatif au ciblage publicitaire et ont vocation à abroger la délibération de la CNIL en date de 2013 portant adoption d'une recommandation relative aux cookies et autres traceurs.

Une nouvelle recommandation présentera en 2020 le mode opératoire de recueil du consentement et parachèvera les lignes directrices de juillet dernier. Les entités concernées disposeront dès lors d'une période de six mois pour se conformer à ce nouveau texte.

A rapprocher : ***Délibération n°2019-093 du 4 juillet 2019 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture ou écriture dans le terminal d'un utilisateur (notamment aux cookies et autres traceurs) (rectificatif)*** **;** ***Cookies et autres traceurs : la CNIL publie de nouvelles lignes directrices***

PROPRIÉTÉ INTELLECTUELLE

Rappel utile : un nom de domaine peut constituer une antériorité à une marque
CA Aix en Provence, 4 juillet 2019, RG n°17/01088

Ce qu'il faut retenir :

Les noms de domaine peuvent constituer des antériorités rendant indisponible un signe à sa réservation comme marque bien qu'ils ne soient pas visés par l'article L.711-4 du Code de la propriété intellectuelle qui donne une liste, non limitative, des antériorités.

Pour approfondir :

L'arrêt rendu par la cour d'appel d'Aix en Provence le 4 juillet dernier n'apporte pas d'enseignement particulièrement nouveau en droit des marques mais offre l'occasion de faire un rappel des règles existantes en matière de disponibilité du signe.

L'affaire opposait le titulaire d'une marque qui estimait être victime d'actes de contrefaçon de celle-ci en raison de **l'exploitation d'un nom de domaine** similaire. En défense, la société poursuivie contestait la validité de la marque qui lui était opposée en faisant valoir le fait que le nom de domaine avait été réservé et exploité antérieurement au dépôt de la marque, le nom de domaine constituait donc une antériorité à la marque.

La cour d'appel rappelle les dispositions de l'article L.711-4 du Code de la propriété intellectuelle selon lesquelles « *ne peut être adopté comme marque un signe portant atteinte à des droits antérieurs* » dont il donne une liste rappelant également que cette liste n'est pas limitative, par conséquent « *un nom de domaine constitue un signe distinctif dont l'antériorité peut être revendiquée pour demander l'annulation d'une marque dès lors que cette antériorité est certaine, se traduisant par une exploitation effective, et qu'il existe un risque de confusion généré par la concomitance des deux signes* ».

L'examen des faits révélait que le nom de domaine avait été réservé avant le dépôt de la marque et était également exploité antérieurement. Le risque de confusion en raison de l'exploitation concomitante du nom de domaine et de la marque était également établi. Par conséquent, le nom de domaine, réservé et exploité avant le dépôt de la marque, constituait bien une antériorité à celle-ci justifiant l'annulation de la marque. L'action en contrefaçon est donc tenue en échec et, pire, se solde par l'annulation de la marque faute de vérification de la disponibilité du signe au moment du dépôt et à nouveau avant d'engager l'action en contrefaçon pour anticiper les demandes reconventionnelles.

Avant de réserver une marque, les diligences préalables imposent de procéder à la vérification de la disponibilité du signe et donc de l'existence de droits antérieurs sur la dénomination. Cette recherche ne doit pas se limiter aux marques déposées mais doit porter, plus largement, sur tous les signes distinctifs (nom de domaine, enseigne, dénomination sociale, etc.) il est donc recommandé de recourir aux services d'un professionnel.

A rapprocher : Articles L.711-4 et L.714-3 du Code de la propriété intellectuelle

---

La délicate preuve de l'acquisition du caractère distinctif par l'usage d'une marque
TPIUE, 19 juin 2019, aff. T-307/17

Ce qu'il faut retenir :

L'équipementier ADIDAS vient de subir un revers important devant le Tribunal de première instance de l'Union européenne qui annule la marque aux trois bandes faute de caractère distinctif.

Pour approfondir :

La condition tenant au **caractère distinctif du signe** est consubstantielle au droit des marques précisément parce qu'une marque est un signe qui doit être apte à permettre au consommateur d'identifier l'origine du produit qui en est revêtu.

Selon la législation tant française qu'européenne, ce caractère distinctif doit exister dès l'origine mais peut être acquis par l'usage. C'est précisément ce dernier aspect qui était en cause dans l'affaire ayant conduit le TPIUE à annuler la marque déposée par ADIDAS consistant en un signe figuratif composé de trois bandes noires.

L'équipementier ADIDAS avait en effet déposé une demande d'enregistrement d'un signe figuratif représentant ses célèbres 3 bandes décrites ainsi : « *La marque consiste en trois bandes parallèles équidistantes de largeur égale, appliquées sur le produit dans n'importe quelle direction* » pour désigner en classe 25 les « *vêtements, chaussures* ».

La validité de cette marque a été contestée et la division d'annulation a fait droit à la demande en nullité, au motif que la marque en cause était dépourvue de tout caractère distinctif, tant intrinsèque qu'acquis par l'usage. L'équipementier a formé un recours dans lequel il n'a pas contesté l'absence de caractère distinctif intrinsèque de la marque en cause mais a, en revanche, fait valoir que cette marque avait acquis un caractère distinctif par l'usage. Toutefois, la chambre des recours a considéré que la preuve que ladite marque avait acquis, dans l'ensemble de l'Union européenne, un caractère distinctif par l'usage n'était pas rapportée et a donc confirmé la nullité de la marque.

C'est dans ce contexte que l'affaire a été portée devant le TPIUE qui, à son tour, a estimé que le signe n'avait pas acquis de caractère distinctif et a confirmé la nullité de la marque aux termes d'un **jugement rendu le 19 juin 2019**.

La décision considère, en premier lieu, que certains des éléments de preuve fournis ne sont pas probants et, en second lieu, que les autres sont insuffisants à démontrer le caractère distinctif acquis par l'usage.

Concernant les preuves qui étaient fournies tendant à démontrer l'acquisition du caractère distinctif du signe par l'usage qui en a été fait, le Tribunal rappelle que l'appréciation doit porter sur l'usage de la marque sous la forme sous laquelle celle-ci a été soumise à l'enregistrement et, le cas échéant, enregistrée, mais également sur l'usage de la marque sous des formes qui ne diffèrent de cette forme que par des variations négligeables et qui, de ce fait, peuvent être considérées comme globalement équivalentes à ladite forme.

Or, compte tenu de l'extrême simplicité de la marque en cause, dans la mesure où cette marque présentait relativement peu de caractéristiques et consistait en trois lignes noires parallèles dans une configuration rectangulaire sur un fond blanc, même une légère

variation pouvait entraîner une altération significative des caractéristiques de la marque, de sorte que la forme modifiée ne pourra pas être considérée comme globalement équivalente à la forme enregistrée de ladite marque. En effet, plus une marque est simple, moins elle est susceptible d'avoir un caractère distinctif et plus une modification apportée à cette marque est susceptible d'affecter une de ses caractéristiques essentielles et d'altérer ainsi la perception de ladite marque par le public pertinent.

Le Tribunal conclut donc que la chambre de recours était fondée à écarter les éléments de preuve montrant non la marque en cause, mais d'autres signes consistant en trois bandes blanches (ou claires) sur un fond noir (ou foncé).

Concernant la preuve de l'acquisition du caractère distinctif du signe, le Tribunal encore se montrer particulièrement rigoureux. En particulier, il estime que les images produites en grand nombre ne fournissent aucune indication sur l'importance et la durée de l'usage ni sur l'impact dudit usage sur la perception de cette marque par le public pertinent. Elles ne permettent pas de démontrer que cet usage a été suffisant pour qu'une fraction significative du public pertinent identifie grâce à la marque en cause le produit comme provenant d'une entreprise déterminée. S'agissant ensuite des données relatives au chiffre d'affaires et aux dépenses de marketing et de publicité, il conclut au fait qu'il n'est pas possible d'établir un lien entre les données chiffrées fournies par la requérante et la marque en cause ainsi qu'entre ces données et les produits en cause, et qu'elles ne sont donc pas pertinentes pour démontrer l'acquisition du caractère distinctif par l'usage.

La décision est pour le moins sévère : on sait que la preuve de l'acquisition du caractère distinctif d'un signe est délicate certes, mais dans cette affaire il nous semble que les juges ont fait montre d'une rigueur excessive. Pour limiter la portée de cette décision, on rappellera toutefois qu'elle ne concerne que la marque européenne, les titres nationaux restant, pour leur part, valides.

A rapprocher : Article 7, § 1, du règlement UE n°207/2009 du 26 février 2009 sur la marque communautaire (devenu art. 7, § 3, du règlement UE 2017/1001 du 14 juin 2017, sur la marque de l'Union européenne)

SERVICES NUMÉRIQUES

Proposition de loi Avia pour mieux lutter contre la haine en ligne

Proposition de loi, adoptée par l'Assemblée nationale, visant à lutter contre les contenus haineux sur internet le 9 juillet 2019, T.A. n°310

Ce qu'il faut retenir :

L'Assemblée nationale a voté, le 9 juillet 2019, la proposition de loi de Laetitia Avia pour lutter contre les contenus haineux sur internet. La proposition a par la suite été notifiée à la Commission européenne, le 21 août, comme il convient de le faire lorsqu'un État membre entend réguler le secteur des nouvelles technologies. Cette notification a ouvert une période de *statu quo* de trois mois au cours duquel le processus législatif interne est suspendu.

Sur le fond, cette proposition contraint les plateformes et les moteurs de recherche à retirer les contenus manifestement illicites sous 24 heures, sous peine d'être condamnés à des amendes allant jusqu'à 1,25 millions d'euros. Le texte prévoit également des mécanismes de contrôle des nouvelles prérogatives accordées aux plateformes et moteurs de recherche, en imposant une transparence sur les moyens mis en œuvre et les résultats obtenus, ainsi qu'une coopération renforcée avec la justice.

Pour approfondir :

- **Suspension de la procédure d'adoption de la proposition de loi Avia**

La proposition de loi de Laetitia Avia pour lutter contre les contenus haineux sur internet a été adoptée par l'Assemblée nationale le 9 juillet 2019. Cependant, elle n'a pas encore été soumise au vote su Sénat. En effet, en vertu de la Directive (UE) 2015/1535, les Etats membres sont tenus de notifier à la Commission européenne, leurs projets et propositions de loi concernant les produits et les services de la société de l'information.

Le 21 août 2019, l'Etat français s'est donc conformé à cette obligation et a notifié la proposition de loi à la Commission européenne.

A partir de la date de notification de la proposition de loi, une période de *statu quo* de trois mois a débuté.

Durant cette période, l'Etat membre ne peut adopter la règle technique en question.

Une procédure d'urgence est prévue par la Directive, afin de permettre l'adoption immédiate d'un projet de loi, mais la Commission européenne a rejeté la demande de la France visant à la mettre en œuvre. La Commission a en effet considéré que les conditions d'urgence, à savoir l'existence d'« *une situation grave et imprévisible qui a trait à la protection de la santé publique ou à la sécurité, à la protection des animaux ou à la protection des végétaux* » n'étaient pas réunies.

Il convient de noter que cette période de *statu quo* supplémentaire pourrait d'ailleurs être étendue de trois mois supplémentaires s'il apparaissait que le texte notifié était susceptible de créer des obstacles à la libre circulation des marchandises ou à la libre prestation de services de la société de l'information ou au droit dérivé de l'Union européenne. Dans cette hypothèse, la Commission et les autres Etats membres doivent émettre un avis circonstancié à l'Etat à l'origine de la notification.

La proposition de loi ne pourra donc être présentée au Sénat, au plus tôt, que le 21 novembre 2019.

En attendant que le texte soit présenté au Sénat, il est entre les mains de la Commission des lois constitutionnelles, de la législation et de l'administration générale de la République qui assure le dialogue avec la Commission européenne.

- **Mesures prévues par la proposition de loi Avia**

S'agissant du fond, cette proposition de loi contient de nombreuses mesures qui méritent d'être détaillées.

  - **Suppression des contenus haineux par les plateformes et les moteurs de recherche dans les 24 heures de leur notification.**

La principale mesure de cette proposition de loi consiste à imposer aux plateformes un délai de 24h pour retirer les commentaires manifestement illicites, après notification par une ou plusieurs personnes. L'article 1er ter III précise que les éventuels signalements abusifs par les utilisateurs de plateforme seront eux, passibles d'un an d'emprisonnement et de 15 000 euros d'amende.

Les publications concernées sont celles portant sur l'apologie des crimes contre l'humanité, provoquant à la commission d'actes de terrorisme, faisant l'apologie de tels actes ou comportant une incitation à la haine, à la violence, à la discrimination ou une injure envers une personne ou un groupe de personnes à raison de l'origine, d'une prétendue race, de la religion, de l'ethnie, de la nationalité, du sexe, de l'orientation sexuelle, de l'identité de genre ou du handicap.

  - **Le contrôle des agissements des plateformes et des moteurs de recherche**

Les plateformes privées et les moteurs de recherche visés par l'article premier de la proposition de loi ont déjà développé leur propre système d'automatisation de la modération des contenus.

De nombreux politiques et journalistes se sont inquiétés du rôle de censeur laissé à ces acteurs privés.

Une série d'amendements est ainsi venue apporter des précisions sur les modalités concrètes de traitement des notifications.

Ces amendements prévoient notamment que soient mis en place par les plateformes, des procédures, des moyens technologiques et des moyens humains appropriés, afin d'éviter tout retrait injustifié.

Un autre amendement impose en outre aux opérateurs de s'assurer qu'un contenu retiré ne soit pas, par la suite, rediffusé et devienne viral.

  - **Création d'un parquet numérique**

La proposition de loi comprend un nouveau chapitre consacré au volet pénal, avec la création d'un parquet numérique et d'une juridiction spécialisée. Leur mise en place sera précisée par une circulaire et ce, dès l'adoption définitive de cette proposition de loi.

  - **Rôle du Conseil supérieur de l'audiovisuel (CSA) dans la lutte contre les contenus haineux en ligne**

La proposition de loi prévoit également que le CSA s'assure du contrôle de la bonne exécution par les plateformes et les moteurs de recherche, de l'ensemble de leurs obligations issues de la proposition de loi. Il bénéficie également d'un pouvoir de sanction. En effet, l'article 4, II de la proposition dispose :

> *« En cas de manquement par un opérateur mentionné au premier alinéa du I de l'article 6-2 de la loi n°2004-575 du 21 juin 2004 précitée au devoir de coopération dans la lutte contre les contenus*

haineux en ligne résultant de l'article 6-3 de la même loi, le Conseil supérieur de l'audiovisuel peut engager une procédure de sanction ».

La proposition de loi prévoit à ce titre que le CSA, en premier lieu, mette en demeure l'opérateur de se conformer à ses obligations ou aux recommandations qu'il adopte, dans le délai qu'il fixe, puis, en l'absence de mise en conformité, il peut prononcer une sanction pécuniaire dont le montant prend en considération la gravité des manquements commis et, le cas échéant, leur caractère réitéré, sans pouvoir excéder 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent.

A rapprocher : Proposition de loi, adoptée par l'Assemblée nationale, visant à lutter contre les contenus haineux sur internet le 9 juillet 2019, T.A. n°310

E-COMMERCE

Absence d'entente malgré des comportements parallèles de refus de contracter dans le secteur du commerce électronique
Décision de l'Autorité de la concurrence n°19-D-18 du 31 juillet 2019

Ce qu'il faut retenir :

Des comportements parallèles de ruptures de contrat et de refus de contracter par la plupart des acteurs du marché ne constituent pas nécessairement une entente anticoncurrentielle

Pour approfondir :

En début d'année 2019, une entreprise active dans le téléchargement de fichiers en ligne – téléchargements que l'Autorité de la concurrence décrit comme étant réalisés dans des conditions illicites – a saisi l'ADLC de pratiques mises en œuvre par plusieurs prestataires de paiement en ligne.

La saisissante reprochait aux prestataires de paiement, d'avoir procédé à des ruptures unilatérales de contrat, ou d'avoir refusé de contracter avec elle (directement ou par le recours à des causes que la saisissante qualifiait de « léonines »), qui l'auraient privée d'une solution de paiement « vente à distance » (VAD) indispensable à son activité d'hébergement de fichiers.

Elle soutenait que ces refus constituaient des pratiques anticoncurrentielles au sens des articles L.420-1 et L.420-2 du Code de commerce. En effet, ces pratiques auraient été de nature à évincer certains acteurs, tels que la saisissante, du marché de l'hébergement de fichiers et des réseaux de diffusion de contenus. Elle soutenait par ailleurs que les prestataires VAD auraient collectivement abusé de son état de dépendance économique à leur égard.

1. L'activité illicite de l'entreprise saisissante

Depuis 2014, plusieurs rapports et études officiels ou indépendants avaient établi que le site de la saisissante servait à héberger des fichiers susceptibles d'enfreindre la législation sur le droit d'auteur, notamment de fichiers « contrefaisants » au sens des dispositions du Code de la propriété intellectuelle relatives au délit de contrefaçon d'œuvres de l'esprit ou de logiciels. Le site fournissait en effet des espaces de stockages aux membres, dans lesquels étaient principalement stockés des fichiers vidéo (ex : films) en vue du stockage ou du partage ultérieur de ces fichiers par l'utilisateur.

2. Les marchés pertinents

S'agissant des marchés pertinents sur lesquels les pratiques sont jugées, l'Autorité de la concurrence rappelle sa pratique décisionnelle (décision n°11-D-11 du 7 juillet 2011 relative à des pratiques mises en œuvre par le Groupement des Cartes Bancaires) qui a identifié 3 marchés distincts :

- un marché amont, sur lequel les systèmes de paiement par carte se font concurrence pour affilier les établissements de crédit ou de paiement,
- deux marchés aval :
  - le marché de l'émission relatif à la distribution de cartes auprès des consommateurs, et
  - le marché de l'acquisition concernant l'affiliation de commerçants.

L'Autorité de la concurrence considère qu'une délimitation plus précise de ces marchés, que ce soit le marché de l'acquisition dans sa dimension géographique ou le marché des services d'hébergement et de partage de fichiers numériques,

dans ses dimensions matérielle et géographique, n'apparaît pas nécessaire dans cette affaire.

3. Le rejet de la qualification d'entente

Pour rappel, la reconnaissance d'une entente nécessite que soit établi l'objet ou l'effet anticoncurrentiel de la pratique concernée.

En l'espèce, le refus des opérateurs de poursuivre ou d'entamer une relation commerciale avec l'entreprise qui se prétendait victime d'une entente était fondé sur les règles mises en place par les différents acteurs du marché notamment pour lutter contre le caractère illicite de certaines pratiques, et en particulier la violation des droits de propriété intellectuelle des auteurs de films, musiques, etc.

L'Autorité de la concurrence indique que les opérateurs de cartes bancaires ont ainsi défini, à la charge des établissements adhérents (acquéreurs), des obligations de contrôle de l'activité des commerçants titulaires de contrats VAD. Elle constate que ces règles avaient pour double objet, d'une part, d'évaluer les risques liés à une relation d'affaires avec le bénéficiaire d'un contrat d'acquisition et, d'autre part, d'appliquer toute diligence nécessaire afin d'éviter l'utilisation d'une carte de paiement pour la rémunération d'activités illégales. Par ailleurs, ces règles laissaient, selon l'ADLC, une marge de manœuvre aux opérateurs quant au comportement à adopter.

Les règles mises en place par les opérateurs de carte bancaire et appliquées en aval à l'encontre de la saisissante avaient alors pour seul objectif d'éviter que les moyens de paiement ne soient utilisés à des fins illicites, et notamment pour financer une activité d'hébergement de fichiers illégale. Leur objet n'était donc pas de porter atteinte à la concurrence, mais d'appeler l'attention des établissements acquéreurs sur l'activité potentiellement contrefaisante des commerçants avec lesquels ils concluent des contrats VAD.

En conséquence, l'Autorité de la concurrence considère que les pratiques reprochées ne constituent pas des restrictions de concurrence par l'objet.

De même, l'Autorité de la concurrence rejette les arguments de la saisissante sur le prétendu effet anticoncurrentiel des pratiques.

En premier lieu, aucun lien de causalité direct ne peut être établi entre les règles des schémas quadripartites mis en place par les opérateurs de cartes bancaires et les décisions de rupture ou de refus de contracter reprochées par la saisissante. A fortiori, aucun impact sur le marché ne peut leur être imputé.

En deuxième lieu, les établissements de crédit, de paiement ou tout autre prestataire de services de paiement, étaient, pendant la période litigieuse, soumis à des contraintes et des incitations indépendantes des seules règles contractuelles, dues, notamment, à la réputation de la saisissante comme acteur majeur de téléchargements illicites de fichiers.

En troisième lieu, les pratiques mises en évidence dans la saisine ne concernant que l'entreprise saisissante, ce qui est insuffisant pour qu'un effet sensible sur la concurrence puisse en résulter sur le marché de l'acquisition, du fait de la présence d'autres clients pour les établissements concernés.

Enfin, l'Autorité de la concurrence refuse de considérer que le parallélisme de comportement des opérateurs (par la rupture des relations ou le refus de contracter à la même période) suffise à démontrer l'existence d'une entente entre eux. L'ADLC confirme ici sa pratique décisionnelle antérieure en affirmant qu'« *un parallélisme de comportement de la part de concurrents prenant des décisions autonomes, sur le fondement d'informations accessibles à tous et selon une rationalité économique propre, ne suffit pas, à lui seul, à démontrer l'existence d'une entente* ».

L'Autorité de la concurrence conclut donc à l'inexistence d'une entente anticoncurrentielle des opérateurs du marché.

A rapprocher : Décision de l'Autorité de la concurrence n°19-D-18 du 31 juillet 2019 relative à des pratiques mises en œuvre dans le secteur des moyens de paiement par carte bancaire

CONTENUS ILLICITES / E-RÉPUTATION

Contrefaçon sur internet et protection des données personnelles : le caractère licite de la collecte des données des présumés contrefacteurs est le préalable incontournable

TGI Paris, ordonnance de référé du 2 août 2019, *Mile High Distribution / Orange*

Ce qu'il faut retenir :

L'absence du caractère licite du traitement des adresses IP de présumés contrefacteurs est un empêchement légitime à la communication, par un fournisseur d'accès internet, des données permettant d'identifier les titulaires de ces adresses IP.

Pour approfondir :

Une société de production d'œuvres audiovisuelles canadienne a découvert que certaines de ses œuvres étaient disponibles sur des plateformes d'échange de fichiers en ligne sans son autorisation.

Elle a alors mandaté une société de droit allemand afin de capter des données de trafic en lien avec ses téléchargements en vue d'identifier les auteurs des téléchargements prétendument illicites.

Ces données de trafic incluent notamment l'adresse IP utilisée lors du téléchargement, la date et l'heure du téléchargement, l'intitulé de l'œuvre téléchargée ainsi que le nom du fournisseur d'accès Internet auquel se rattache l'adresse IP identifiée.

La société de production a ainsi constitué un fichier répertoriant près de 900 adresses IP qui auraient permis le téléchargement illicite d'œuvres audiovisuelles.

Par une ordonnance du 8 avril 2019, le juge des requêtes du tribunal de grande instance de Paris a ordonné à la société Orange de conserver toutes les informations qui permettraient d'identifier les titulaires des adresses IP figurant dans le fichier de la société de production. La société a ensuite fait citer devant le juge des référés la société Orange pour obtenir en urgence la communication des données d'identification.

À cette occasion, la société Orange a considéré que la mesure d'identification sollicitée ne pouvait être admissible que si la collecte réalisée des adresses IP des présumés contrefacteurs par la société de production avait elle-même été réalisée légalement.

À cet effet, la société Orange a précisé que conformément à la réglementation applicable en matière de protection des données à caractère personnel, tant la loi informatique et libertés que le Règlement Général sur la Protection des Données (RGPD), avant toute sollicitation des données d'identification, la société de production canadienne devait démontrer avoir respecté les obligations qui découlent de cette réglementation.

Le juge des référés a suivi l'argumentation de la société Orange en précisant que pour être licites, la collecte et le traitement des adresses IP par la société de production canadienne doivent avoir été opérés dans le respect des règles applicables à la protection des données à caractère personnel.

Le juge a rappelé qu'en application des articles 27, 30 et 37 du RGPD, il incombe à la société canadienne, en sa qualité de responsable de traitement établi en dehors de l'Union européenne, de désigner un représentant en Europe et de tenir à jour un registre des traitements au sein duquel une fiche du registre doit être consacrée au traitement des données des présumés contrefacteurs.

Par ailleurs, dans la mesure où les adresses IP collectées dans le contexte de la lutte contre la contrefaçon sur internet doivent être considérées comme une collecte à grande échelle de données d'infraction au sens de l'article 10 du RGPD, la société canadienne doit également désigner un délégué à la protection des données.

En outre, il appartient à la demanderesse d'assurer la sécurité des données et de garantir leur confidentialité.

A cet égard, la société de production n'a produit aucun élément démontrant sa conformité et par conséquent permettant de prouver la licéité de son traitement.

Dès lors, le juge des référés a précisé que l'absence du caractère licite du traitement constitue un empêchement légitime à la communication des données et ce, d'autant que les éléments produits par la société de production sont insuffisants à démontrer l'existence des œuvres litigieuses ainsi que la titularité des droits d'exploitation invoqués sur ces œuvres.

Pour ces raisons, la société canadienne a été déboutée de l'ensemble de ses demandes.

A rapprocher : Articles 27, 30 et 37 du RGPD ; Article 145 du Code de procédure civile

INTERNATIONAL

Transferts de données internationaux : quelles seront les conséquences du Brexit ?

Actualité

Ce qu'il faut retenir :

En cas de Brexit sans accord, les transferts de données personnelles vers le Royaume-Uni seront considérés comme des transferts vers un État n'offrant pas de niveau de protection adéquat (à défaut d'une décision d'adéquation prise par la Commission européenne).

Pour approfondir :

Le 23 juin 2016 a eu lieu le référendum sur l'appartenance du Royaume-Uni à l'Union européenne.

Les citoyens résidents du Royaume-Uni ont voté à 51,89 % pour que le Royaume-Uni quitte l'Union européenne.

Le gouvernement britannique a alors enclenché le Brexit.

Alors que la sortie du Royaume-Uni était initialement prévue le 29 mars 2019, cette date a été reportée au 31 octobre prochain.

Toutefois, aucun accord n'a pour l'instant été trouvé entre l'État sortant et l'Union européenne.

En cas de Brexit sans accord, les transferts de données personnelles vers le Royaume-Uni seront considérés comme des transferts vers un État n'offrant pas de niveau de protection adéquat (à défaut d'une décision d'adéquation prise par la Commission européenne).

Des lors, quelle est la marche à suivre pour les responsables de traitements et sous-traitants opérant de tels transferts ?

Tous les traitements et transferts de données vers le Royaume-Uni qui se poursuivront à compter du 1er novembre 2019, devront être assortis de garanties et encadrés par l'un des outils prévus par le Règlement Général sur la Protection des Données personnelles (RGPD).

Ainsi, l'entité émettrice des données depuis le territoire de l'UE devra signer des clauses contractuelles types avec l'entité destinataire au Royaume-Uni ou adopter des règles contraignantes d'entreprise (BCR) ou des codes de conduite / mécanismes de certifications.

A défaut d'un tel encadrement, les responsables de traitement et sous-traitants s'exposeront à des sanctions pouvant atteindre 20 000 000 € ou 4 % de leur chiffre d'affaires.

L'article 49 du RGPD prévoit néanmoins quelques exceptions permettant des transferts de données vers un territoire situé en dehors de l'UE en l'absence de décision d'adéquation ou de garanties.

Ces exceptions sont en revanche à interpréter de manière stricte comme le rappelle la CNIL et les opérateurs ne pourront y recourir que de manière ponctuelle.

Parmi ces exceptions, le consentement des personnes concernées pourrait permettre le transfert de données. En revanche, les personnes devront préalablement être informées des risques que le transfert pourrait comporter en raison de l'absence de décision d'adéquation et de garantie appropriées.

Par ailleurs, outre cet encadrement, les opérateurs réalisant des transferts devront mettre à jour leur registre des traitements pour y renseigner ces transferts de données hors UE.

Ils devront également procéder à une nouvelle information des personnes concernées afin de leur notifier l'existence de ces transferts.

Enfin, s'agissant des transferts de données en provenance du Royaume-Uni, ces derniers pourront se poursuivre sans garantie supplémentaire, le gouvernement britannique ayant annoncé que la libre circulation des données vers l'Union européenne serait permise.

A rapprocher : *Brexit*, Lettre des Réseaux, 16 sept. 2016

***

ACTUALITÉ NUMÉRIQUE SIMON ASSOCIÉS

ÉVÉNEMENTS

Données dans un réseau : comment les collecter, les utiliser et les céder

Atelier animé par SANDRINE RICHARD et FRANÇOIS-LUC SIMON
lors du **Congrès de la Franchise et des Réseaux**
25 septembre 2019 – Paris

En savoir plus et s'inscrire

Le droit sur le logiciel à l'heure du numérique ou comment protéger ses créations

Petit-déjeuner organisé par SIMON ASSOCIES et l'Agence de Protection des Programmes (APP),
et animé par FABRICE DEGROOTE et PAULINE PUELL
8 octobre 2019 – Paris

En savoir plus et s'inscrire