SOMMAIRE

DATA / DONNÉES PERSONNELLES	
La mise en conformité avec le RGPD des PME Guide de la CNIL et de BPI France du 17 avril 2018	p. 2
Suppression d'une fiche Google My Business TGI Paris, Ord. Réf., 6 avr. 2018	p. 3
Partage de responsabilité entre acteurs d'un traitement de données personnelles : l'article 82 du RGPD Article 82 du Règlement Général sur la Protection des Données	p. 4
PROPRIÉTÉ INTELLECTUELLE	
Conformité des marques à l'ordre public TPIUE, 15 mars 2018, aff.T-1/17	p. 7
Protection de l'aménagement intérieur d'un point de vente CA Douai, 5 avril 2018, RG n°17/03809	p. 8
Bases de données, logiciels et droit d'auteur CA Aix-en-Provence, 19 avril 2018, RG n°15/14362	p. 9
SERVICES NUMÉRIQUES	
Victime d'hameçonnage : la Cour de cassation impose à l'utilisateur une vigilance de plus en plus accrue Cass. com., 28 mars 2018, n°16-20.018	p. 9
E-COMMERCE	
La publicité en ligne sous la surveillance de l'Autorité de la concurrence Adlc, avis n°2018-A-03 du 6 mars 2018	p. 11
CONTENUS ILLICITES / E-RÉPUTATION	
Avis critique sur internet, par principe non-fautif, sauf intention de nuire CA Dijon, 1ère Ch. civ., 20 mars 2018, n°15/02004	p. 12
INTERNATIONAL	
Action individuelle d'un consommateur et cessions de droits CJUE, 25 janvier 2018, aff. C-498/16	p. 13
LEGALTECHS / TENDANCES	
La promotion de l'Intelligence Artificielle par la Commission européenne Communiqué de presse du 25 avril 2018	p. 14
ACTUALITÉ NUMÉRIQUE SIMON ASSOCIÉS	p. 16

PARIS - NANTES
MONTPELLIER - LYON
FORT-DE-FRANCE

Bureaux intégrés

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

Réseau SIMON Avocats

ALGÉRIE - ARMÉNIE
AZERBAÏDJAN - BAHREÏN
BELGIQUE - BRÉSIL
BULGARIE - CAMEROUN
CHILI - CHINE - CHYPRE
COLOMBIE - COREE DU SUD
CÔTE D'IVOIRE - ÉGYPTE
ÉMIRATS ARABES UNIS
ESTONIE - ÉTATS-UNIS
HONGRIE - ÎLE MAURICE
INDE - INDONÉSIE - IRAN
ITALIE - LUXEMBOURG
MAROC - OMAN
PARAGUAY - PÉROU
PORTUGAL - RD CONGO
SENEGAL - THAÏLANDE
TUNISIE

Conventions transnationales

www.simonassocies.com
www.lettredunumerique.com

DATA / DONNÉES PERSONNELLES

La mise en conformité avec le RGPD des PME
Guide de la CNIL et de BPI France du 17 avril 2018

Ce qu'il faut retenir :

A moins d'un mois avant l'entrée en application du RGPD, de nombreuses entreprises n'ont pas encore entamé leurs démarches de mises en conformité. Si ce texte n'est pas inédit en tout point, ce sont les sanctions qu'il introduit qui sont révolutionnaires.

Consciente des difficultés que peuvent rencontrer les entreprises dans leurs démarches, la CNIL a édité une méthodologie présentée en six étapes leur permettant d'appréhender concrètement les actions de mise en conformité à mettre en place. Malgré tout, les PME qui ne disposent ni d'un budget dédié pour une mise en conformité dans les meilleures conditions, ni de moyens humains adéquats n'ont su comment mettre en application la méthodologie de la CNIL. La Commission a alors voulu tenir compte des particularités de ces structures en adoptant un guide, rédigé en partenariat avec Bpifrance, dédié aux PME.

Ce guide était ainsi très attendu.

Pour approfondir :

1. **Présentation du guide : une compréhension du texte facilitée et des avantages motivant**

Le guide de la CNIL et de Bpifrance propose tout d'abord une présentation du règlement dans termes simplifiés et vulgarisés. Cela a pour mérite de favoriser la compréhension du texte par des personnes non initiées.

Il présente également les avantages de la mise en conformité pour les entreprises. Ainsi, les rédacteurs mettent en avant le fait que l'arrivée du règlement européen est une occasion de construire une relation de confiance avec les clients et d'améliorer son image de marque.

En étant transparent sur les activités de l'entreprise et en garantissant le respect des droits des personnes concernées, la relation entre un responsable de traitement et une personne concernée est ainsi plus fluide et rassurante.

La constitution d'un fichier de clients et prospect à jour permet également de gagner en efficacité et en productivité souligne la CNIL et Bpifrance.

Cela a aussi pour avantage d'éviter de conserver des données périmées ou inutiles, demandant des moyens techniques et humains de plus en plus importants pour gérer cette accumulation d'informations.

Le respect des principes du RGPD permet ainsi de réduire les coûts liés à la gestion des données et d'optimiser les investissements des entreprises.

La sécurité des données est également un point essentiel qui permet à toute entreprise de se développer sereinement.

En matière de sous-traitance, les donneurs d'ordre rechercheront avant tout des prestataires en conformité avec le règlement. La mise en conformité offre donc un avantage concurrentiel d'importance pour les prestataires qui respectent le texte.

Enfin, le guide rappelle que l'introduction de nouveaux concepts par le RGPD peut être une véritable opportunité pour les entreprises de créer de nouveaux services et produits susceptibles de motiver la décision d'achat.

2. **Les actions à mener pour la mise en conformité**

La CNIL et Bpifrance présentent une nouvelle méthodologie adaptée aux PME, non plus en 6 étapes mais en 4 étapes.

Deux étapes sont donc supprimées, ce qui simplifie la méthodologie pour ces entreprises modestes. En premier lieu, la CNIL présente l'obligation de tenir un registre des traitements.
Pour ce faire, il est recommandé de recenser les activités principales et d'en identifier les principales caractéristiques que sont la finalité, les catégories de données, les destinataires des données et leur durée de conservation.

En second lieu, il est recommandé aux entreprises de procéder à un tri de leurs données. Il s'agit ici de respecter les principes de minimisation, de définir les habilitations des membres du personnel, de fixer une durée de conservation, de s'interroger sur la pertinence des données et de détecter l'existence de données sensibles.

Pour la troisième étape des actions à suivre, l'autorité de contrôle rappelle l'importance de respecter les droits des personnes concernées, en intégrant les mentions d'information et en prévoyant un processus pour recevoir les demandes des dites personnes.

Enfin, le guide rappelle qu'il est essentiel de sécuriser les données à l'aide de mesures techniques et organisationnelles appropriées.

La désignation du délégué à la protection des données (DPO) ainsi que les obligations tenant à la documentation de sa conformité ne semblent donc plus au programme des étapes à suivre par les PME.

En effet, le délégué à la protection des données est un des grands absents de ce guide. Il n'est mentionné que de façon anecdotique, en précisant les critères de sa désignation. Cette référence, bien que succincte, rappelle donc que la désignation d'un DPO n'est pas à exclure pour les PME.

Nous ne pouvons que regretter le fait que le guide n'oriente pas les PME face aux problématiques qu'elles peuvent rencontrer pour une telle désignation.

En effet, ces entreprises ne disposent généralement pas des ressources financières suffisantes pour faire appel à un DPO externalisé, dont les tarifs sont souvent élevés. Quand bien même les entreprises choisiraient de désigner un DPO en interne, elles ne sauraient pas qui désigner sans encourir un risque de conflit d'intérêt. Certaines PME n'ont parfois même aucun salarié qui pourrait endosser ce rôle. Sur ce point, le guide n'apporte aucune réponse.

En outre, l'étape consacrée aux mesures de sécurité est insuffisante. La CNIL et Bpifrance ne voient le problème que sous l'angle du responsable du traitement, risquant d'occulter les nombreuses PME agissant comme sous-traitants, et se contentent principalement d'ériger en premier réflexe de sécurité le principe de minimisation des données. La réalité est pourtant bien plus exigeante. Les PME ne disposent pas d'autant de moyens de se mettre à niveau que les entreprises plus importantes.

Enfin, il aurait été souhaitable que le guide propose des instruments spécifiques à destination des PME, tels que des modèles de mentions d'information adaptés aux PME ou encore un registre pré-rempli avec les traitements les plus communs.

Pour autant, la CNIL reste un bon partenaire dans ses démarches de mise en conformité et de nombreux modèles et guides généraux sont présents sur son site internet.

A rapprocher : Guide pratique de sensibilisation au RGPD pour les PME de la CNIL et BPI France

---

Suppression d'une fiche Google My Business
TGI Paris, Ord. Réf., 6 avril 2018

Ce qu'il faut retenir :

Un traitement de données à caractère personnel concernant une personne physique et répondant à des fins de prospection, malgré l'opposition de cette personne, est constitutif d'une infraction pénale.

Pour approfondir :

En effectuant une saisie de son nom et de son prénom sur le moteur de recherche Google.fr, un chirurgien-dentiste a pu prendre connaissance de l'existence d'une fiche *Google My Business* relative à son activité professionnelle, indiquant ses coordonnées et horaires d'ouverture ainsi que des avis d'internautes.

L'existence de cette fiche, outre la présentation de l'activité du chirurgien, impliquait notamment l'envoi par Google de courriels à des fins de prospection commerciale.

Le professionnel a alors formalisé une demande de suppression de cette fiche auprès de Google France et Google Inc.

Google ayant refusé de faire droit à sa demande, le professionnel l'a assigné devant le Tribunal de Grande Instance de Paris, aux fins de faire supprimer la fiche litigieuse et 3 avis qu'il considère comme ayant un caractère manifestement illicite.

L'action du professionnel était fondée sur les dispositions de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, (ci-après *loi informatique et libertés*) laquelle prévoit que seul un responsable de traitement (à savoir celui qui détermine les finalités et moyens de traitement), ne répond aux manquements aux dispositions de cette loi et ne peut engager sa responsabilité.

Dans la mesure où les conditions d'utilisation de Google précisent que *« les services sont fournis par la société Google LLC. sise au 1600 Amphitheatre Parkway, Mountain View, CA 94043, Etats-Unis »* et que la fiche *« nous contacter »* mentionne cette même adresse du siège social de Google Inc., (désormais Google LLC), le tribunal a considéré aucune preuve ne permettait d'établir l'intervention et la responsabilité de la société Google France dans ce traitement de données. Dès lors, le tribunal a prononcé la mise hors de cause de la société Google France.

La société Google LLC a a alors tenté de soustraire le traitement de données réalisé via les fiches *Google My Business* aux dispositions de la loi informatique et libertés en soutenant que la notion de donnée à caractère personnel, tel qu'elle est appréhendée par la loi, était restreinte aux seules informations relatives à la vie privée. Partant, Google LLC a considéré que la demande du professionnel, dès lors qu'elle était relative à un traitement de données d'ordre professionnel échappé à la loi informatique et libertés.

Le tribunal a retenu une lecture de la notion de donnée personnelle stricte et fidèle à la loi. Ainsi, le TGI a pu rappeler que la notion couvrait tous les éléments permettant d'identifier une personne physique et que « *la circonstance que de telles données soient relatives, comme en l'espèce, à l'activité professionnelle de la personne en question est donc sans incidence sur cette qualification, dès lors qu'elle est désignée ou rendue identifiable* ».

En considération des articles 226-18-1 et 226-24 du Code pénal – lesquels prévoit que le fait de procéder à un traitement de données à caractère personnel malgré l'opposition de la personne concernée, lorsque ce traitement répond à des fins de prospection est passible d'emprisonnement, d'amendes ainsi que des peines prévues par les 2° à 5° et 7° à 9° de l'article 131-39.

En l'espèce, le TGI a considéré que le traitement des données du chirurgien dans le cadre de sa fiche professionnel constituait un trouble manifestement illicite qu'il y a lieu de faire cesser, dans la mesure où s'il avait bien accepté l'existence de sa fiche après sa création, il en a par la suite demandé la suppression.

La suppression de la fiche du chirurgien a donc été ordonnée par le TGI sous astreinte de 1000 euros par jour de retard. La société Google LLC. a également été condamnée à verser au demandeur une somme de 3.500 euros en application des dispositions de l'article 700 du Code de procédure civile.

A rapprocher : Article 2 Loi du 6 janvier 1978 ; Article 226-18-1 et 226-24 du Code pénal

---

Partage de responsabilité entre acteurs d'un traitement de données personnelles : l'article 82 du RGPD

Article 82 du Règlement Général sur la Protection des Données

Ce qu'il faut retenir :

L'article 23 de la Directive 95/46/CE sur la protection des données personnelles (abrogé par le RGPD) prévoyait le droit d'obtenir du responsable du traitement – et de lui seul – la réparation du préjudice subi par toute personne du fait d'un traitement illicite ou de toute action incompatible avec les dispositions nationales prises en application de cette Directive. En droit français, aucune disposition spécifique n'avait été insérée dans la LIL, de sorte que le droit commun était seul applicable. L'article 82 du RGPD confirme le principe du droit à réparation issu de la Directive 95/46/CE (non transposée en droit français) et le précise en 6 paragraphes, fixant ainsi les principes directeurs gouvernant désormais la réparation du préjudice subi par toute personne résultant d'une violation du Règlement.

Pour approfondir :

Article 82, §.1 du RGPD :

Texte : *« Toute personne ayant subi un dommage matériel ou moral du fait d'une violation du présent règlement a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi ».*

Commentaire : Pour ce qui concerne la nature du dommage subi, le texte « ratisse large » en visant tout « dommage matériel ou moral ». La Directive 95/46/CE visait le seul dommage. Le fait que le « dommage matériel ou moral » ouvre droit à réparation va sans dire, mais va sans doute mieux en le disant.

Pour ce qui concerne l'auteur du dommage, il est précisé que la réparation peut être obtenue du « responsable du traitement » **ou** – et c'est là une nouveauté – du « sous-traitant ». Le §.1 vise la conjonction de coordination « ou », mais il faut lire « et/ou » ainsi que cela ressort de la lecture des paragraphes suivants.

Article 82, §.2 du RGPD :

Texte : *« Tout responsable du traitement ayant participé au traitement est responsable du dommage causé par le traitement qui constitue une violation du présent règlement. Un sous-traitant n'est tenu pour responsable du dommage causé par le traitement que s'il n'a pas respecté les obligations prévues par le présent règlement qui incombent spécifiquement aux sous-traitants ou qu'il a agi en-dehors des instructions licites du responsable du traitement ou contrairement à celles-ci ».*

Commentaire : Le critère de mise en œuvre de la responsabilité propre au responsable du traitement est sa « participation » au « traitement ». Le terme de « traitement », lui, est défini (très largement) à l'article 4 du Règlement : *« toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction »*. Il semble difficile de faire plus large. Le terme de « participation » n'est en revanche pas défini, pas plus qu'est définie la nature même de cette participation. L'action de « participer » revient à « prendre part », ce qui incite à retenir une acception large de la notion. Il paraît d'ailleurs raisonnable de considérer que cette « participation » se traduise par la réalisation d'un acte matériel accompli soit par le responsable du traitement lui-même (participation directe), soit par le sous-traitant, sur instruction du responsable du traitement (participation indirecte). C'est dire que le critère de mise en œuvre de la responsabilité propre au responsable du traitement présente un caractère « quasi-automatique ».

Le critère de mise en œuvre de la responsabilité propre au sous-traitant est tout autre. Tout d'abord, dans l'esprit du texte, et au contraire de ce qui vient d'être indiqué à propos du responsable du traitement, cette responsabilité ne présente aucun caractère d'automaticité, ainsi que le souligne la formulation du texte : « *Un sous-traitant n'est tenu pour responsable du dommage causé par le traitement que (…)* ». Ensuite, le texte énonce deux cas, présentés comme ayant un caractère « limitatif », dont le point commun est l'existence d'une violation par le sous-traitant, la première au Règlement *(« s'il n'a pas respecté les obligations prévues par le présent règlement qui incombent spécifiquement aux sous-traitants »*), la seconde au regard des instructions du responsable du traitement (*« s'il a agi en-dehors des instructions licites du responsable du traitement ou contrairement à celles-ci »*). On entrevoit ici l'importance que revêt le contrat conclu entre le responsable du traitement et le sous-traitant au regard des conditions de mise en œuvre de la responsabilité propre au sous-traitant.

Article 82, §.3 du RGPD :

Texte : *« Un responsable du traitement ou un sous-traitant est exonéré de responsabilité, au titre du paragraphe 2, s'il prouve que le fait qui a provoqué le dommage ne lui est nullement imputable ».*

Commentaire : Ce texte énonce un principe d'exonération applicable au bénéfice des deux acteurs (responsable du traitement et sous-traitant), chacun en ce qui les concerne ; ce faisant, ce texte rappelle une évidence : la responsabilité du responsable du traitement ou du sous-traitant nécessite l'imputabilité personnelle d'un fait ayant provoqué le dommage. Il suffit donc que le fait qui a provoqué le dommage ne leur soit pas imputable. Toutefois, le texte fait peser sur chacun d'eux l'obligation de prouver l'absence d'imputabilité personnelle du fait ayant provoqué le dommage. On entrevoit encore ici l'importance que le contrat conclu entre le responsable du traitement et le sous-traitant aura pour permettre à ces acteurs de rapporter la preuve qui leur incombe au titre du §.3.

Article 82, §.4 du RGPD :

Texte : *« Lorsque plusieurs responsables du traitement ou sous-traitants ou lorsque, à la fois, un responsable du traitement et un sous-traitant participent au même traitement et, lorsque, au titre des paragraphes 2 et 3, ils sont responsables d'un dommage causé par le traitement, chacun des responsables du traitement ou des sous-traitants est tenu responsable du dommage dans sa totalité afin de garantir à la personne concernée une réparation effective ».*

Commentaire : Ce texte institue un principe de responsabilité solidaire du (ou des) responsable(s) du traitement et/ou du (ou des) sous-traitant(s) intervenant dans le même traitement. Toutefois, cette solidarité n'a rien d'automatique ; elle implique que le(s) responsable(s) du traitement et/ou sous-traitant(s) qui participent au même traitement puissent chacun être tenus responsables d'un dommage causé par le traitement en vertu des § 2 et 3. Dans ce cas, chacun d'eux – le(s) responsable(s) du traitement et/ou le(s) sous-traitant(s) – est alors tenu responsable du dommage dans sa totalité, afin de mieux garantir une compensation effective à la victime.

Article 82, §.5 du RGPD :

Texte : *« Lorsqu'un responsable du traitement ou un sous-traitant a, conformément au paragraphe 4, réparé totalement le dommage subi, il est en droit de réclamer auprès des autres responsables du traitement ou sous-traitants ayant participé au même traitement la part de la réparation correspondant à leur part de responsabilité dans le dommage, conformément aux conditions fixées au paragraphe 2 ».*

Commentaire : A la différence des quatre premiers paragraphes, ce texte concerne les rapports entre le responsable du traitement et le sous-traitant, en envisageant la possibilité d'une action récursoire, corolaire du principe de solidarité institué au paragraphe 4. Ici encore, le contrat conclu entre le responsable du traitement et le sous-traitant pourra aménager les conditions de cette action récursoire.

Article 82, §.6 du RGPD :

Texte : *« Les actions judiciaires engagées pour exercer le droit à obtenir réparation sont intentées devant les juridictions compétentes en vertu du droit de l'État membre visé à l'article 79, paragraphe 2 ».*

Commentaire : Toute personne concernée a droit à un recours juridictionnel effectif si elle considère que les droits que lui confère le Règlement ont été violés du fait d'un traitement de ses données à caractère personnel effectué en violation du Règlement. Le choix de la juridiction compétente est large car les critères de sa détermination sont alternatifs.

En effet, l'article 79, §. 2 retient tout d'abord que *« Toute action contre un responsable du traitement ou un sous-traitant est intentée devant les juridictions de l'État membre dans lequel le responsable du traitement ou le sous-traitant dispose d'un établissement ».*

Puis, l'article 79, §. 2 retient ensuite qu' *« une telle action peut aussi être intentée devant les juridictions de l'État membre dans lequel la personne concernée a sa résidence habituelle, sauf si le responsable du traitement ou le sous-traitant est une autorité publique d'un État membre agissant dans l'exercice de ses prérogatives de puissance publique ».*

Toute personne concernée a le droit d'introduire une réclamation auprès d'une autorité de contrôle, en particulier dans l'État membre dans lequel se trouve sa résidence habituelle, son lieu de travail ou le lieu où la violation aurait été commise, si elle considère que le traitement de données à caractère personnel la concernant constitue une violation du présent règlement (Règlement, article 77), ce qui conduit à envisager l'article 83 du Règlement, relatif aux conditions de mise en œuvre des amendes administratives.

A rapprocher : Article 23 de la Directive 95/46/CE sur la protection des données personnelles

PROPRIÉTÉ INTELLECTUELLE

Conformité des marques à l'ordre public
TPIUE, 15 mars 2018, aff.T-1/17

Ce qu'il faut retenir :

La conformité à l'ordre public et aux bonnes mœurs est une condition de validité des marques. La marque « *La Mafia se sienta à la mesa* » est donc annulée compte tenu de la mention du nom de l'organisation criminelle.

Pour approfondir :

La conformité à l'ordre public du signe choisi comme marque est une condition de validité tant en France qu'au niveau européen. La rareté des décisions ayant à se prononcer sur ce sujet confère un intérêt tout particulier à cette décision.
L'affaire portait sur une marque communautaire semi-figurative représentant une rose sur fond noir et le texte « *La Mafia se sienta a la mesa* » pour désigner des produits et services relevant des classes 25, 35, et 43.

Une demande de nullité avait été formée par la République italienne à l'encontre de cette marque aux motifs de la violation de l'article 7.1 f) du Règlement n°207/2009 du 29 février 2009, ainsi rédigé : « *Sont refusés à l'enregistrement (…) les marques qui sont contraires à l'ordre public ou aux bonnes mœurs* ».

Le Tribunal va confirmer la nullité de cette marque.

Une partie de la décision s'attache à définir le public qui doit être pris en référence. Le point 28 de la décision est sur ce point particulièrement éclairant : « *Il doit également être rappelé que le public pertinent situé sur le territoire de l'Union est, par définition, situé sur le territoire d'un État membre et que les signes susceptibles d'être perçus comme contraires à l'ordre public ou aux bonnes mœurs ne sont pas les mêmes dans tous les États membres, notamment pour des raisons linguistiques, historiques, sociales ou culturelles* » et 29 : « *Il s'ensuit que, pour l'application du motif absolu de refus prévu à l'article 7, paragraphe 1, sous f), du règlement n° 207/2009, il convient de prendre en considération aussi bien les circonstances communes à l'ensemble des États membres de l'Union que les circonstances particulières à des États membres pris individuellement qui sont susceptibles d'influencer la perception du public pertinent situé sur le territoire de ces États* ».

Le Tribunal détermine ensuite l'élément dominant de la marque et juge à cet égard que la dénomination « la mafia » occupe la position centrale. Puis, pour conclure au fait que l'enregistrement d'un signe comportant cette dénomination est contraire à l'ordre public, le Tribunal considère que ce signe est : « *mondialement compris comme renvoyant à une organisation criminelle ayant ses origines en Italie et dont les activités se sont étendues à d'autres États (…)* », « *… que cette organisation criminelle a recours à l'intimidation, à la violence physique et au meurtre afin de mener à bien ses activités, qui incluent notamment le trafic illicite de drogues, le trafic illicite d'armes, le blanchiment d'argent et la corruption* » et « *que de telles activités criminelles violent les valeurs mêmes sur lesquelles l'Union est fondée, en particulier les valeurs de respect de la dignité humaine et de liberté* ».

Aussi, la marque contestée, envisagée dans son ensemble :

- renvoie à une organisation criminelle, donne une image globalement positive de cette organisation et, ainsi, banalise les atteintes graves portées par ladite organisation aux valeurs fondamentales de l'Union,

- est ainsi de nature à choquer ou à offenser non seulement les victimes de cette organisation criminelle et leurs familles, mais également toute personne qui, sur le territoire de l'Union, est mise en présence de ladite marque et possède des seuils moyens de sensibilité et de tolérance.

La marque « La mafia *se sienta à la mesa* » est donc jugée contraire à l'ordre public, au sens de l'article 7, paragraphe 1, sous f), du règlement n° 207/2009, et déclarée nulle

A rapprocher : Règlement (CE) n°207/2009 du 29 février 2009 sur la marque communautaire (devenu Règlement (UE) n°2017/1001 du 14 juin 2017)

Protection de l'aménagement intérieur d'un point de vente

CA Douai, 5 avr. 2018, RG n°17/03809

Ce qu'il faut retenir :

L'architecture intérieure d'un point de vente peut être jugée comme une œuvre objet de droit d'auteur à condition que l'originalité - condition sine qua non de la reconnaissance de droit d'auteur - soit démontrée. L'arrêt commenté revient sur cette condition.

Pour approfondir :

L'affaire opposait l'ancien franchisé d'un réseau de salons de coiffure et le franchiseur en raison de la rupture unilatérale du contrat de franchise par le franchisé et les conséquences de sa sortie du réseau. En particulier, le franchiseur lui reprochait de ne pas avoir apporté de modifications dans l'aménagement de son point de vente lequel maintenait, à son sens, les caractéristiques d'un point de vente du réseau.

La demande du franchiseur consistait donc à faire juger que l'aménagement intérieur des salons de coiffure du réseau devait être considéré comme une œuvre architecturale protégée par le droit d'auteur en application de l'article L112-2 du code de la propriété intellectuelle et, en conséquence, que l'exploitation de cet aménagement (postérieurement à la cessation du contrat de franchise) constituait un acte de contrefaçon. Le franchiseur sollicitait donc la cessation de ces agissements et la modification de l'aménagement intérieur du salon litigieux ainsi que l'allocation de dommages-intérêts pour réparer son préjudice (54.000 euros).

La Cour d'appel a recherché, en premier lieu, si l'aménagement intérieur pouvait être envisagée comme une œuvre donc objet de droit d'auteur. Les juges vont répondre positivement au terme d'un examen détaillé, au cours duquel ils relèvent que l'espace de vente est « *conçu comme une scène de théâtre, se dessinant en courbe, avec une segmentation en plusieurs espaces distincts dont les caractéristiques essentielles sont les suivantes : une entrée la plus vaste et la plus ouverte possible, un espace caisse avec une caisse proche du vestiaire et du mail, de forme courbe, avec à proximité un téléviseur (…), un espace vente, situé de l'autre côté de la caisse, sous forme de linéaire de distribution des produits à la vente, un corps de salon également conçu avec une courbe généreuse par juxtaposition des espaces de coiffage et des miroirs, un espace labo soit fermé conçu comme une tour, soit ouvert tel un bar à colorations, donnant à voir aux clients le travail de préparation, les bacs étant placés en rayonnement autour du labo, un espace shampoing en rayonnement autour du laboratoire, situé face à l'espace de coiffage, permettant une circulation totale entre les bacs à shampoing et maintenant le client en spectateur de la coiffure, un espace coiffure aménagé en fonction du bâti, avec des postes de coiffage, placé selon une courbe* ».

La Cour ajoute que sont associés à ces éléments « *selon les prescriptions du franchiseur, les formes douces du logo, reproduit en petites touches sur tous les éléments, la couleur rouge qui constitue la couleur caractéristiques de la marque se retrouve sur tous les accessoires et encore imposés : le stylisme des photos avec un cadrage spécifique des mannequins photographiés, la forme, les couleurs et le positionnement des meubles, les matériaux mis en œuvre, leurs textures, leurs couleurs, etc.* »

Tous ces éléments permettent à la Cour d'en conclure que « *les éléments pris dans leur ensemble révèlent un travail de création, un parti pris esthétique, empreint de la personnalité de l'auteur, qui n'est pas dicté par des contraintes fonctionnelles et donne au salon de coiffure, de type Shampoo, une physionomie propre, différente de celle des salons d'enseignes concurrentes, et donc protégeable comme œuvre de l'esprit* ».

La motivation de cette décision est particulièrement circonstanciée : cela tient au fait que l'originalité d'une œuvre doit être examinée au cas par cas, pour chaque type d'œuvre, les juges devant justifier de ce qui porte l'empreinte de la personnalité de l'auteur.

Dans un second temps, la Cour s'est attachée à rechercher si, l'ancien franchisé, avait commis les actes de contrefaçon qui lui étaient reprochés. La conclusion négative tient, probablement, de l'insuffisance des preuves rapportées : les juges soulignent ici que les procès-verbaux d'huissier qui lui sont soumis comportent des photographies prises de l'extérieur et « *… à travers une vitrine aux effets réfléchissants, ne lui permettent toujours pas d'apprécier, dans les locaux incriminés, la présence de la combinaison d'éléments caractérisant l'originalité de l'agencement et de la décoration intérieure de l'espace* ».

Le franchiseur aurait probablement dû obtenir, avant d'engager son action, l'autorisation d'accéder à l'intérieur du point de vente pour faire procéder aux constations utiles.

A rapprocher : Article L.112-2 du code de la propriété intellectuelle

---

Bases de données, logiciels et droit d'auteur
CA Aix-en-Provence, 19 avril 2018, RG n°15/14362

Ce qu'il faut retenir :

Les bases de données et les logiciels font l'objet de droit d'auteur si la preuve de leur originalité est rapportée.

Pour approfondir :

Les bases de données sont appréhendées par le droit de la propriété intellectuelle qui :

- reconnaît que celles-ci peuvent être considérées comme des œuvres de l'esprit, objets de droit d'auteur (**article L.112-3 du Code de la propriété intellectuelle**),
- en donne une définition (alinéa 2) comme suit : « *un recueil d'œuvres, de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodique, et individuellement accessibles par des moyens électroniques ou par tout autre moyen* »,
- et organise un régime spécifique (**article L.341-1 du Code de la propriété intellectuelle**) conférant au producteur d'une base de données, entendu comme la personne qui prend l'initiative et le risque des investissements correspondants, un droit *sui generis* lui conférant une protection – indépendante du droit d'auteur sur la base de données et du contenu de la base – du contenu de la base lorsque la constitution, la vérification ou la présentation de celui-ci atteste d'un investissement financier, matériel ou humain substantiel.

Les logiciels sont également spécifiquement visés à l'article **L.112-2 du Code de la propriété intellectuelle** comme des œuvres de l'esprit.

Dans cette affaire, une société ayant participé à un appel d'offres quelques années plus tôt, agissait en contrefaçon en raison d'un nouvel appel d'offre à l'occasion duquel la base de données et le logiciel qu'elle avait réalisés et fournis avaient été utilisés. En particulier, elle contestait avoir cédé ses droits d'auteur sur ces éléments et considérait qu'elle n'avait consenti qu'une concession temporaire du droit de les utiliser.

La Cour va rejeter l'action aux motifs que la preuve d'un investissement substantiel permettant de bénéficier d'un droit *sui generis* n'était pas rapportée, ni celle de l'originalité de la base et du logiciel. Il est ici essentiel de rappeler que, nonobstant leur nature particulière, une base de données ou un logiciel ne fait l'objet de droit d'auteur qu'à la condition qu'ils soient originaux, condition commune à toutes les créations. La Cour considère, au surplus, que la cession des droits était prévue dans la documentation contractuelle dont avait connaissance la société ayant participé à l'appel d'offre.

Si le droit de la propriété intellectuelle peut s'appliquer aux œuvres telles que les bases de données et les logiciels, c'est à la condition qu'ils soient originaux, preuve que le demandeur à une action en contrefaçon doit rapporter.

A rapprocher : L.112-2 du Code de la propriété intellectuelle ; L.112-3 du Code de la propriété intellectuelle ; L.341-1 du Code de la propriété intellectuelle

---

SERVICES NUMÉRIQUES

Victime d'hameçonnage : la Cour de cassation impose à l'utilisateur une vigilance de plus en plus accrue
Cass. com., 28 mars 2018, n°16-20.018

Ce qu'il faut retenir :

La Cour de cassation renforce à nouveau l'obligation de prudence pesant sur l'internaute victime d'hameçonnage, dans la droite lignée de sa jurisprudence actuelle.

Elle a jugé, dans un arrêt du 28 mars 2018, au visa des articles L.133-16 et L.133-19 du Code monétaire et financier que « *manque par négligence grave, à son obligation de prendre toute mesure raisonnable pour préserver la sécurité de ses dispositifs de sécurité personnalisés, l'utilisateur d'un service de paiement qui communique les données personnelles de ce dispositif de sécurité en réponse à un courriel qui contient des indices permettant à un utilisateur normalement attentif de douter de sa provenance, peu important qu'il soit, ou non, avisé des risques d'hameçonnage*. »

Pour approfondir :

La Cour de cassation a, par cette décision, annulé l'arrêt de la Cour d'appel d'Amiens en date du 19 avril 2016, qui avait condamné l'établissement de crédit à rembourser les sommes indument prélevées sur le compte d'un de ses clients, victime de **phishing**, soit 2 731,98 € au titre des paiements frauduleux réalisés par carte bancaire, et 4 500 € au titre d'un virement litigieux débité de son livret. La Cour de cassation a retenu la négligence grave du client, victime d'une opération d'**hameçonnage**, pour faire échec à l'obligation de garantie de la banque.

Elle a également rappelé le principe selon lequel c'est à l'établissement de crédit de rapporter la preuve de cette éventuelle négligence grave, laquelle ne peut se déduire du seul fait que l'instrument de paiement ou les données personnelles qui lui sont liées ont été utilisés.

Dans les faits, le client d'une banque, victime de phishing consistant en l'envoi de mails successifs frauduleux portant le logo parfaitement imité dudit établissement de crédit, avait consciencieusement et bien naïvement renseigné ses coordonnées bancaires. Des prélèvements frauduleux étaient ensuite intervenus sur ses comptes, dont il avait sollicité le remboursement au titre de l'obligation de garantie de la banque.

Cette dernière, pour s'y opposer, se fondait sur la combinaison des articles L.133-16 et L.133-19 du Code monétaire et financier, qui dispose en son dernier alinéa : « *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]* ».

La banque, devant la Cour d'appel, avait reconnu que « *seul un examen vigilant des adresses internet changeantes du correspondant ou certains indices, comme les fautes d'orthographe, sont de nature à interpeler le client* ». En outre, il était constaté que le client ne se connectait quasiment jamais au site internet de la banque, de telle sorte qu'il n'avait pas été avisé des messages d'alerte relatifs au délit d'hameçonnage. La Cour d'appel d'Amiens avait donc considéré que la preuve de la négligence grave de l'utilisateur n'était pas rapportée, et condamné la banque à rembourser les montants frauduleusement prélevés sur les comptes de l'internaute.

La Cour de cassation a annulé l'arrêt de la Cour et jugé que « *manque par négligence grave, à son obligation de prendre toute mesure raisonnable pour préserver la sécurité de ses dispositifs de sécurité personnalisés, l'utilisateur d'un service de paiement qui communique les données personnelles de ce dispositif de sécurité en réponse à un courriel qui contient des indices permettant à un utilisateur normalement attentif de douter de sa provenance, peu important qu'il soit, ou non, avisé des risques d'hameçonnage*. »

La banque peut donc rapporter par tous moyens la preuve de la négligence fautive de l'utilisateur, qui semble de plus en plus facile à démontrer lorsque l'on examine la jurisprudence récente de la Cour suprême (à rapprocher : **Paiement en ligne frauduleux : obligations pesant sur l'utilisateur**) et ce, d'autant que désormais il n'est plus nécessaire que la victime soit avisée par son établissement bancaire des risques de phishing.

Ainsi, elle pourra aisément échapper à son obligation de garantie. Les utilisateurs de services de banque en ligne, pour leur part, doivent encore et à nouveau redoubler de vigilance.

A rapprocher : Art. L133-16 Code monétaire et financier ; Art. L133-19 Code monétaire et financier ; Cass. com., 18 janvier 2017, n°15-18.466 ; Cass. com., 25 octobre 2017, n°16-11.644

E-COMMERCE

La publicité en ligne sous la surveillance de l'Autorité de la concurrence
Adlc, avis n°2018-A-03 du 6 mars 2018

Ce qu'il faut retenir :

L'Autorité de la concurrence soulève des préoccupations de concurrence concernant la publicité sur internet, et plus précisément l'exploitation des données issues de cette publicité.

Pour approfondir :

Après une année d'enquête sur la **publicité** en ligne, devenue aujourd'hui le premier média publicitaire en France (devant la télévision), l'Autorité de la concurrence a rendu le 6 mars 2018 un avis particulièrement volumineux (125 pages) relatif à l'exploitation des données dans le secteur de la publicité sur internet, après avoir consulté les principaux acteurs du marché, et recueilli leurs observations.

L'Autorité y présente le marché protéiforme de la publicité en ligne, qui représente à ce jour plus de 4 milliards d'euros en France, avec une progression de 12% en 2017, ainsi que ses multiples acteurs. Selon l'Autorité de la concurrence, le marché de la publicité en ligne se distingue par plusieurs spécificités, parmi lesquelles figurent la place des internautes dans l'animation de la concurrence et l'importance de l'exploitation des données.

L'Autorité de la concurrence distingue la publicité dite « Search » liée aux recherches effectuées par les internautes (première source de revenus dans la publicité en ligne), de la publicité dite « display », à plus forte croissance, que l'Autorité de la concurrence définit comme recouvrant « toutes les formes de publicité affichée sur les écrans et non spécifiquement liée aux recherches » (ex : bannières, vidéos, publicité native, etc.). La publicité display se développe notamment par le biais des réseaux sociaux, de la publicité vidéo et du mobile.

L'Autorité de la concurrence procède à une description précise des types d'outils permettant la collecte des données des internautes, qui servent ensuite à programmer les publicités qui leurs sont adressées. Elle présente en particulier un encadré instructif sur les types de traceurs non logués (cookie first-party, tag, pixel de traçage, de conversion ou Javascript, etc.) utilisés pour les besoins de la publicité en ligne, avec leurs fonctionnalités propres.

Selon l'Autorité de la concurrence, le marché de la publicité en ligne dispose d'un équilibre concurrentiel fragile, lié notamment à la présence de deux acteurs globaux prédominants que sont Google (entreprise qui aurait généré seule environ la moitié des revenus du secteur de la publicité sur internet en 2016) et Facebook, qui tirent environ 90% de leurs revenus de la vente de services publicitaires.

Ces deux entités bénéficient de plusieurs avantages concurrentiels significatifs, tels que leur forte popularité auprès des internautes, une intégration verticale (par leur présence à la fois au stade de l'édition et de celui de l'intermédiation publicitaire), des capacités de ciblages publicitaires très performants, l'importance du volume et de la variété des données traitées et la taille des inventaires publicitaires mis à la disposition des annonceurs.

Si la situation prédominante de ces deux acteurs majeurs de l'internet n'est pas en tant que telle problématique, certaines entreprises se sont émues auprès de l'Autorité de la concurrence de pratiques, dont l'Autorité de la concurrence a confirmé qu'elles étaient susceptibles – si elles étaient établies – de constituer des pratiques anticoncurrentielles, en particulier de potentiels abus de position dominante.

Il s'agirait de :

- stratégies de couplage/ventes liées, de prix bas et d'exclusivité (relatifs notamment à l'association de plusieurs services d'intermédiation, ou encore la soumission de l'accès aux données à la souscription à certains services) ;

- utilisation par les acteurs d'effets de levier grâce à leur position prépondérante sur des marchés, pour développer des positions sur d'autres marchés (où ils ne sont pas en position dominante). Ces pratiques concerneraient les secteurs de l'audit média et des agences médias, ainsi que la fourniture de services publicitaires et de services d'exploitation de données aux annonceurs ;

- pratiques discriminatoires dans le secteur de l'intermédiation publicitaire, soit pour renforcer de manière artificielle la position dominante des acteurs, soit pour distordre le jeu de la concurrence en avantageant ou désavantageant de manière artificielle certains des acteurs du marché par rapport à d'autres ;

- freins à l'interopérabilité dans le secteur de l'intermédiation publicitaire. Ces pratiques pourraient alors être considérées comme des refus d'accès à une facilité essentielle, ou comme des discriminations, des absences de transparence ou encore des pratiques de couplage ;

- restrictions concernant les possibilités de collecter et d'accéder à certaines données (ex : refus opposé aux acteurs de services de télévision d'accéder aux données sur l'usage de leurs propres services ; opacité des informations fondées sur des bases strictement déclaratives). L'Autorité de la concurrence précise que ces restrictions peuvent être considérées comme anticoncurrentielles si les données concernées constituent une facilité essentielle ou si le refus est discriminatoire (constituant ainsi un abus de position dominante), ou encore sous l'angle de l'entente anticoncurrentielle ;

- problématiques rencontrées par certains acteurs relatives à la mesure d'audience et la certification de certaines entreprises par des organismes tiers.

En cas de situation de position dominante sur l'un des marchés pertinents définis par l'Autorité de la concurrence dans son avis (v. points 154 à189 de l'avis), ces pratiques pourraient donc être poursuivies et sanctionnées.

Enfin, l'Autorité de la concurrence a appelé de ses vœux, à la fin de son avis, la mise en place d'un cadre législatif rééquilibrant les règles de transparence et favorisant une concurrence durable. En particulier, elle souligne la nécessité que les éditeurs et annonceurs puissent bénéficier d'un niveau de transparence élevé dans leurs relations avec les intermédiaires publicitaires et les plateformes de distribution de contenus, et que soit garantie l'absence d'asymétrie en matière de transparence et d'exploitation de données des individus.

Dans ce contexte, l'Autorité de la concurrence formule plusieurs observations sur la mise en œuvre du décret dit « Sapin » sur la transparence du 9 février 2017, ainsi que sur le projet de règlement européen sur la vie privée (proposition de règlement dit « *ePrivacy* » de la Commission européenne du 10 janvier 2017), qui vient compléter le dispositif mis en place par le RGPD de 2016. L'Autorité de la concurrence considère, s'agissant du projet de règlement *ePrivacy*, que par la protection des internautes qu'il instaure, notamment du fait d'un recueil du consentement de l'internaute au niveau du navigateur web et dans une logique d'*opt-in*, le règlement *ePrivacy* est susceptible de créer des distorsions de concurrence entre les acteurs de la publicité sur internet.

Cette distorsion s'exercerait en faveur des acteurs ayant mis en place des environnements logués et qui obtiendraient le consentement de l'internaute lors de son inscription, ce qui favoriserait en pratique des acteurs puissants, disposant de la capacité de mise en œuvre de tels environnements.

A rapprocher : Avis Adlc, n°18-A-03 du 6 mars 2018

CONTENUS ILLICITES / E-RÉPUTATION

Avis critique sur internet, par principe non-fautif, sauf intention de nuire
CA Dijon, 1ère Ch. civ., 20 mars 2018, n°15/02004

Ce qu'il faut retenir :

La Cour d'appel de Dijon, dans un arrêt du 20 mars 2018, rappelle le principe selon lequel le fait d'exprimer son avis, qu'il soit positif ou négatif, sur internet quant à une prestation de services, en l'espèce un service de restauration, n'est pas fautif en soi. Cependant, il le devient lorsque son auteur n'a pas bénéficié des services ou prestations critiqués, et si l'intention de nuire de l'internaute est caractérisée.

Pour approfondir :

La Cour d'appel de Dijon a jugé qu'un internaute ayant laissé un avis négatif relatif à un restaurant prestigieux sur le site www.pagesjaunes.fr, avait engagé sa responsabilité délictuelle sur le fondement des dispositions de l'article 1382 du Code civil au motif que le dénigrement de l'établissement était manifeste.

Elle a écarté l'application de l'article 29 de la Loi du 29 juillet 1881 relatif au délit de diffamation, considérant que la critique était dirigée à l'encontre d'une prestation de services, et ne concernait pas une personne physique ou morale.

En l'espèce, la Cour a retenu le caractère nécessairement mensonger du commentaire négatif (« *surfait* » à destination d'un restaurant prestigieux) dès lors que son auteur l'avait posté quelques jours avant l'ouverture dudit restaurant. Alertée par la société exploitant le restaurant, la société LES PAGES JAUNES avait immédiatement supprimé ce commentaire. Les juges ont, en outre, considéré que la mauvaise foi de l'auteur de la critique était particulièrement caractérisée par les faits de la cause puisque malgré cette suppression, l'internaute l'avait à nouveau posté dans des termes identiques, quelques jours plus tard, soit le jour même de l'ouverture, et qu'il l'avait modifié à plusieurs reprises, réitérant ainsi ses propos dénigrants, sans qu'il ne démontre avoir effectivement pris un quelconque repas dans l'établissement visé.

La preuve était ainsi rapportée que les commentaires peu flatteurs étaient uniquement destinés à dissuader une potentielle clientèle à fréquenter le restaurant.

La Cour d'appel a jugé que le comportement de l'auteur des avis litigieux révélait son intention de nuire caractérisant la faute exigée par l'ancien article 1382 du Code civil, pour retenir un dénigrement manifeste.

L'auteur a donc été condamné à verser des dommages-intérêts tendant à indemniser le préjudice financier ainsi que l'atteinte à l'image du restaurant, outre les frais de procédure.

Toutefois, le principe demeure : le commentaire critique de services ou de prestations publié sur un site internet n'est pas en soi constitutif d'une faute, sauf circonstances particulières démontrant l'intention de nuire.

A rapprocher : Art. 1382 ancien du Code civil ; Art. 1240 nouveau du Code civil ; Art. 29 de Loi du 29 juillet 1881

INTERNATIONAL

Action individuelle d'un consommateur et cessions de droits
CJUE, 25 janvier 2018, aff. C-498/16

Ce qu'il faut retenir :

Le fait de publier des livres ou de participer à des conférences de manière rémunérée ne fait pas perdre à un utilisateur d'un compte Facebook privé sa qualité de consommateur au sens de l'article 15 du règlement Bruxelles I. Il peut donc engager une procédure à titre personnel contre Facebook, en revanche il ne peut agir au nom d'autres consommateurs domiciliés dans le même Etat membre, dans d'autres Etats membres ou dans des Etats tiers.

Pour approfondir :

Maximilian Schrems, un Autrichien a attrait Facebook Ireland (« Facebook »), devant les juridictions autrichiennes en application de l'article 16 du Règlement Bruxelles I, à propos de son compte Facebook et des comptes de sept autres personnes, domiciliées en Autriche, en Allemagne et en Inde, qui lui ont cédé leurs droits pour cette action. Il a reproché à Facebook d'avoir violé plusieurs dispositions en matière de protection des données, notamment au regard des lois autrichienne et irlandaise et de la directive n°95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Facebook a considéré que les juridictions autrichiennes n'étaient pas compétentes internationalement car le plaignant ne pouvait bénéficier des lois de protection des consommateurs, tel que le Règlement de Bruxelles I, du fait qu'il utilisait sa page Facebook à des fins professionnelles. En effet, M. Schrems avait ouvert un compte Facebook à des fins privées, puis par la suite, une page Facebook afin d'informer les internautes de ses démarches contre Facebook.

Par ailleurs, Facebook a fait valoir que le for du consommateur qui permet à un consommateur d'attaquer une entreprise devant les juridictions de son pays, est strictement personnel, et que l'intéressé ne pouvait donc pas l'invoquer pour les sept autres plaignants.

La Cour suprême d'Autriche a donc demandé à la Cour de préciser les conditions dans lesquelles le for du consommateur pouvait être invoqué et la portée en matière de compétence, d'une cession de droits. La question de la définition du consommateur est récurrente dans la jurisprudence européenne.

Tout d'abord, la Cour a considéré qu'il fallait, en présence d'un utilisateur d'un réseau social numérique, tenir compte « *de l'évolution de l'usage qui est fait de ces services* » au fil du temps, et que par ailleurs, la qualification de consommateur était « *indépendante des connaissances et des informations dont la personne concernée dispose réellement* ». Elle a ajouté que l'interprétation de la notion de « consommateur » qui exclurait de telles activités reviendrait à empêcher la préservation des intérêts des consommateurs à l'égard de leurs cocontractants professionnels.

La Cour a donc conclu que l'utilisateur d'un compte Facebook privé ne perd pas la qualité de consommateur lorsqu'il publie des livres, donne des conférences, exploite des sites Internet, collecte des dons et se fait céder les droits de nombreux consommateurs afin de faire valoir ceux-ci en justice.
M. Schrems peut donc toujours être considéré comme un consommateur dans ses actions judiciaires conte Facebook.

La Cour a ensuite rappelé, que le for du consommateur a été créé afin de protéger le consommateur en tant que partie au contrat en cause et que dès lors, il ne pouvait bénéficier de cette protection que dans la mesure où il serait personnellement demandeur ou défendeur dans une procédure. Dès lors, celui qui n'est pas lui-même partie au contrat de consommation en cause ne peut pas bénéficier de ce for.

Par conséquent, la Cour a retenu que le for du consommateur ne pouvait pas être invoqué pour l'action d'un consommateur visant à faire valoir devant le tribunal du lieu où il est domicilié, non seulement ses propres droits, mais aussi les droits cédés par d'autres consommateurs domiciliés dans le même Etat membre, d'autres Etats membres ou dans des Etats tiers.

Il faut néanmoins noter, qu'au-delà du cas de Facebook, cette décision intéresse l'ensemble des acteurs du numérique dès lors que leurs utilisateurs font usage de leurs services à des fins professionnelles.

A rapprocher : Articles 15 et 16 du règlement Bruxelles I ; Directive n°95/46/CE du 24 octobre 1995

LEGALTECHS / TENDANCES

La promotion de l'Intelligence Artificielle par la Commission européenne

Communiqué de presse du 25 avril 2018

Ce qu'il faut retenir :

Dans un communiqué de presse du 25 avril 2018, La Commission européenne expose son approche et ses lignes directrices pour favoriser l'introduction et le développement de l'Intelligence Artificielle à tous les niveaux, aussi bien dans les PME que dans les grandes entreprises.

Pour approfondir :

L'intelligence artificielle (IA) n'a de cesse de se développer ces dernières années.

Les effets potentiels de cette technologie sont importants et peuvent concerner de nombreux secteurs, notamment la médecine, l'agriculture, l'industrie, l'environnement ou encore la cybersécurité.

Plusieurs nations investissent déjà massivement dans la recherche sur l'intelligence artificielle, espérant même construire une société reposant essentiellement sur cette technologie, comme la Chine et les États-Unis.

Devant cette future révolution et pour n'accuser aucun retard, la Commission européenne a fait le choix de ne pas rester passive. Elle a donc pris l'initiative de définir quelle sera sa politique en matière d'intelligence artificielle. Dans un communiqué de presse du 25 avril 2018, elle expose son approche et ses lignes directrices pour favoriser l'introduction et le développement de cette technologie à tous les niveaux, aussi bien dans les PME que dans les grandes entreprises.

L'ambition affichée par la Commission est claire : l'intelligence artificielle est une ressource stratégique capable de transformer la société et, dès lors, l'Union Européenne doit investir dans cette technologie pour en développer la prochaine génération et lui donner des applications concrètes.

Parallèlement à cette volonté de compétitivité, la Commission souhaite que ce développement s'accompagne d'un encadrement éthique et juridique approprié. Retour sur les principales annonces de la Commission.

Le premier message des commissaires est de renforcer les investissements de la part des secteurs public et privé dans l'IA. L'objectif est d'atteindre un montant d'investissement d'au moins 20 milliards d'euros d'ici la fin de l'année 2020. Ces fonds permettront le financement des différents projets de recherche fondamentale et d'amélioration des résultats technologies de l'IA. Dans le même temps, la Commission entend établir des « centres d'excellence en IA » à travers toute l'Europe, pour stimuler la collaboration et le travail en réseau dans la recherche et les projets conjoints sur le sujet.

Le Commission européenne souhaite également offrir des conseils et rendre accessible les derniers algorithmes et le savoir-faire à tous les utilisateurs potentiels, y compris les PME, par le biais d'une plateforme européenne d' « IA à la demande ». Le but est d'encourager l'adoption de l'IA à tous les niveaux.

Pour accompagner cela, elle évoque aussi la création d'un réseau de pôles d'innovation numérique dédiés aux essais et expérimentations, et de plateformes de données industrielles contenant des données de qualité pour exploiter le potentiel des IA. Les pôles d'innovation permettront aux PME de demander l'utilisation d'une IA pour améliorer la qualité de leurs produits et services. L'idée est de construire un écosystème local capable de soutenir les entreprises d'une région.

La deuxième annonce vise à préparer le monde professionnel aux changements socio-économiques provoqués par l'IA. Les Européens doivent pouvoir acquérir les compétences et les connaissances nécessaires pour maîtriser les nouvelles technologies à venir. Pour ce faire, la Commission encourage la mise en place de programmes nationaux pour proposer ces formations. Des « secteurs pilotes » ont déjà été sélectionnés pour définir les compétences nécessaires et les lacunes à combler dans leur domaine, ce qui permettra d'établir une stratégie européenne commune et d'élaborer des programmes d'études adaptés.

La Commission européenne annonce que les étudiants et jeunes diplômés bénéficieront d'opportunités de stages à l'étranger pour acquérir une expérience numérique en entreprise, en particulier dans les secteurs déficitaires, et pour renforcer leurs compétences en matière de nouvelles technologies.

Les États-membres devront aussi élaborer des stratégies nationales en matière d'apprentissage des compétences numériques et créer des coalitions nationales pour les mettre en œuvre.

À ce titre, les entreprises spécialisées dans le secteur des NTIC seront encouragées à faire des partenariats avec le monde éducatif, pour créer des programmes orientés vers l'IA.

Enfin, la troisième orientation de la Commission européenne consiste à mettre en place un cadre éthique et juridique approprié pour l'IA. Consciente de l'importance des algorithmes dans la vie quotidienne des citoyens, elle souhaite adopter des lignes directrices en matière d'éthique d'ici la fin de l'année, élaborées sur la base de la charte des droits fondamentaux de l'UE. Les lignes directrices aborderont notamment la transparence des algorithmes, l'avenir du travail, l'équité, la sécurité, l'inclusion sociale, et l'impact sur les droits fondamentaux, dont le respect à la vie privée, la dignité, la protection des consommateurs et la non-discrimination.

Sur le plan juridique, la Commission européenne annonce qu'il est prévu la publication d'orientations interprétatives pour clarifier les notions de la directive de 1985 relatives à la responsabilité du fait de produits défectueux. Ces orientations se présenteront sous l'angle des nouvelles technologies numériques, en tenant compte de l'intégration de l'IA dans les produits.

L'entrée en application du RGPD le 25 mai prochain aura également un impact sur l'utilisation de l'IA, en raison des dispositions visant la prise de décision fondée sur un traitement automatisé, notamment le profilage.

A rapprocher : Communiqué de presse de la Commission européenne du 25 avril 2018

***

ACTUALITÉ NUMÉRIQUE SIMON ASSOCIÉS

MAI 2018

Atelier RGPD
Événement organisé par l'IMIE D'ANGERS et animé par STEPHANE BAÏKOFF
18 mai 2018 – Angers

Atelier RGPD : Jamais trop tard !
Événement organisé par l'Association FEMMES DU DIGITAL OUEST et animé par STEPHANE BAÏKOFF
25 mai 2018 – Nantes
En savoir plus et s'inscrire

JUIN 2018

La gouvernance des données personnelles
Petit-déjeuner RGPD organisé par SIMON ASSOCIES et animé par AMIRA BOUNEDJOUM
19 juin 2018 – Paris
Plus d'informations prochainement

Sécurisation des données de santé : enjeux juridiques et techniques
Formation organisée par SIMON ASSOCIES et animée par AMIRA BOUNEDJOUM,
en partenariat avec ZIWIT, leader européen de la cyber sécurité,
à destination des DSI et des Directeurs juridiques
22 juin 2018 – Montpellier
Plus d'informations prochainement