SOMMAIRE

DATA / DONNÉES PERSONNELLES

Manquement à l'obligation de sécurité des données : OPTICAL CENTER condamnée à 250 000 € d'amende
CNIL, Délibération n°SAN- 2018-002 du 7 mai 2018

Ce qu'il faut retenir :

La CNIL a condamné, sur le fondement de la Loi informatique et Libertés dans sa version applicable en juillet 2017, la société OPTICAL CENTER à régler une sanction pécuniaire à hauteur de 250 000 €, après avoir constaté que cette dernière avait manqué à son obligation d'assurer la sécurité et la confidentialité des données de ses clients enregistrées sur son site internet www.optical-center.fr.

En effet, la CNIL a constaté que la société n'avait pas pris les mesures de sécurité élémentaires en amont de la mise en œuvre d'une nouvelle fonctionnalité de son site internet. Elle a ainsi relevé que « *le site internet de la société, qui permet d'effectuer des commandes en ligne après avoir créé un compte dédié, n'intégrait pas de fonctionnalité permettant de vérifier qu'un client s'est bien authentifié à son espace personnel avant de lui donner accès auxdits documents*. »

Pour approfondir :

La CNIL a été informée, en juillet 2017, d'une faille de sécurité concernant la société OPTICAL CENTER. A l'issue d'un contrôle réalisé en ligne, la CNIL a constaté qu'il était possible d'accéder librement, à partir d'adresses URL, à des factures de clients ayant passé commande en ligne. Ces factures contenaient les données à caractère personnel suivantes : nom, prénom, adresse postale, données de santé, date de naissance et, parfois même, le numéro de sécurité sociale.

La société a immédiatement reconnu auprès de la CNIL le défaut de sécurité résidant dans l'absence de contrôle de connexion d'un client à son compte avant l'affichage de son contenu.

A l'issue d'une procédure contradictoire devant la commission restreinte de la CNIL, la société a été condamnée à une sanction pécuniaire de 250 000 €, telle que proposée par le rapporteur.

Pour mémoire, le maximum encouru était alors de 3 millions d'euros.

La CNIL a tenu compte de nombreux éléments pour suivre les conclusions du rapporteur. Elle a, dans un premier temps, constaté que le manquement relevé à l'encontre du responsable de traitement à son obligation de sécurité était d'une particulière gravité. En effet, elle relève que ce sont des mesures élémentaires de sécurité qui n'ont pas été mises en œuvre par le responsable de traitement. Il lui appartenait de mettre en place une fonctionnalité permettant la restriction d'accès des documents mis à la disposition des clients sur leur espace dédié, ce qui constitue une précaution d'usage essentielle.

La CNIL s'est également fondée sur le fait que la base de données de la société contenait plus de 330 000 documents à la date de constatation de la faille de sécurité, et que ce défaut a rendu librement accessible des données à caractère personnel telles que nom, prénom, date de naissance, mais également des données sensibles au sens de l'article 8 de la Loi Informatique et Libertés, à savoir des données de santé et le numéro de sécurité sociale. Il est donc indéniable que la quantité et la nature sensible ou non de données manipulées sont des critères retenus par l'autorité administrative pour fixer le quantum de la sanction. Le risque ainsi créé pour les personnes dont les données étaient librement accessibles de se voir l'objet d'un hameçonnage ciblé (phishing) a également été souligné par la CNIL.

Enfin, le fait que le responsable de traitement ait été condamné deux ans auparavant par la même autorité à une sanction pécuniaire de 50 000 € rend d'autant plus grave, bien que la CNIL s'en défende expressément dans cette décision, le manquement constaté. Cette première amende aurait naturellement dû inciter la société OPTICAL CENTER à la plus grande vigilance en matière de sécurité et confidentialité des données à caractère personnel dans le cadre de la mise en œuvre de ses traitements.

A rapprocher : Art. 34 de la Loi Informatique et Libertés ; Art. 8 de la Loi Informatique et Libertés

Transparence et vigilance en matière de cookies sur les sites internet

CE, 10ème - 9ème ch. réunies, 6 juin 2018, n°412589

Ce qu'il faut retenir :

L'éditeur d'un site internet qui utilise des cookies doit s'assurer d'informer de manière claire et transparente ses internautes des finalités des cookies déposés à l'occasion d'une visite sur son site et de définir et respecter une durée de conservation proportionnée à la finalité de ces cookies. Le Conseil d'Etat a confirmé la décision de la CNIL qui a prononcé une sanction à l'encontre de l'éditeur du site challenge.fr qui s'est contenté de présenter à ses internautes comment paramétrer leur navigateur pour refuser les cookies et qui n'a ni respecté une durée de conservation limitée ni vérifié que ses partenaires déposant des cookies tiers (sur lesquels il n'a aucune maitrise technique) respectent bien la réglementation en la matière.

Pour approfondir :

Le Conseil d'Etat a confirmé, dans sa décision du 6 juin 2018, la position de la Cnil sur le fait que le paramétrage du navigateur n'est pas un mode valable d'opposition au dépôt de cookies.

Pour rappel, l'éditeur du site internet challenge.fr avait été condamné par la CNIL le 18 mai 2017 pour ne pas avoir respecté ses obligations d'information quant au dépôt de cookies sur le terminal de ses visiteurs et sur leur droit d'opposition alors qu'il avait été mis en demeure de le faire.

La CNIL avait alors prononcé une sanction pécuniaire de 25 000 € contre l'éditeur du site challenges.fr qui a décidé de faire un recours contre cette décision devant le Conseil d'Etat.

En matière de dépôt de cookies, la loi impose l'information des utilisateurs sur les finalités de ces cookies et sur les moyens de s'y opposer. Le recueil du consentement doit nécessairement avoir lieu avant leur dépôt, sauf si les cookies déposés sont nécessaires au fonctionnement du site ou qu'ils correspondent à la fourniture du service à la demande de l'utilisateur.

Si l'éditeur du site faisait valoir que ses cookies à finalités publicitaire et commerciale étaient nécessaires à la survie économique du site, le Conseil d'Etat a précisé que cette circonstance ne permettait pas de considérer que ces cookies relevaient de la catégorie de ceux strictement nécessaires à la fourniture du site et par conséquent exemptés de consentement.

Le Conseil d'Etat a par ailleurs précisé que l'information délivrée par le site n'était pas suffisamment transparente et ne permettait pas aux internautes de différencier clairement les catégories de cookies, ni de s'opposer à leur dépôt. Dès lors, le simple fait pour l'éditeur de proposer à ses internautes de paramétrer leur navigateur ne permet pas d'en conclure que ceux n'ayant pas refusé via leurs paramètres les cookies y avaient consenti.

Le Conseil d'Etat a clairement précisé que c'est à bon droit que *« la formation restreinte de la CNIL a considéré que le paramétrage du navigateur proposé aux utilisateurs ne constituait pas un mode valable d'opposition au dépôt de cookies ».*

Dans sa délibération, la CNIL avait également relevé que l'éditeur avait manqué à son obligation de définir et respecter une durée de conservation des données proportionnée à la finalité du traitement et qu'il n'avait pas donné suite à sa mise en demeure de ne pas conserver les cookies au-delà de treize mois.

En ce qui concerne les « cookies » déposés par des tiers, la CNIL a également caractérisé les manquements de l'éditeur du fait qu'il n'avait apporté aucune justification qu'il aurait effectué des démarches auprès de ses partenaires afin qu'ils respectent eux aussi une durée de conservation adéquate et proportionnée.

Le Conseil d'Etat a confirmé la décision de la CNIL et a précisé que *« les éditeurs de site qui autorisent le dépôt et l'utilisation de tels « cookies » par des tiers à l'occasion de la visite de leur site doivent également être considérés comme responsables de traitement, alors même qu'ils ne sont pas soumis à l'ensemble des obligations qui s'imposent au tiers qui a émis le « cookie », notamment lorsque ce dernier conserve seul la maitrise du respect de sa finalité ou de sa durée de conservation. »*

En conséquence, il appartient à tout éditeur d'un site internet de s'assurer que les partenaires autorisés à déposer des cookies respectent la réglementation sous peine d'engager leur propre responsabilité.

A rapprocher : Nouvel article 32 de la loi informatique et liberté (modifié par la loi n°2018-493 du 20 juin 2018)

Loi informatique et libertés III : articulation avec le RGPD
Modification de la Loi informatique et Libertés n°78-17 du 6 janvier 1978

Ce qu'il faut retenir :

La loi du 20 juin 2018 n°2018-493, prise en application du Règlement (UE) 2016/679 sur la Protection des données du 27 avril 2016, vient désormais modifier la Loi informatique et Libertés n°78-17 du 6 janvier 1978.

Pour approfondir :

La loi du 20 juin 2018 promulguée le 21 juin 2018, a été publiée au Journal Officiel le jour même, et ce, dans la plus grande intimité.

S'il est indéniable que les débats parlementaires, qui l'ont précédée, ont été assidument suivis et relayés dans la presse, il n'en demeure pas moins que son adoption a été plus que discrète, nous semble-t-il.

Sans doute, les acteurs sont-ils aujourd'hui plus accaparés par leur propre chantier de mise en conformité que par les évolutions législatives en droit national.

En toute hypothèse, cette loi a finalement été adoptée et intègre partiellement les dispositions du RGPD et de la Directive Police-Justice dans la loi Informatique et Libertés, tout en complétant cet arsenal juridique, notamment s'agissant du traitement des données de santé, et des fichiers d'infraction.

Son imperfection étant soulignée, et le manque de lisibilité du cadre juridique national ainsi fixé dénoncé, une ordonnance de refonte de la Loi Informatique et Libertés doit être adoptée dans les six prochains mois.

En effet, la coexistence de deux socles de règles (le RGPD, d'une part, et la Loi du 6 janvier 1978 modifiée, d'autre part) est susceptible de poser quelques difficultés sur le plan pratique.

C'est la raison pour laquelle il convient de revenir aux fondamentaux du droit et à la hiérarchie des normes.

Pour mémoire, le Règlement Européen sur la Protection des Données est d'application directe sur tout le territoire de l'Union Européenne, et donc en France. La théorie de la hiérarchie des normes pose comme principe qu'une norme inférieure doit respecter celle d'un rang supérieur, et qu'en cas de conflit de normes, l'on doit faire prévaloir la norme de rang supérieur.

En conséquence, et dans les hypothèses dans lesquelles la nouvelle Loi Informatique et Libertés modifiée par la loi du 20 juin 2018 n°2018-493, serait muette ou en contradiction avec le RGPD, il y aura lieu d'appliquer le RGPD, puisque les normes européennes sont de rang supérieur aux normes nationales.

L'on aurait naturellement pu attendre du législateur français qu'il procède à un travail complet d'adaptation. Tel n'étant pas le cas, il nous apparaissait important de rappeler les règles sus-évoquées permettant d'appréhender l'articulation du RGPD et de la Loi Informatique et Libertés dans l'attende de l'ordonnance de réécriture complète de cette même loi, et de son nouveau décret d'application.

A rapprocher : Loi n°2018-493 du 20 juin 2018

PROPRIÉTÉ INTELLECTUELLE

« MESSI » : le joueur peut enregistrer son nom à titre de marque
TUE, 26 avril 2018, aff. T-554/14

Ce qu'il faut retenir :

Lorsque des signes présentent des similitudes visuelles et phonétiques, les différences conceptuelles entre les signes peuvent être telles qu'en définitive les signes ne seront pas jugés comme similaires.

Pour approfondir :

Lors de l'enregistrement d'une marque, il convient au préalable de vérifier l'existence d'antériorités susceptibles d'empêcher l'enregistrement de celle-ci. Les tiers ont en effet la possibilité de s'opposer au dépôt lorsque, notamment, ils sont titulaires d'une marque antérieure, identique ou similaire pour désigner les mêmes produits et services.

Pour apprécier la similitude entre les signes, on s'attache à rechercher si les similitudes entre les signes, au niveau visuel, phonétique et conceptuel, sont

susceptibles d'entraîner un risque de confusion pour le consommateur concerné.

Le célèbre, et même légendaire, joueur de football Lionel Messi a déposé une demande de marque européenne semi-figurative – incluant son nom « Messi » pour désigner, notamment, des vêtements, chaussures et articles de sport. Une opposition à cette demande a été formée par le titulaire de marques antérieures verbales « Massi » déposées pour désigner des produits similaires. Le joueur se devait donc de défendre la possibilité de se réserver son nom à titre de marque !

Dans un premier temps, l'opposition à la demande d'enregistrement a été accueillie : la division d'opposition de l'EUIPO a jugé que les signes en présence étaient similaires sur le plan visuel et phonétique, ces similarités étant de nature à créer un risque de confusion entre les signes en présence.

Dans un deuxième temps, la Chambre de recours de l'EUIPO a confirmé la décision estimant que les termes « massi » et « messi », sont quasiment identiques sur les plans visuel et phonétique et qu'une éventuelle différenciation conceptuelle ne sera opérée, le cas échéant, que par une partie du public pertinent.

Cette appréciation n'est pas celle adoptée par le Tribunal de l'UE, saisi d'un recours contre cette décision par le joueur à qui l'EUIPO avait refusé la possibilité de déposer, à titre de marque, un signe intégrant son nom.

Le Tribunal va reprendre l'examen de la comparaison entre les signes et de la recherche de similitudes :

- sur le plan visuel : le Tribunal approuve l'appréciation portée selon laquelle la demande de marque peut être considérée comme similaire à la marque antérieure parce que son élément dominant « messi » est extrêmement similaire au signe « massi » ;

- sur le plan phonétique : le Tribunal approuve encore l'appréciation selon laquelle les signes en présence ont une similarité phonétique très importante, voire identique dans certains pays ;

- sur le plan conceptuel : le Tribunal relève tout d'abord que la renommée dont jouit Lionel Messi ne concerne pas que la partie du public qui s'intéresse au football et au sport. Celui-ci est un personnage public connu par la plupart des personnes informées, raisonnablement attentives et avisées, qui lisent la presse, regardent les informations à la télévision, vont au cinéma ou écoutent la radio, où l'on peut le voir et où l'on parle de lui régulièrement.

Ensuite, il convient de tenir compte du fait que les produits visés par les deux marques pour lesquels un risque de confusion pourrait exister sont, notamment, des articles et des vêtements de sport, même s'ils ne se limitent pas au domaine du football.

Or, il paraît peu vraisemblable qu'un consommateur moyen d'articles et de vêtements de sport, raisonnablement attentif, informé et avisé, n'associera pas directement, dans la grande majorité des cas, le terme « messi » au nom du célèbre joueur de football.

Le Tribunal reconnaît la renommée du nom Messi et, en conséquence, estime que compte tenu de cette notoriété le terme « messi » a une signification clairement différente, sur le plan conceptuel, du terme « massi », qui fait référence à un nom à consonance italienne, sans véhiculer de signification particulière, sauf en italien, où il pourrait être traduit comme « grosses pierres ».

Cette différence conceptuelle entre les signes a des conséquences importantes, le Tribunal estime qu'elle neutralise les similitudes visuelles et phonétiques et, en conséquence, exclut tout risque de confusion pour un consommateur d'attention moyenne.

La demande de marque est donc admise et le joueur va pouvoir faire enregistrer le nom Messi à titre de marque.

Les amateurs de football seront rassurés de voir que leur idole pourra déposer une marque intégrant son nom et que sa notoriété est reconnue, les amateurs du droit des marques retiendront, quant à eux, que nonobstant des similitudes visuelles et phonétiques entre deux signes, le fait que l'un d'entre eux soit porteur d'un sens particulier peut exclure toute similitude conceptuelle et, partant, tout risque de confusion.

A rapprocher : Règlement (UE) 2017/1001 du Parlement européen et du Conseil du 14 juin 2017

Clause de non-dépôt de brevet
Cass. com., 3 mai 2018, n°16-25.067

Ce qu'il faut retenir :

La clause par laquelle le salarié s'engage, postérieurement à la cessation de son contrat de travail, à ne pas déposer une invention créée pendant l'exécution de son contrat de travail, n'est pas une clause de non-concurrence.

Pour approfondir :

L'affaire opposait un ancien salarié, licencié pour faute grave, à son ancien employeur à qui il réclamait diverses sommes au titre d'une invention réalisée pendant son contrat de travail.

Les inventions de salariés obéissent, en effet, à un régime spécifique organisé par le Code de la propriété intellectuelle (article L.611-7 du Code de la propriété intellectuelle), lequel varie selon qu'il s'agisse d'inventions dites de mission, d'inventions hors mission.

En l'espèce, en particulier, le salarié sollicitait le paiement d'une rémunération supplémentaire, en se fondant sur les dispositions du Code de la propriété intellectuelle et celles de la convention collective applicable. A l'aune des stipulations de celle-ci, la Cour va casser l'arrêt de la Cour d'appel, faisant grief aux juges du fond d'avoir alloué une rémunération supplémentaire alors que l'invention n'était pas brevetable et que la convention collective stipulait, s'agissant des inventions non brevetables, qu'elles peuvent donner lieu à l'attribution de primes. Selon la Haute Cour, le versement d'une prime est laissé à la libre appréciation de l'employeur. Précisons ici que la solution ne doit pas être étendue à toutes les situations, la convention collective applicable à chaque situation étant susceptible de contenir des dispositions différentes.

Le second fondement utilisé par le salarié pour obtenir une indemnisation résidait dans la clause de son contrat de travail lui faisant interdiction, pendant la durée de son contrat et les cinq ans suivant sa cessation, de procéder en son nom ou celui d'un tiers, à tout dépôt ou formalités auprès des registres de marques, dessins et modèles, brevets pour des créations inventées pendant l'exécution de son contrat, et lui faisant interdiction, pendant un délai de trois ans à compter de la résiliation du contrat, de publier des articles scientifiques, de diffuser des informations commerciales, des renseignements techniques relatifs à son employeur. Le salarié prétendait que cette clause avait pour objet et pour conséquence de limiter la liberté d'utilisation du savoir-faire acquis auprès de l'employeur et qu'elle devait, en conséquence, être assimilable à une clause de non-concurrence supposant une contrepartie financière. La clause ne comportant pas une telle contrepartie, il réclamait en conséquence d'être indemnisé de la perte de chance d'obtenir telle contrepartie.

Tandis que la Cour d'appel avait suivi l'argumentation, la Haute Cour va au contraire affirmer qu'une telle assimilation ne peut être opérée : « … *alors que l'engagement du salarié, après la rupture du contrat de travail, à ne déposer aucun brevet pour des créations inventées pendant l'exécution de son contrat ainsi que son engagement à ne publier aucun article scientifique et à ne diffuser aucune information commerciale ni aucun renseignement technique, relatifs à la société [-], n'étaient pas assimilables à une clause de non-concurrence et n'ouvraient pas droit au paiement d'une contrepartie financière ».*

Il faut donc retenir que la clause par laquelle le salarié s'engage, postérieurement à la cessation de son contrat de travail, à ne pas déposer une invention créée pendant l'exécution de son contrat de travail, n'est pas une clause de non-concurrence, elle ne suit donc pas son régime spécifique et, en particulier, ne nécessite pas de contrepartie financière.

La clause de non-concurrence restreint le libre exercice, par le salarié, d'une activité professionnelle ; or, la clause stipulant une interdiction de déposer un brevet n'a pas de tels effets, il est donc logique qu'elle ne soit pas assimilée à une clause de non-concurrence et la solution est, à notre sens, à approuver.

A rapprocher : Article L.611-7 du Code de la propriété intellectuelle ; Article 1134 ancien du Code civil ; Article L.1221-1 du Code du travail

Incidence de la connaissance d'une marque sur le marché pour sa défense
Cass. com., 30 mai 2018, n°16-22.994

Ce qu'il faut retenir :

La connaissance de la marque sur le marché est un facteur pertinent de l'appréciation du risque de confusion, en ce qu'elle confère à cette marque un caractère distinctif élevé et lui ouvre une protection étendue.

Pour approfondir :

Le titulaire de la **marque** complexe Joker + déposée en couleurs, avait formé une opposition à l'encontre de la demande d'enregistrement de la marque Joker déposée pour désigner les mêmes produits.

Le directeur de l'INPI avait accepté l'opposition et rejeté la demande d'enregistrement mais sa décision a été censurée par la Cour d'appel qui a considéré que le risque de confusion n'était pas établi.

Pour statuer ainsi, la Cour d'appel a jugé que si les signes en cause ont en commun le terme « Joker », en raison des importantes différences visuelles et phonétiques que présentent ces signes pris dans leur ensemble, le consommateur moyennement attentif ne sera pas amené à croire que le signe contesté serait la déclinaison ou l'adaptation de la marque antérieure et en déduit qu'il n'existe pas de risque de confusion.

La Cour de cassation reproche à l'arrêt de ne pas avoir recherché si les signes en cause présentent des similitudes sur le plan conceptuel. La solution est logique. En effet, pour l'appréciation globale du risque de confusion la similitude des signes doit être examinée d'un point de vue tant visuel et auditif que conceptuel, la similitude des signes sur un seul de ces plans étant susceptible de créer un risque de confusion entre les marques en cause. Aussi, en s'abstenant de procéder à l'examen de la similitude au niveau conceptuel les juges d'appel n'ont pas procédé à un examen global des signes en présence. La cassation est logique.

Le risque de confusion dans l'esprit du public doit être apprécié globalement en tenant compte de façon interdépendante de tous les facteurs pertinents du cas d'espèce et notamment de la connaissance de la marque sur le marché. Le risque de confusion est d'autant plus élevé que le caractère distinctif de la marque antérieure s'avère important. Or en l'espèce, le titulaire de la marque invoquait la très large connaissance de la marque antérieure dans le public ce qui, selon lui, venait renforcer le risque de confusion entre sa marque antérieure et le signe contesté. A nouveau, la Cour de cassation va reprocher aux juges du fond de ne pas avoir tenu compte de cet élément et énonce à cet égard : « *la connaissance de la marque sur le marché est un facteur pertinent de l'appréciation du risque de confusion, en ce qu'elle confère à cette marque un caractère distinctif élevé et lui ouvre une protection étendue* ».

La formulation interpelle, la Cour de cassation énonce explicitement que plus une marque est connue, plus sa protection est étendue et ce, sans faire référence au caractère renommé de la marque tandis que seules les marques renommées bénéficient d'un régime spécifique leur conférant de fait une protection plus large.

On se félicitera de cet arrêt qui tient compte de la valeur commerciale de la marque, de sa connaissance plus ou moins importante sur le marché pour apprécier les atteintes qui lui sont portées.

A rapprocher : article L713-3 du code de la propriété intellectuelle

SERVICES NUMÉRIQUES

Hameçonnage : la négligence fautive des utilisateurs de plus en plus facilement admise
Cass. com., 6 juin 2018, n°16.29-065

Ce qu'il faut retenir :

A la faveur de cette décision, la Cour de cassation a censuré l'arrêt de la Cour d'appel de Douai en date du 3 novembre 2016, qui avait condamné la banque à rembourser à sa cliente les sommes frauduleusement prélevées sur son compte, à la suite d'un mailing s'apparentant à une opération de phishing. La Cour de cassation a, en effet, 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 ces dispositifs de sécurité en réponse à un courriel qui contient des indices permettant à un utilisateur normalement attentif de douter de sa provenance* ».

La Cour de cassation continue ainsi son œuvre de durcissement de l'obligation de prudence pesant sur l'internaute en cas de phishing.

Pour approfondir :

Encore et à nouveau dans cette affaire, une victime de phishing a contesté certaines opérations de paiement réalisées sur son compte, lesquelles ont été, selon elle, faites frauduleusement. Les demandes de remboursement amiables étant restées vaines, elle n'a eu d'autre choix que de saisir la juridiction compétente pour obtenir de la banque qu'elle s'exécute.

L'internaute se prévalait du principe issu de la combinaison des articles L.133-17 et suivants du Code monétaire et financier selon lequel il appartient à la banque de supporter les conséquences de toute utilisation frauduleuse d'un instrument de paiement mis à la disposition du client, sauf à ce que cette utilisation résulte notamment de la négligence grave du client.

La Cour d'appel a fait droit à la demande de remboursement, après avoir relevé que la cliente avait communiqué ses coordonnées bancaires en réponse à un courriel comportant le logo de son opérateur de téléphonie. Les juges du fond ont ainsi pu se convaincre de ce que la négligence grave susceptible de faire obstacle à la demande de remboursement n'était pas constituée par les faits de l'espèce.

En effet, les juges ont constaté que le mail litigieux avait l'apparence de l'authenticité, comme ne présentant pas d'anomalies grossières, de telle sorte que l'internaute n'avait pas de raison de douter de l'origine de ce message, et y avait légitimement répondu.

La Banque a formé un pourvoi en cassation à l'encontre de l'arrêt de la Cour d'appel de Douai, en se fondant sur l'articulation des articles L.133-16 et L.133-19 du Code monétaire et financier. Le premier impose à l'utilisateur de moyens de paiement de prendre toute mesure raisonnable pour en préserver la sécurité. Le second le prive de la possibilité d'obtenir le remboursement de mouvements irréguliers sur son compte, s'ils l'ont été du fait de sa propre négligence fautive.

La Cour de cassation a cassé l'arrêt de la Cour d'appel de Douai, et censuré le raisonnement des juges du fond en ces termes : « *qu'en statuant ainsi, après avoir relevé que Mme Y réglait ses factures de téléphone par prélèvements et non par carte bancaire et qu'un examen attentif du courrier de rappel de paiement, révélait de sérieuses irrégularités, de nature à faire douter de sa provenance, telles que l'inexactitude de l'adresse de l'expéditeur et du numéro du contrat mentionné ainsi que la discordance entre les montants réclamés, la Cour d'appel, qui n'a pas tiré les conséquences légales de ses constatations, a violé les textes susvisés.* »

La Cour de cassation fait peser sur la victime de phishing une responsabilité de plus en plus accrue, nous semble-t-il. Cette dernière doit, pour pouvoir bénéficier de la garantie de la banque, rapporter la preuve de ce qu'elle n'a commis aucune négligence grave à l'occasion de la communication de ses coordonnées bancaires. Cette preuve apparaît de plus en plus difficile à rapporter eu égard aux dernières décisions de la Cour suprême, qui tient compte des habitudes de consommation de l'internaute, ainsi que d'erreurs, aussi subtiles soient-elles, glissées dans un mail illicite tel que le numéro de contrat erroné, ou encore adresse de l'expéditeur inexacte. Ces éléments ne sont, à notre sens, jamais vraiment vérifiés par les utilisateurs. Cette jurisprudence semble sévère à l'égard des victimes de phishing, qui supporteront alors toutes les conséquences financières de ce qui nous semble relever de l'inadvertance plus que d'une négligence grave.

Les utilisateurs de services en ligne sont désormais invités à la plus grande méfiance face aux sollicitations de règlement adressées par mail.

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

E-COMMERCE

Cartographie du e-commerce 2018 publiée par la FEVAD
FEVAD, communiqué de presse du 21 juin 2018

Ce qu'il faut retenir :

La FEVAD a publié le 21 juin dernier une cartographie du e-commerce en France en 2018, qui constitue le 3e marché en ligne d'Europe après le Royaume-Uni et l'Allemagne.

Pour approfondir :

La Fédération du e-commerce et de la vente à distance publie chaque année des chiffres-clés de référence, permettant de mesurer les évolutions et l'importance du e-commerce en France.

Les éléments fournis par la FEVAD reposent sur les chiffres réalisés en 2017 par les acteurs du e-commerce.

L'e-commerce est en nette progression dans les rapports B to C, avec une hausse de chiffre d'affaires de 14,3% (par rapport à 2016), pour un chiffre d'affaires total de 81,7 milliards d'euros, constitué par 1,24 milliards de transactions en ligne (en augmentation de 20,5% par rapport à l'année précédente).

En revanche, le montant moyen des transactions subit un léger recul, à 65,5 euros HT, soit une baisse de 5% par rapport à l'année 2016.

La part du e-commerce dans le marché global est elle aussi en progression, et représente désormais 8,5% des ventes du commerce de détail.

Les produits culturels constituent le premier secteur d'activité du e-commerce (à hauteur de 45% du marché total du e-commerce en France), devant les produits du secteur high-tech (23%) et ceux du secteur maison et électroménager (18%).

Les places de marché représentent près d'un tiers des ventes (29% du volume d'affaires des places de marché, soit une augmentation de 15% depuis 2016).

La consommation collaborative augmente d'année en année.

Enfin, la FEVAD précise que malgré la multiplication des modes de règlement, les paiements sont toujours réalisés très majoritairement par carte bancaire (85%).

S'agissant des ventes B to B, les transactions électroniques représentaient en 2015 14,5% du chiffre d'affaires des entreprises de 10 personnes ou plus implantées en France.

Ces ventes sont réalisées via EDI ou via des sites web B to B.

A rapprocher : Communiqué de presse de la FEVAD du 21 juin 2018

INTERNATIONAL

Directive 95/46 : Interprétation de la notion de responsable de traitement
CJUE, 5 juin 2018, aff. C-210/16

Ce qu'il faut retenir :

L'administrateur d'une plateforme mise en place par un réseau social, opérant un traitement de données en dehors d'un cadre personnel, est un responsable de traitement soumis aux obligations de la directive 95/46 et désormais du Règlement général sur la protection des données.

Pour mémoire :

La directive 95/46/CE du Parlement européen et du Conseil 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 donnée,s constituait le texte de référence en matière de protection des données à caractère personnel.

Cette directive a été abrogée au 25 mai 2018 par le Règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (le « Règlement »).

Pour approfondir :

Une société allemande, Wirtschafttsakademie (« la Société »), spécialisée dans le domaine de l'éducation, assurait la promotion de services de formation au moyen d'une page fan hébergée sur Facebook. En tant qu'administrateur de la page, la Société pouvait obtenir des données statistiques anonymes sur les visiteurs de sa page grâce à une fonction mise à la disposition des administrateurs par Facebook, « Facebook Insight ». Les données étaient collectées grâce à des cookies comportant chacun un code utilisateur unique, actifs pendant deux ans et sauvegardés par Facebook. Le code utilisateur pouvait être mis en relation avec les données de connexion des utilisateurs enregistrés sur Facebook, était collecté et traité au moment de l'ouverture de la page fan.

L'Autorité régionale indépendante de protection des données du Land Schleswig-Holstein en Allemagne (« l'Autorité »), était chargée, par l'article 28 paragraphe 1 de la directive 95/46, de « *surveiller l'application, sur son territoire, des dispositions adoptées par les États membres en application de la présente directive* ». L'Autorité a été saisie et a ordonné à la société de procéder à la désactivation de la page au motif que ni la Société, ni Facebook n'avaient informé les visiteurs de la page que Facebook collectait, à l'aide de cookies, des informations à caractère personnel les concernant et qu'ils traitaient ensuite ces informations.

La Société a contesté cette décision devant le Tribunal administratif allemand en faisant valoir que le traitement des données personnelles effectué par Facebook ne pouvait lui être imputé et qu'elle n'avait pas non plus chargé Facebook de procéder à un traitement de données qu'elle contrôlerait ou qu'elle pourrait influencer. Elle a soutenu que l'Autorité aurait dû agir directement contre Facebook et non contre elle.

Par un arrêt rendu le 9 octobre 2013, le Tribunal administratif a accueilli la demande de la Société. Elle a retenu que l'administrateur d'une page fan sur Facebook n'était pas un organisme responsable.

L'Autorité de protection des données a interjeté appel de cette décision auprès de la Cour administrative fédérale allemande qui a posé deux questions à la Cour de justice afin qu'elle interprète la directive 95/46 sur la protection des données.

Dans un premier temps, la Cour de justice a rappelé que la société américaine Facebook et sa filiale irlandaise Facebook (Facebook Ireland) devaient être regardées comme étant « responsables du traitement » des données à caractère personnel des utilisateurs du réseau social ainsi que celles des visiteurs. Elle a souligné le fait que ces sociétés déterminaient les finalités et les moyens du traitement de ces données à titre principal.

La Cour s'est donc interrogée sur la contribution de la Société quant aux finalités et aux moyens d'un tel traitement.

Elle a noté que l'administrateur de la page fan pouvait demander l'obtention de données démographiques concernant son audience cible, d'informations sur le style de vie et les centres d'intérêt de son audience cible, et de données géographiques afin de cibler au mieux son offre d'information.

Elle a constaté qu'à raison d'un tel ciblage, cet administrateur participait à la détermination des finalités et des moyens du traitement des données personnelles des visiteurs de sa page fan, conjointement avec Facebook Ireland.

De ce fait, la Société a été qualifiée de responsable au sens de de la directive 95/46.

La Cour a jugé que le fait pour un tel administrateur d'utiliser la plateforme mise en place par Facebook ne saurait l'exonérer du respect de ses obligations en matière de protection des données à caractère personnel.

Par cet arrêt, on assiste à un élargissement de la qualification liée à la notion responsable de traitement. Par la reconnaissance d'une responsabilité conjointe, l'objectif premier de la Cour a été « *d'assurer une protection plus complète des droits dont disposent les personnes qui visitent une page fan* ».

Dans un second temps, la Cour a jugé que l'Autorité était compétente pour assurer le respect des règles y afférentes tant à l'égard de la Société que de la société Facebook Germany et ce, même si la société mère ou filiale en charge du traitement demeurent dans un pays tiers ou dans un autre pays de l'Union.

Lorsqu'une entreprise établie en dehors de l'Union (en l'espèce, la société américaine Facebook) détient plusieurs établissements dans différents Etats membres, l'autorité de contrôle d'un Etat membre (en l'espèce, l'Autorité) est habilitée à exercer les pouvoirs que lui confère l'article 28 paragraphe 3 de la directive 95/46, à l'égard d'un établissement de cette entreprise situé sur le territoire de cet Etat membre (en l'espèce, la Société) ; quand bien même cet établissement est chargé uniquement de la vente d'espaces publicitaires et d'autres activités de marketing sur le territoire de l'Etat membre en question et que la responsabilité exclusive de la collecte et du traitement des données personnelles incombe pour l'ensemble du territoire de l'union, à un établissement situé dans un autre Etat membre (en l'espèce, Facebook Ireland).

L'Autorité était compétente pour procéder au contrôle de la légalité d'un tel traitement de données de manière autonome par rapport à l'autorité de l'Irlande. L'Autorité pouvait exercer ses pouvoirs d'intervention à l'égard de la société sans préalablement appeler l'autorité de contrôle de l'Irlande à intervenir.

Cette décision, bien que rendue sous l'empire de la directive 95/46, peut s'inscrire dans la ligne du Règlement général sur la protection des données (« RGPD »). Le RGPD met à la charge de tout Responsable de traitement situé sur le territoire de l'Union Européenne une série d'obligations visant à garantir les droits de l'utilisateur.

Il faut noter que le RGPD n'a pas modifié la définition du responsable de traitement. De ce fait, elle conserve tout son intérêt au regard du nouveau Règlement.

Désormais, tout opérateur susceptible de traiter des données personnelles doit se conformer aux articles 13 et 14 du RGPD qui instaurent une obligation d'information auprès des personnes concernées avant tout traitement de leurs données personnelles. Un tel traitement est subordonné au consentement exprès de la personne. En effet, de telles obligations sont importantes afin d'éviter d'impacter les droits et libertés des personnes physiques (article 35 du RGPD *« analyse d'impact relative à la protection des données »*)

A rapprocher : Règlement Général sur la Protection des Données personnelles

LEGALTECHS / TENDANCES

Nouvelle application pour la blockchain dans le domaine du covoiturage

Partenariat entre l'IRT et la Métropole Lyonnaise

Ce qu'il faut retenir :

Afin de fluidifier le trafic sur l'A6/A7 aux alentours de l'agglomération de Lyon, l'Institut de Recherche Technologique (IRT) implanté sur le Campus Lyon-Tech de la Doua à Villeurbanne, a développé un service utilisant la technologie blockchain dont l'objectif est de mutualiser les différentes plates-formes de covoiturage de la région de Lyon.

Pour approfondir :

En effet, l'axe A6/A7 étant malheureusement souvent impraticable, les autorités locales ont souhaité mettre en place un service de covoiturage fiable en proposant une offre suffisamment conséquente.

En pratique, il s'agira de mettre en place une voie de covoiturage dynamique sur certains tronçons de l'autoroute. Les automobilistes qui font du covoiturage pourront se repérer grâce à une série de signalisations dynamiques leur indiquant que la voie de gauche leur est dédiée ainsi qu'aux taxis, transports en commun, et aux véhicules à faibles émissions notamment.

Le projet démarrera officiellement au début de l'été 2018.

Cette innovation a vu le jour grâce à un partenariat conclu en avril 2018 entre l'Institut de Recherche Technologique (IRT) et la Métropole Lyonnaise, pour une durée de 5 ans.

Cet accord s'inscrit dans un contexte plus global favorisant l'expérimentation de solutions alternatives sur la régulation du trafic routier, notamment en lien avec la future loi d'orientation sur les mobilités.

Voici une nouvelle application de la blockchain, inspirée de ce qui existe déjà dans la Silicon Valley, inspirante et qui, on le souhaite, sera vite déclinée dans les autres grandes agglomérations françaises !

A rapprocher : La Métropole de Lyon noue un partenariat de recherche appliquée avec l'IRT SystemX

ACTUALITÉ NUMÉRIQUE SIMON ASSOCIÉS

LABELLISATION CNIL

SIMON ASSOCIÉS a permis à la start-up française CADRE DE VIE d'obtenir son label CNIL « Gouvernance Informatique et Libertés »

Pour obtenir son label CNIL, la start-up française, experte de la « smart data » dans le secteur de l'immobilier, s'est tournée vers SIMON ASSOCIÉS pour son expertise en protection des données personnelles

En savoir plus

NOUVEAUTE RGPD

SIMON ASSOCIÉS et le Groupe VISIATIV lancent « Mission RGPD »

Pour relever le défi de la conformité à l'entrée en application du Règlement Général pour la Protection des Données (RGPD), VISIATIV et SIMON ASSOCIÉS lancent « Mission RGPD », solution complète et évolutive combinant la puissance d'une plateforme numérique et l'expertise juridique RGPD.

En savoir plus

ÉVENEMENTS MARQUANTS

L'ASEAN : un grand marché tourné vers l'innovation

Colloque organisé par BUSINESS FRANCE - Participation de CRISTELLE ALBARIC, Avocat associée

15 juin 2018 - Paris | Palais du Luxembourg

En savoir plus