SOMMAIRE

PARIS - NANTES
MONTPELLIER - PERPIGNAN

Bureaux intégrés

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

Réseau SIMON Avocats

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

Conventions transnationales

www.simonassocies.com
www.lettredunumerique.com

DATA / DONNÉES PERSONNELLES

Comment transmettre un fichier clients en conformité avec le RGPD dans le cadre d'une cession de fonds de commerce exploité en franchise ?
Conseils pratiques

Ce qu'il faut retenir :

Dans le cadre d'une cession de fonds de commerce, il y a souvent confusion entre cession d'une clientèle et cession d'un fichier clients. Pourtant ces deux termes ne sont pas synonymes (l'un vise la clientèle personnelle rattachée à un fonds de commerce et l'autre adopte une conception plus large et peut viser aussi bien la clientèle personnelle que des prospects ou encore une clientèle rattachée exclusivement au franchiseur).

En tout état de cause, lorsque concomitamment à la cession d'un fonds de commerce un fichier est transmis, dès lors que celui-ci est constitué de données à caractère personnel, cette transmission ne peut se réaliser que sous réserve du respect de la règlementation applicable en matière de protection des données personnelles et plus particulièrement du RGPD.

Pour approfondir :

Lors de la cession d'un fonds de commerce, se pose la question relative aux conditions de transmission et d'exploitation du fichier clients.

Si la cession d'un fonds de commerce suppose la cession de la clientèle attachée au fond, rendre synonymes « clientèle » et « fichier clients » est un raccourci trop rapide.

D'ailleurs, puisque l'existence d'un fonds de commerce suggère nécessairement l'existence d'une clientèle, la confusion de ces deux notions laisserait penser que la formalisation d'un fichier clients est une obligation faute de quoi le fonds n'existerait pas.

En tout état de cause, toute transmission d'un fichier clients dans le cadre d'une cession de fonds de commerce doit être réalisée dans le strict respect de la réglementation applicable en matière de protection des données personnelles.

I. « Clientèle » et « fichier clients »

La « clientèle » n'a pas de définition juridique et les contours de cette notion restent floues ce qui, d'ailleurs, a donné lieu à une abondante jurisprudence sur le sujet.

Des critères jurisprudentiels ont alors été dégagés : la clientèle d'un fonds de commerce suppose que celle-ci soit :

- Commerciale (autrement dit provenir d'une activité commerciale) ;

- Réelle et certaine (en principe la clientèle doit être actuelle et ne devrait, sauf cas particulier, préexister au fonds, elle doit également présenter un caractère stable) ;

- Propre (autrement dit, elle doit regrouper les clients qui se fournissent auprès du commerçant car ils sont attirés par le fonds de commerce en fonction des qualités personnelles du commerçant qui exploite son fonds à risques et périls).

Par ailleurs, sur un plan comptable, la clientèle est une des principales composantes du poste « fonds commercial » et semble davantage désigner un potentiel assuré et valorisable de chiffre d'affaires que la formalisation d'une liste nominative.

A ce titre, n'entreraient donc pas dans la définition de la clientèle :

- Les prospects ;

- Les clients du réseau qui n'auraient réalisé aucun acte d'achat auprès du franchisé. A titre d'illustration, nous pouvons mentionner les clients qui réaliseraient une commande en ligne sur le site du franchiseur et qui sélectionneraient, via l'interface en ligne, le magasin auprès duquel ils souhaitent retirer leur commande ;

- De même les clients préexistants à la naissance du fonds de commerce et affectés à un franchisé suite à la création de son fonds car ils relèveraient de sa zone d'exclusivité ne devraient, en principe, pas relever de la définition de la clientèle.

Un « fichier clients » n'a quant à lui aucune définition ni légale ni jurisprudentielle et n'a au surplus, aucune existence comptable en tant que tel.

Dans un réseau de franchise, il existe une multitude de fichiers clients, lesquels peuvent appartenir au franchisé et/ou au franchiseur sans que cela ne puisse remettre en cause la propriété de la clientèle.

Il y a d'abord les fichiers concernant les clients et prospects des points de vente du réseau constitués par les franchisés et, le cas échéant, les succursales du franchiseur.

Il y a ensuite les fichiers constitués à partir des outils digitaux mis en place par le franchiseur comme par exemple les sites internet et applications mobiles ainsi que les fichiers constitués à partir d'opérations mises en œuvre sous la maitrise du franchiseur comme par exemple des programmes de fidélité.

Enfin et en pratique, tous ces fichiers sont régulièrement centralisés dans un fichier unique tenu et structuré par le franchiseur notamment pour assister ses franchisés, en charge des opérations locales, et promouvoir son réseau à l'échelle nationale.

Si l'on s'intéresse au fichier clients rattaché à un point de vente, celui-ci est composé de plusieurs éléments.

S'il vise généralement des éléments permettant l'identification des personnes constituant la clientèle attachée au point de vente, le fichier a une conception plus large puisqu'il peut, dans certains cas et dans une certaine mesure, intégrer également des éléments permettant d'identifier des clients en partie rattachés au franchiseur et surtout des prospects.

En conséquence, « clientèle » et « fichier clients » ne se confondent pas et font référence à deux notions de nature différentes, qui peuvent être complémentaires. Dans un cas, la notion de « clientèle » renvoie à un élément constitutif du fonds de commerce, dans l'autre cas, la notion de « fichier clients » ne fait pas partie des éléments constitutifs du fonds de commerce et ne représente rien d'autre qu'un document créé à la libre discrétion de son producteur regroupant des éléments brutes permettant d'identifier les membres de la clientèle et de manière générale toute personne ayant entretenu une interaction de quelque nature que ce soit avec le producteur du fichier.

Un fonds de commerce n'existe que lorsqu'une clientèle propre au fonds existe.

Un fichier clients n'existe qu'en raison de la volonté de son producteur et conformément à ce qu'il décide d'y voir apparaitre (les types de données contenues dans le fichier, l'organisation des données au sein du fichier, etc.).

Ces deux notions, sans se contredire, sont régulièrement confondues au point où se pose fréquemment la question de la transmission du fichier clients dans le cadre de la cession d'un fonds de commerce par un franchiseur alors que cette transmission n'est nullement une obligation à moins que cédant et cessionnaire en aient convenu autrement dans les actes de cession.

II. Comment encadrer la transmission d'un fichier

En pratique, un fichier clients va tout de même être transmis dans le cadre d'une cession de fonds de commerce notamment en raison de sa présence dans le matériel cédé.

Toutefois, compte tenu du fait que le fichier contient des données à caractère personnel, la règlementation en matière de protection des données personnelles s'applique.

Tout d'abord, le fichier transmis devra avoir été constitué conformément à la règlementation.

En effet, les choses illicites étant hors commerce, tout manquement pouvant entrainer l'illicéité du fichier (il s'agit principalement des obligations de fonds prévues par le RGPD en matière d'information des personnes concernées, de recueil de consentement ou de justification d'une base légale au traitement des données, de formalités préalables et de respect des principes de finalité, proportionnalité et minimisation) conduirait à la nullité des actes. Par un arrêt du 25 juin 2013 (Cass. com., 25 juin 2013, n°12-17037), la Cour de cassation avait par exemple admis que la vente d'un fichier non déclaré à la CNIL devait être sanctionnée par la nullité en raison de l'illicéité de son objet au visa de l'article 1128 du Code civil et de l'article 22 de la loi du 6 janvier 1978.

Ensuite, dans la mesure où la cession d'un fichier clients a pour conséquence de permettre à un nouveau responsable de traitement de traiter les données des personnes concernées, ces dernières devront :

- Être informées de la cession de leurs données et de l'identité du cessionnaire ;

- Consentir à la cession de leurs données (à moins qu'un intérêt légitime puisse se justifier, auquel cas, les personnes concernées disposent toujours de la faculté de s'opposer à la transmission de leurs données).

Si les contours de l'intérêt légitimes restent flous, le RGPD précise néanmoins que doivent être prise en compte « *les attentes raisonnables des personnes concernées fondées sur leur relation avec le responsable du traitement* ». Le considérant n°47 du RGPD précise également qu'un tel intérêt légitime pourrait, par exemple, se justifier lorsqu'il existe une relation pertinente et appropriée entre la personne concernée et le responsable de traitement.

A contrario, si les personnes concernées ne peuvent raisonnablement s'attendre au traitement ultérieur de leurs données, leurs intérêts et droits fondamentaux pourraient alors prévaloir sur l'intérêt du responsable du traitement.

Au cas particulier, il nous parait plus pertinent que la clientèle personnelle attachée à un fonds de commerce puisse raisonnablement s'attendre à ce que ses données soient traitées par l'exploitant du fonds puis par son cessionnaire contrairement à ce à quoi pourraient s'attendre des prospects et les clients du franchiseur.

Dès lors, pour lever ou tout du moins atténuer les risques de contestation de la part du cessionnaire et des clients, il nous semble approprié d'adopter une démarche prudente consistant, d'une part, à nettoyer le fichier clients pour n'y voir apparaitre que les coordonnées de la clientèle attachée au fonds et, d'autre part, à déterminer les modalités de communication des données de sorte que le cessionnaire soit au courant de l'information préalable des clients avant toute transmission des données et du fait que le fichier clients pourrait ne pas contenir l'ensemble des informations relatives à sa clientèle (cette dernière étant en droit de s'opposer à la cession de ses données).

En tout état de cause, même si le RGPD ne prévoit pas d'obligation de déterminer par écrit les conditions d'intervention de deux responsables de traitement lorsque ces derniers n'agissent pas en qualité de responsables conjoints, il nous semble néanmoins important de prévoir par écrit (et en dehors des actes de cession) les conditions et les délais attachés à la transmission des données ainsi que les engagements pris par chacune des parties afin notamment de s'assurer qu'une telle cession de fichier n'aura pas d'impact sur la réputation et l'image de marque du franchiseur (qu'il soit cessionnaire ou cédant).

A rapprocher : Règlement Général sur la Protection des Données Personnelles n°2016/679 du 27 avril 2016 ; Articles L.141-5 et suivants du Code de commerce

Attention aux systèmes de vidéosurveillance, la CNIL s'en préoccupe particulièrement

Conseils pratiques

Ce qu'il faut retenir :

La CNIL est depuis l'année dernière particulièrement vigilante et soucieuse quant à la conformité des dispositifs de vidéosurveillance sur le lieu de travail et a ainsi multiplié les contrôles, mises en demeures et sanctions.

Ses décisions sont relativement proches car les sociétés commettent systématiquement les mêmes types de manquements : leurs dispositifs de vidéosurveillance sont considérés comme excessifs en raison d'une mise sous surveillance permanente de leurs salariés et de l'absence de toute information préalable.

La clôture de la mise en demeure à l'encontre de l'Institut des techniques informatiques et commerciales (ITIC), le 2 septembre 2019, nous donne l'occasion de rappeler les erreurs à ne plus commettre.

Pour approfondir :

Il y a un an déjà, dans un communiqué de presse du 19 septembre 2018, la CNIL appelait à la tenue d'un débat démocratique sur les nouveaux usages des caméras vidéo.

Partant du constat que de nouveaux outils de captation associés à des technologies particulièrement invasives se développaient très rapidement, la Commission a fait part de son inquiétude et a rappelé l'urgence de prévoir des garde-fous afin d'encadrer ces dispositifs dans le respect d'un juste équilibre entre les impératifs de sécurisation et la préservation des droits et libertés.

Depuis, la CNIL a réalisé de nombreux contrôles pour vérifier la conformité des dispositifs vidéo (souvent oubliés des travaux de mise en conformité au RGPD) et a prononcé plusieurs mises en demeure et sanctions à l'encontre d'entités publiques et privées cette année.
La plus marquante est sans doute la décision de la CNIL, en juin dernier, prise à l'encontre de la société UNIONTRAD COMPANY, laquelle a été condamnée à payer une amende de 20.000 € car son système de vidéosurveillance n'était pas conforme à la réglementation.

Ce qui rend cette décision marquante n'est pas le montant de la sanction mais ce qu'il représente à l'échelle de la société.

Si beaucoup d'opérateurs se sentaient à l'abri d'une sanction notamment en raison de leur taille, du caractère non sensible de leur(s) activité(s), du fait que leur chiffre d'affaires et bénéfices commerciaux étaient relativement bas ou encore du fait qu'ils n'avaient pas de rayonnement important à l'échelle nationale, cette décision est venue remettre en cause cette pensée.

En effet, la société UNIONTRAD COMPANY est une très petite entreprise (TPE) comptant seulement 9 salariés et ayant réalisé l'année précédant le contrôle de son système vidéo un résultat net négatif de 110.844 €.

Même si la Commission avait tenu compte de la situation économique de la société, une sanction pécuniaire d'un montant représentant plus de 2 % de son chiffre d'affaires lui était tout de même infligée.

Plusieurs autres entités ont fait face aux contrôles de la CNIL. Toutes sans exception ont fait l'objet de mise en demeure ou de sanction pour les mêmes raisons à savoir principalement :

- La mise sous surveillance constante de leurs salariés ;
- Le défaut d'information.

Nous constatons tout de même que les dernières mises en demeure publiques prononcées par la CNIL ont été clôturées sans le prononcé d'une sanction dès lors que les sociétés avaient cessé les manquements qui leur étaient reprochés.

A titre d'illustration, le 2 septembre 2019, la CNIL a prononcé la clôture de la mise en demeure à l'encontre de l'Institut des techniques informatiques et commerciales (ITIC).

Cela nous donne l'occasion de rappeler comment s'assurer de la conformité de son système de vidéosurveillance. Des caméras peuvent être installées sur un lieu de travail à des fins de sécurité des biens et des personnes, à titre dissuasif ou pour identifier les auteurs de vols, de dégradations ou d'agressions à condition que la mise en œuvre du dispositif respecte les principes fondamentaux de la protection des données (principe de finalité, principe de proportionnalité et principe de minimisation).

A ce titre, avant toute mise en œuvre d'un dispositif vidéo sur un lieu de travail (espaces privés non ouvert au public), il est important de s'assurer du respect, *a minima,* des règles suivantes :

- Les caméras ne peuvent avoir pour effet de filmer des employés sur leur poste de travail de manière continue et permanente, **sauf circonstances particulières**. Il faut donc bien choisir l'emplacement et le nombre de caméras à installer et se limiter à une installation des caméras dans des zones qui échappent à la surveillance humaine ou la rendent difficile comme par exemple les entrées et sorties des bâtiments, les issues de secours et les voies de circulation.

- L'orientation de chaque caméra du dispositif de vidéosurveillance doit être particulièrement réfléchie de sorte que les caméras ne puissent filmer que des zones de « risques » et sans porter atteinte à la vie privée des salariés. Ainsi, les caméras peuvent filmer les zones où de la marchandise ou des biens de valeur sont entreposés, mais aucun lieu de vie, espace personnel, espace de pause ou locaux syndicaux ne doivent entrer dans leur champ de vision. De plus, lorsque des caméras sont installées dans des salles où des postes de travail existent, il convient d'orienter les caméras sur les marchandises et/ou machines uniquement et non sur les bureaux/postes de travail.

- Les finalités poursuivies via l'installation d'un tel dispositif doivent être légitimes. Lorsque le seul but recherché est de veiller à la sécurité du personnel et des biens dans la mesure où les caméras ont un effet dissuasif en permettant de prévenir les incidents de sécurité (agressions, vols, dégradation) mais également probatoires car en cas d'incident, les images pourront être transmises aux autorités compétentes et des mesures pourront être prises à l'encontre d'auteurs d'infractions, la légitimité du dispositif est rarement remise en cause.

  Toutefois, dès lors qu'on souhaite affecter d'autres finalités à son dispositif, la CNIL se montre plus stricte.

- Les instances représentatives du personnel doivent être informées et consultées avant toute mise en route d'un tel système.

- Les salariés - et de manière générale l'ensemble des personnes concernées - doivent être informés de l'existence du dispositif.
  Cette information est généralement délivrée en deux temps. D'abord via des panneaux d'information affichées de manière visible dans les locaux et à l'entrée des zones filmées, puis via une information individuelle de chaque salarié via une note de service, une disposition du contrat de travail ou encore du règlement intérieur.

- Les images enregistrées ne peuvent être conservées, en règle générale, que quelques jours, sauf circonstances exceptionnelles (comme par exemple effectuer les vérifications nécessaires en cas d'incident, suivi et enclenchement d'éventuelles procédures disciplinaires ou pénales).
  Si des procédures sont engagées alors les images doivent être extraites du dispositif afin d'être conservées isolément pour la durée de la procédure.

- Dans les limites de leurs attributions, peuvent seules avoir accès aux images filmées, les personnes habilitées par l'employeur, comme par exemple un(e) responsable de la sécurité. La CNIL insiste sur le fait que ces personnes doivent être formées et sensibilisées aux règles à respecter. Par ailleurs, l'accès aux images doit être particulièrement sécurisé pour éviter que tout le monde ne puisse les visionner.

A rapprocher : Règlement Général sur la Protection des Données Personnelles n°2016/679 du 27 avril 2016 ; Décision de la CNIL du 2 septembre 2019 portant clôture de la mise en demeure n°2018-024 du 2 juillet 2018 à l'encontre de l'établissement ITIC ; Délibération de la formation restreinte n°SAN-2019-006 du 13 juin 2019 prononçant une sanction à l'encontre de la société UNIONTRAD COMPANY

PROPRIÉTÉ INTELLECTUELLE

Cas de résiliation d'une licence de marque
CA Paris, 18 octobre 2019, RG n°18/19572

Ce qu'il faut retenir :

Le cessionnaire de marques est substitué au cédant dans ses droits et obligations au titre du contrat de licence précédemment conclu et peut opposer au licencié sa défaillance contractuelle.

Pour approfondir :

Dans cette affaire, s'opposaient le cessionnaire de marques et des contrats de licence sur celles-ci au licencié qui avait conclu avec le précédent titulaire des marques un contrat de licence l'autorisant à fabriquer et commercialiser des chaussures revêtues des marques en cause. Postérieurement à la cession, un conflit opposa le nouveau titulaire des marques au licencié conduisant le concédant à résilier le contrat et solliciter le paiement de redevances échues outre une indemnisation.

Le licencié a contesté la qualité pour agir du cessionnaire des marques estimant que les formalités d'inscription de la cession des marques au registre national (**article L.714-7 du Code de la propriété intellectuelle** : « *Toute transmission ou modification des droits attachés à une marque doit, pour être opposable aux tiers, être inscrite au Registre national des marques* »), n'ayant pas été accomplies, la cession lui était inopposable. En outre, il faisait également valoir le fait que la transmission du contrat de licence à son bénéfice nécessitait son accord de sorte que les droits invoqués tirés du contrat de licence lui étaient inopposables.

La cour ne va pas suivre cette argumentation et estimer, au contraire, que le cessionnaire des marques a qualité pour agir.

Les juges considèrent que les formalités prévues à l'article L.714-7 du Code de la propriété intellectuelle sont destinées à informer les tiers et à leur rendre la cession de marque opposable mais n'est pas applicable dans les rapports entre le cessionnaire de la marque et son contractant étant ici précisé qu'à la date de l'assignation l'inscription de la cession des marques avait finalement été opérée. Les juges relèvent également que le fait qu'un contrat de licence a été conclu en considération de la personne du cocontractant ne fait pas obstacle à ce que les droits et obligations de ce dernier soient transférés à un tiers dès lors que l'autre partie y a consenti de façon non équivoque ce qui ressortait des faits de l'espèce en particulier des nombreux échanges intervenus entre les parties.

Dans un second temps, après avoir admis la recevabilité de l'action, la cour va conclure au bien-fondé de celle-ci. Les juges vont à cet égard se pencher sur la mise en œuvre de la clause résolutoire prévoyant, assez classiquement, qu'en cas de faute grave par l'une des parties, l'autre pourra résilier le contrat. La faute du licencié ressortait ici des difficultés prises lors de la réalisation de la collection PE 2015 dont il était démontré qu'elle était exclusivement imputable au licencié ce qui justifiait donc la mise en œuvre de la clause résolutoire. En conséquence, la cour alloue une indemnisation évaluée sur la base des minimas contractuels garantis.

A rapprocher : Article L.714-7 du Code de la propriété intellectuelle

---

Annulation de la marque semi-figurative vente-privee.com jugée frauduleuse
TGI Paris, 3 octobre 2019

Ce qu'il faut retenir :

La marque vente-privee.com vient de connaître un nouvel assaut judiciaire aboutissant au prononcé de la nullité de la marque semi-figurative sur le terrain de la fraude.

Pour approfondir :

Nouvelle avancée dans l'affaire opposant Vente-privee.com à Showroomprive.com concernant la validité de la marque Vente-privee.com. On se souvient que ce conflit avait conduit la Cour de cassation à se prononcer le **6 décembre 2016** pour admettre la validité de la marque verbale Vente-privee.com estimant que celle-ci avait acquis par l'usage un caractère distinctif au regard des services de promotion des ventes pour le compte des tiers et de présentation de produits sur tout moyen de communication pour la vente au détail ainsi que des services de regroupement pour le compte de tiers de produits et de services, notamment sur un site web marchand.

La société Showroomprive.com a mené un nouvel assaut judiciaire ciblant cette fois la marque semi-figurative Vente-privee.com se présentant sous forme d'une dénomination en lettres minuscules noir et du dessin d'un papillon rose au bout de la ligne.

Le tribunal va, dans un premier temps, reconnaître la validité de la marque puis, dans un second temps, annuler cette marque dont il juge que le dépôt est frauduleux.

- Sur le caractère distinctif du signe :

Selon l'article L.711-2 du Code de la propriété intellectuelle :

« *Le caractère distinctif d'un signe de nature à constituer une marque s'apprécie à l'égard des produits ou services désignés.*
Sont dépourvus de caractère distinctif :

a) *Les signes ou dénominations qui, dans le langage courant ou professionnel, sont exclusivement la désignation nécessaire, générique ou usuelle du produit ou du service ;*
b) *Les signes ou dénominations pouvant servir à désigner une caractéristique du produit ou du service, et notamment l'espèce, la qualité, la quantité, la destination, la valeur, la provenance géographique, l'époque de la production du bien ou de la prestation de service ;*
c) *Les signes constitués exclusivement par la forme imposée par la nature ou la fonction du produit, ou conférant à ce dernier sa valeur substantielle.*

Le caractère distinctif peut, sauf dans le cas prévu au c, être acquis par l'usage. »

Selon les juges, le signe dont l'élément verbal apparaît dominant et sera lu par le consommateur moyen comme si le terme « privee » comportait un accent (« privée »), constitue la désignation usuelle du service consistant à proposer à la vente, lors d'événements d'une durée limitée et à un public restreint, des produits de marques en nombre limité et à très bas prix, issus d'opérations de déstockage. Toutefois, toujours selon les juges, en dépit de l'absence de caractère distinctif *ab initio*, ce signe a pu acquérir un tel caractère par l'usage qui en a été fait. Le jugement retient, en particulier, la position de leader sur le secteur des ventes événementielles, l'intensivité de l'usage (compensant la brève durée puisque la marque en cause a été déposée en 2013), un sondage plaçant la marque au rang de la 5ème marque la plus connue de l'e-commerce, les multiples revues de presse établissant les efforts pour faire connaître la marque.

La marque, dont le caractère distinctif acquis par l'usage est reconnu, va néanmoins être invalidée sur le terrain de la fraude. Cette notion est expressément visée par le Code de la propriété intellectuelle en son article L.712-6 qui permet à la victime de la fraude d'exercer une action en revendication. Le droit commun trouve également à s'appliquer en la matière et l'application de l'adage « *fraus omnia corrumpit* » peut conduire à annuler un dépôt de marque frauduleux, c'est ce fondement qui était en l'espèce visé. Selon le jugement, l'expression « vente privée » a toujours désigné des ventes événementielles, à un public d'invités, de déstockage des invendus, la société Vente-privee.com a adapté ce modèle à la vente en ligne mais « *pour autant, elle ne saurait s'approprier des termes génériques qui doivent rester disponibles pour tous les acteurs économiques de ce secteur et n'a aucune légitimité à monopoliser à son seul profit les termes "vente-privee", extrêmement proches de "vente privée", à titre de marque et à priver ses concurrents de l'usage de ces mots sauf à introduire une distorsion dans les règles de libre concurrence* ». Également, les juges caractérisent l'intention frauduleuse du fait de la connaissance du caractère générique et des intentions d'appropriation de ce terme en dépit de ce caractère sur la base de déclarations faites par son dirigeant.

On imagine que ce jugement est le premier temps d'un long parcours judiciaire et que la cour d'appel aura prochainement à se prononcer sur la position adoptée par les juges de première instance relativement à l'existence, ou non, d'un dépôt frauduleux.

A rapprocher : Articles L.711-2, L.714-3 et L.712-6 du Code de la propriété intellectuelle ; Cass. com., 6 décembre 2016, n°15-19.048

SERVICES NUMÉRIQUES

La CJUE donne des précisions sur la portée du droit au déréférencement

CJUE, 24 septembre 2019, aff. C-136/17 et C-507/17

Ce qu'il faut retenir :

Par deux arrêts du 24 septembre 2019, la Cour de justice de l'Union européenne délivre des précisions quant à la portée géographique du droit au déréférencement et quant à son effectivité lorsqu'il porte sur des catégories particulières de données.

Pour approfondir :

Le droit au déréférencement, consacré par l'arrêt Google Spain du 13 mai 2014 (affaire C-131/12), est le droit pour toute personne de demander à un moteur de recherche la suppression de certains résultats provenant de recherches effectuées à partir de son nom.

Par ces deux arrêts, la Cour de justice de l'Union européenne donne des indications sur la portée du droit au déréférencement et notamment sur sa portée géographique (affaire C-507/17).

En effet, dans cette première affaire, la Haute juridiction limite les conséquences du déréférencement aux seuls résultats de recherches effectuées au sein de l'Union européenne.

Dès lors, à la suite d'un déréférencement, les résultats litigieux resteront accessibles pour toute recherche effectuée hors Union européenne : le déréférencement n'est donc plus mondial mais limité au territoire européen.

La Cour considère en effet qu'il ne ressort aucunement des textes législatifs et règlementaires européens, que la portée du droit au déréférencement « *dépasserait le territoire des Etats membres* ».

La CJUE précise « *que, en l'état actuel, il n'existe pour l'exploitant d'un moteur de recherche qui fait droit à une demande de déréférencement formulée par la personne concernée […] pas d'obligation découlant du droit de l'Union de procéder à un tel déréférencement sur l'ensemble des versions de son moteur* ».

Il est toutefois indiqué que les autorités de contrôle disposent, d'une part, du droit de mettre en balance les droits de la personne concernée au respect de sa vie privée et à la protection de ses données à caractère personnel et, d'autre part, le droit à la liberté d'information. Ainsi, aux termes de cette mise en balance, une autorité telle que la CNIL pourra parfaitement enjoindre l'exploitant de procéder à un déréférencement mondial si cela est justifié.

Dans la seconde affaire (affaire C-136/17), la Cour de justice de l'Union européenne apporte des précisions quant au déréférencement de résultats de moteurs de recherche contenant des données sensibles ou catégories particulières de données au sens du RGPD.

La CJUE rappelle que l'exploitant d'un moteur de recherche doit être qualifié de responsable de traitement et porte donc la responsabilité « *non pas du fait que des données à caractère personnel visées par lesdites dispositions figurent sur une page web publiée par un tiers, mais du référencement de cette page et, tout particulièrement, de l'affichage du lien vers celle-ci dans la liste des résultats présentée aux internautes à la suite d'une recherche effectuée à partir du nom d'une personne physique.* »

Il est précisé que la mise en œuvre du droit au déréférencement doit être précédée d'une mise en balance entre la gravité de l'ingérence dans les droits fondamentaux de la personne concernée et le droit à l'information des internautes.

Enfin, la CJUE précise que les informations relatives à une procédure judiciaire passée, ainsi que celles relatives à la condamnation subie, constituent des données sensibles devant faire l'objet d'un déréférencement par l'exploitant du moteur de recherche lorsque celles-ci ne correspondent plus à la situation actuelle. Dès lors, dans ces circonstances, les droits fondamentaux de la personne concernée prévalent sur le droit à l'information des potentiels internautes intéressés.

A rapprocher : CJUE, 24 septembre 2019, aff. C-136/17 et C-507/17

Les médias et éditeurs français, un village gaulois entré en résistance face aux géants du net

Actualités

Ce qu'il faut retenir :

La Directive sur le droit d'auteur et le droit voisin à l'ère numérique, qui vise à rétablir un équilibre entre auteurs de contenu et géants du numérique en créant un internet régulé, se heurte au blocage de Google, qui refuse de l'appliquer.

Pour approfondir :

« *Nous sommes en 50 avant Jésus-Christ. Toute la Gaule est occupée par les Romains… Toute ? Non. Un village peuplé d'irréductibles Gaulois résiste encore et toujours et à l'envahisseur…* ».

Aujourd'hui, les irréductibles sont les médias et les éditeurs français qui ont décidé de rentrer en résistance contre les GAFAM et notamment contre Google en déposant plainte à son encontre. L'Alliance de la presse d'information générale (APIG) a annoncé, le 24 octobre 2019, le dépôt de plaintes auprès de l'Autorité de la concurrence pour dénoncer un abus de position dominante du leader mondial de la recherche en ligne. Les médias français espèrent ainsi forcer Google à négocier le droit voisin instauré par la loi du 23 juillet, qui leur donne la possibilité de s'entendre sur une rémunération pour la reprise d'extraits de leurs articles – ce que l'entreprise américaine refuse.

Mais comment en est-on arrivé là ?

Après avoir protégé ses citoyens en adoptant Le Règlement Général sur la Protection des Données en avril 2016 avec une entrée en vigueur en mai 2018, l'Europe entend protéger ses médias et ses artistes en approuvant le 26 mars 2019 la Directive sur le droit d'auteur et le droit voisin à l'ère numérique.

Très attendu par les médias et les artistes, ce texte vise à rétablir un équilibre entre auteurs de contenu et géants du numérique en créant un internet régulé, "à l'européenne" où les plateformes rémunèrent mieux les créateurs. Un vote important obtenu de haute lutte face aux plateformes américaines et aux partisans de la liberté du net. Les États-membres disposent de deux ans pour transposer la directive dans leur droit national.

L'objectif de la directive est de permettre aux créateurs de contenus de percevoir une plus grande partie des revenus générés par la diffusion de leurs productions et œuvres sur internet. Les sommes en jeu sont colossales et les grandes plateformes américaines l'ont bien compris : « *La création artistique européenne, son poids économique, équivaut à 536 milliards d'euros chaque année, c'est 7 200 000 emplois* », expliquait Jean-Marie Cavada, eurodéputé et fervent soutien de la réforme sur France Inter, l'ancien journaliste d'ironiser en ces termes : « *alors je comprends qu'ils [les GAFAM] se comportent comme des terroristes 'Pac-man', qu'ils veuillent manger cet argent et qu'ils ne veuillent pas payer* ».

Le nouveau partage du revenu des œuvres sera introduit par deux articles :

- L'article 15 (ancien article 11),
- L'article 17 (ancien article 13).

L'article 15 prévoit que les plateformes en ligne rémunèrent les éditeurs de presse dont elles utilisent les contenus (comme Google Actualités) : ce droit sera valable pendant deux ans après la publication d'un article de presse.

L'article 17 concerne les plateformes qui autorisent leurs utilisateurs à publier du contenu par eux-mêmes (comme YouTube ou Facebook) : la directive leur impose de conclure des accords avec les auteurs et de filtrer les œuvres qui sont publiées (le cas échéant, d'empêcher la publication d'œuvres protégées).

Le Parlement français a transposé la directive en droit français à la quasi-unanimité le 23 juillet dernier pour une entrée en vigueur il y a un mois le 24 octobre 2019.

Ce texte tant attendu risque d'être vidé de toute portée avant même sa mise en œuvre.

La directive se heurte au blocage de Google, qui refuse de l'appliquer. L'entreprise américaine a demandé aux éditeurs de renoncer à ce nouveau droit s'ils souhaitent que leurs contenus demeurent visibles sur le moteur de recherche (titre, chapeau, photo, extrait vidéo).

Ainsi comme le titrait le journal Le Monde : « *Google a offert aux médias un cynique choix de dupes* ». Soit les médias signent un blanc-seing à Google en renonçant à toute rémunération pour conserver le modèle actuel basé sur la gratuité. Une mort lente. Soit les médias refusent de signer les nouvelles conditions de Google, et obtenir une juste rémunération. Google promet en représailles que la visibilité de leurs contenus soit réduite à sa plus simple expression. Plus de photo, plus de textes, un bout de titre, rien de plus, apparaîtra quand les internautes feront des recherches sur une information. Un suicide pour la presse française.

C'est pourquoi à ce jour, aucun grand média n'a refusé, de peur de voir son audience s'effondrer, mais la contre-attaque a débuté.

La première manifestation de cette résistance sera la tribune signée par 800 journalistes et personnalités médiatiques qui a été publiée le 23 octobre dans la presse européenne (Le Parisien, en France), réclamant aux pouvoirs publics une contre-attaque face à Google.

> « *Nous appelons à une contre-attaque des décideurs publics. Ils doivent muscler les textes pour que Google ne puisse plus les détourner, utiliser tout l'arsenal des mesures qui permettent de lutter contre l'abus de position dominante.*
> *De notre côté, nous, journalistes, photographes, JRI et artistes en appelons à l'opinion publique et mènerons ce combat car ce qui est en cause, c'est la survie de médias indépendants et pluralistes, et in fine la vitalité de notre démocratie.* »

Suite à cette tribune, le gouvernement français en a appelé à une décision européenne coordonnée.

L'acte fort de cette contre-attaque sera le dépôt de la plainte de l'Alliance de la presse d'information générale (APIG) qui regroupe 305 journaux français. Pour marquer les esprits, l'APIG a déposé cette plainte le 24 octobre 2019 date d'entrée en vigueur de la loi transposant la Directive.

Les plaignants demandent à l'Autorité de la concurrence de prendre des « mesures conservatoires » :

- Ordonner à Google de proposer une offre tarifaire pour la reprise des contenus,

- Désigner un expert de l'Autorité sous l'égide duquel la négociation se mènera,

- Fixer un délai de négociation de trois mois, et

- Imposer que le prix s'applique de façon rétroactive à partir du 24 octobre, date d'entrée en vigueur de la loi.

La bataille n'est pas que juridique, elle est aussi politique et le débat va intégrer Facebook qui a fait savoir elle aussi qu'elle n'entendait pas plus que Google payer de droits voisins.

A suivre…

A rapprocher : Loi n°2019-775 du 24 juillet 2019 tendant à créer un droit voisin au profit des agences de presse et des éditeurs de presse

---

Sites internet et cookies : pas de consentement en cas de case cochée par défaut
CJUE, 1er octobre 2019, aff. C-673/17

Si le RGPD suggère fermement que la validité du consentement d'une personne relève d'une action positive de sa part, la règlementation antérieure ne faisait nullement référence à cet acte. Dès lors et concernant spécifiquement les cookies déposés sur le terminal d'un internaute à l'occasion de sa navigation sur un site internet, de nombreux éditeurs de sites et de cookies ont profité d'un flou juridique pour mettre en place des mécanismes de consentement peu contraignant et facilitant la collecte d'information.

Ce qu'il faut retenir :

La CJUE confirme que le consentement d'un internaute au dépôt de cookies sur son équipement ne saurait être valable s'il résulte d'une case cochée par défaut qu'il convient de décocher si l'internaute refuse ces cookies.

En outre, la validité de ce consentement dépend également de l'information qui est délivrée à l'internaute et qui doit notamment inclure la durée des cookies ainsi que les tiers qui peuvent y avoir accès.

Pour approfondir :

Dans un arrêt du 1er octobre 2019 de la CJUE, la Cour est revenue sur les conditions à respecter pour le dépôt de cookies lors de la navigation sur un site internet. En l'espèce, la société allemande PLANET49 a organisé un jeu concours sur internet. Le site internet via lequel les internautes pouvaient participer prévoyait notamment une case à cocher qui prévoyait par défaut l'acceptation de l'internaute au dépôt de cookies par PLANET49 lui permettant notamment d'exploiter les navigations sur le web et les visites de l'internaute sur les sites web des partenaires publicitaires et d'adresser de la publicité centrée sur leurs intérêts.

Après mise en demeure restée infructueuse, la fédération des organisations et associations de consommateurs a introduit devant le tribunal régional de Francfort-sur-le-Main un recours contre PLANET49 afin que cette dernière cesse la mise en place d'un accord par défaut au dépôt de cookies. Après que le tribunal régional ait fait droit partiellement à la demande de la fédération et que la société allemande ait interjeté appel de cette décision, l'affaire a été portée devant la Cour fédérale de justice.

La Cour fédérale de justice allemande a saisi la CJUE de plusieurs questions préjudicielles en interprétation des dispositions applicables en matière de consentement et d'information préalable au dépôt de cookies prévues par la directive 2002/58 du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et de la directive 95/46.

Il est à noter que la directive 95/46 a été abrogée par le Règlement général sur la protection des données personnelles n°216/679 (RGPD), toutefois les faits de cette affaire et la saisie de la CJUE sont antérieurs à l'abrogation de ladite directive et à l'adoption du RGPD.

La CJUE a donc notamment dû répondre aux questions préjudicielles suivantes :

1. Le consentement tel que visé par ces dispositions est-il valablement donné lorsqu'il résulte d'une case cochée par défaut que l'utilisateur doit décocher pour refuser de donner son consentement ?

2. L'information préalable qui doit être délivrée à l'internaute doit-elle inclure la durée de fonctionnement des cookies ainsi que la possibilité ou non pour des tiers d'avoir accès à ces cookies ?

➢ **S'agissant de la première question préjudicielle relative au consentement**

Pour répondre à cette question, la Cour a d'abord relevé que les dispositions applicables prévoient expressément que l'utilisateur doit avoir « donné son accord » au placement et à la consultation de cookies sur son équipement sans préciser de quelle manière cet accord doit être donné. La Cour a néanmoins précisé qu'il ressortait du considérant 17 de la directive 2002/58 que le consentement d'un utilisateur peut être donné selon toute modalité appropriée permettant à l'utilisateur d'indiquer ses souhaits librement, de manière spécifique et informée, notamment « en cochant une case lorsqu'il visite un site Internet ».

La Cour en a conclu que dès lors que le consentement, tel que prévu par la directive de 2002, avait la même définition que celle prévue par la directive 95/46, à savoir « *toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement* », il n'est pas possible de déterminer si un internaute a véritablement donné son accord en ne décochant pas une case cochée par défaut ainsi que, en tout état de cause, si ce consentement a été donné de manière informée. En effet, la Cour avance que le fait de ne pas décocher une telle case peut résulter de l'inattention de l'internaute qui n'aurait pas lu l'information accompagnant la case cochée par défaut, voire qu'il n'aurait pas aperçu cette case, avant de poursuivre son activité sur le site Internet qu'il visite.

En conséquence, la CJUE a répondu à la question préjudicielle qui lui était posée que le consentement d'un internaute n'est pas valablement donné lorsqu'il est autorisé au moyen d'une case cochée par défaut que cet utilisateur doit décocher pour refuser de donner son consentement.

➢ **S'agissant de la deuxième question préjudicielle relative à l'information préalable**

La Cour relève tout d'abord que l'article 10 de la directive 95/46, à laquelle fait référence l'article 5, paragraphe 3, de la directive 2002/58, ainsi que l'article 13 du règlement 2016/679 énoncent les informations qu'un responsable du traitement doit fournir à la personne auprès de laquelle il collecte des données à caractère personnel.

Ces informations comprennent « au moins » :

- L'identité du responsable du traitement ;
- Les finalités du traitement ;
- Toute information supplémentaire (dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont collectées, ces informations supplémentaires sont nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données) telle que :
    - Les destinataires ou les catégories de destinataires des données,
    - Le fait de savoir si la réponse aux questions est obligatoire ou facultative ainsi que les conséquences éventuelles d'un défaut de réponse,
    - L'existence d'un droit d'accès aux données et de rectification de ces données.

A la lecture de cet article, l'identité des tiers qui peuvent avoir accès aux cookies est explicitement visée dans l'information devant être délivrée à l'internaute puisque les destinataires sont inclus dans la liste dudit article.

Quant à la durée du traitement des données, celle-ci ne figure pas parmi ces informations. Néanmoins, la liste figurant à l'article 10 de la directive 95/46 n'est pas exhaustive, l'expression « au moins » ayant été utilisée par le législateur européen.

La Cour a retenu que la durée de fonctionnement des cookies doit être considérée comme répondant à l'exigence d'un traitement loyal des données dans une situation telle que celle en l'espèce puisqu'une durée longue, voire illimitée, implique la collecte de nombreuses informations sur les habitudes de navigation et la fréquence des visites éventuelles de l'internaute sur les sites des partenaires publicitaires de PLANET49.

En conséquence, qu'il s'agisse de pratiques antérieures ou postérieures à l'entrée en application du RGPD, qui pose un cadre strict et explicite en matière de consentement et d'information, le consentement nécessaire à un éditeur avant dépôt de ses cookies ne doit pas résulter d'une case cochée par défaut et être accompagné d'une information claire et complète précisant notamment la durée de validité de ces cookies et des tiers pouvant y avoir accès.

Cet arrêt s'inscrit dans un mouvement de renforcement du consentement des internautes.

En effet, alors qu'un règlement « vie privée et communications électroniques » (qui abrogera la directive 2002/58) est actuellement en discussion au niveau européen, la CNIL a publié, en juillet dernier, de nouvelles lignes directrices rappelant les règles de droit applicables en matière d'expression du consentement sur internet tenant compte des dispositions du RGPD. Ces lignes directrices remplacent sa recommandation « Cookie » de 2013. La Commission annonce également la publication prochaine d'une nouvelle recommandation durant le premier trimestre 2020 qui précisera les modalités de recueil du consentement au dépôt des cookies et qui complètera sa délibération de juillet dernier.

Pour l'heure, et en synthèse, la CNIL recommande aux éditeurs de :

- Prévoir un consentement via un acte positif qui ne peut résulter d'une case pré-cochée ou de l'acceptation globale de conditions générales d'utilisation ;

- Prévoir un consentement pour chaque finalité de traitement. Dès lors, si un éditeur a recours à plusieurs types de cookies aux finalités différentes comme par exemple, des cookies publicitaires et des cookies de mesure d'audience, il devra solliciter un accord pour chacune de ces finalités. En conséquence, l'acceptation globale de tous les cookies n'est pas envisageable, à moins que la possibilité d'accepter ou refuser chacune des finalités soit offerte aux internautes ;

- Prévoir une information complète, visible, et mise en évidence au moment du recueil du consentement, rédigée en des termes simples et accessibles. Il convient donc de bannir toute documentation trop complexe, rédigée en des termes trop juridiques. De plus, si une information complète suggère beaucoup de mentions obligatoires, *a minima* dans un premier niveau, les mentions suivantes devront être portées à la connaissance de l'internaute :

    - L'identité du ou des responsables de traitement ;

    - La finalité des opérations de lecture ou écriture des données ;

    - L'existence du droit de retirer son consentement.

A rapprocher : Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) ; 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) ; Délibération n°2019-093 du 4 juillet 2019 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture ou écriture dans le terminal d'un utilisateur (notamment aux cookies et autres traceurs)

E-COMMERCE

Condamnation pour pratiques commerciales trompeuses en raison d'un référencement de pharmacies d'un réseau concurrent dans son annuaire

CA Versailles, 14ème ch., 7 novembre 2019, *Pharmarket / Elsie groupe, Pharmacie Chabrol, et autres*

Ce qu'il faut retenir :

La cour d'appel de Versailles a confirmé l'ordonnance de référé condamnant la société Pharmarket en raison de pratiques commerciales trompeuses. En référençant des pharmacies concurrentes dans son annuaire, Pharmarket a créé une confusion dans l'esprit du consommateur qui pouvait penser que toutes les pharmacies référencées appartenaient au réseau Pharmarket.

Pour approfondir :

La société Pharmarket édite le site internet www.pharmarket.com, qui se présente comme le premier réseau de pharmacies et de parapharmacies en ligne. Ce site – qui référence, dans son « annuaire des pharmacies françaises », près de 22 000 officines – permet aux internautes de commander des produits directement auprès d'officines partenaires.

La société Elsie Groupe et les pharmacies de son réseau ont constaté apparaître dans l'annuaire du site de Pharmarket alors qu'elles n'y ont jamais consenti. Elles ont alors notamment reproché à Pharmarket d'entretenir à travers cet annuaire une confusion dans l'esprit du consommateur qui pourrait penser que toutes les officines référencées appartiennent au réseau Pharmarket.

Après avoir mis en demeure la société Pharmarket de cesser de les référencer sur son site www.pharmarket.com, la société Elsie Groupe et les pharmacies de son réseau concernées l'ont assignée en référé afin d'obtenir leur déréférencement.

Les pratiques de Pharmarket ont été considérées comme caractérisant un trouble manifestement illicite par le juge des référés. Elle a alors été condamnée par le président du tribunal de commerce de Nanterre, sous astreinte de 250 euros par jour de retard, à retirer de son site internet toute référence ou mention à la société Elsie Groupe et aux pharmacies de de son réseau.

Pharmarket a alors interjeté appel de l'ordonnance de référé estimant que le trouble manifestement illicite et les pratiques prétendument déloyales qui lui ont été reprochés n'étaient pas établis.

Elle a alors notamment soutenu devant la cour d'appel de Versailles que son site internet et plus particulièrement son annuaire n'étaient pas susceptibles d'induire le consommateur en erreur dans la mesure où celui-ci est systématiquement informé et mis en mesure d'effectuer la distinction entre les pharmacies partenaires de Pharmarket et celles qui ne le sont pas.

Suivant constat d'huissier, la cour a retenu que le site internet de Pharmarket présentait l'annuaire comme celui « des pharmacies Pharmarket ». Dès lors, il n'était pas contestable pour la cour que le consommateur est trompé quant à l'appartenance au réseau Pharmarket de toutes les pharmacies figurant dans son annuaire et qu'il est incité à poursuivre sa recherche pour procéder à un achat en ligne puisqu'il peut penser que toutes les officines figurant dans l'annuaire offrent le service de vente en ligne.

De plus, toujours selon constat d'huissier, la cour a relevé qu'une recherche sur le moteur Google à partir de mots clés se rapportant à l'enseigne d'une des pharmacies du réseau Elsie Santé donnait pour premier résultat l'annuaire du site « Pharmarket ».

Lorsqu'un consommateur clique sur ce lien, il a accès au catalogue des produits vendus. Ce n'est qu'en fin de recherche qu'il est informé que la vente en ligne n'est pas disponible pour ladite pharmacie via le message d'alerte suivant : « *La Pharmacie est présente dans notre annuaire des pharmacies françaises mais n'est pas partenaire de Pharmarket. Il n'est donc pas possible de passer commande en ligne auprès de cette pharmacie. Tous les produits affichés dans le catalogue de produits Pharmarket sont proposés et vendus par d'autres pharmacies françaises partenaires* ».

La cour d'appel de Versailles en a alors déduit que grâce à son annuaire incluant des pharmacies concurrentes à celles de son réseau, Pharmarket capte les recherches des internautes vers son site internet puisque la présentation qui en est faite (y compris via l'utilisation de logos et icônes) laissent à penser que la pharmacie recherchée par l'internaute appartient au réseau de vente en ligne Pharmarket.

En outre, même si le consommateur est finalement informé en fin de recherche, la cour d'appel a considéré qu'en référençant sur son annuaire des pharmacies concurrentes, Pharmarket « *a favorisé le renvoi des consommateurs vers son propre site marchand à partir des moteurs de recherche, les trompant par les premières mentions figurant sur son site sur l'appartenance desdites officines à son propre réseau pour ensuite les inciter à s'orienter vers des pharmacies partenaires grâce notamment aux annonces publicitaires de produits et aux liens vers son catalogue de vente en ligne qui figurent sur les pages de son annuaire* ».

En application des articles L.121-1 et L.121-2 du Code de la consommation, ces procédés constituent des pratiques commerciales trompeuses et déloyales dès lors que Pharmarket « *crée une confusion entre son réseau de pharmacies en ligne et celui du groupe Elsie et induit ainsi en erreur le consommateur moyen tout en le conduisant à prendre une décision commerciale qu'il n'aurait pas prise autrement, en l'incitant à finalement procéder à son achat auprès de ses pharmacies partenaires dont elle présente les produits* ».

En conséquence, la cour d'appel a confirmé l'ordonnance de référé en raison de l'existence d'un trouble manifestement illicite caractérisé.

A rapprocher : Articles L.121-1 et L.121-2 du Code de la consommation

INTERNATIONAL

La loi sur la cryptographie en Chine
Loi du 26 octobre 2019 - entrée en vigueur le 1er janvier 2020

Ce qu'il faut retenir :

L'Assemblée populaire nationale (parlement chinois), lors d'une réunion du Comité permanent (13ème Congrès, 14ème réunion), a adopté le 26 octobre 2019 une nouvelle loi sur la cryptographie, laquelle entrera en vigueur le 1er janvier 2020 (la « Loi »). Le pays s'apprête à lancer sa propre monnaie numérique.

Pour mémoire :

De manière générale, la cryptographie est une technique d'écriture qui consiste à rédiger un message crypté, via l'utilisation de codes secrets ou de clés de décryptage.

La cryptographie est principalement utilisée pour protéger un message jugé confidentiel.

La cryptographie est une des disciplines de la cryptologie s'attachant à protéger des messages en s'aidant souvent de secrets ou clés.

Avant l'adoption de la Loi, Xi Jinping, président de la République populaire de Chine et secrétaire général du Parti communiste chinois, a déclaré, le 24 octobre 2019, que le pays doit « *saisir l'opportunité* » offerte par la technologie de la blockchain en tant que noyau de l'innovation, en s'exprimant, dans le cadre de la 18ème étude collective du Bureau politique du Comité permanent (« **Etude collective** »).

La technologie de la blockchain a un large éventail d'applications en Chine, allant du financement des entreprises au transport en commun et à la lutte contre la pauvreté.

Pour approfondir :

L'un des objectifs de la Loi est de faciliter le développement du secteur de la cryptographie et d'assurer la sécurité du cyberespace et de l'information.

L'État encourage et soutient la recherche et l'application de la science et de la technologie en cryptographie et garantit la confidentialité (**Art 9**).

La Loi garantit les droits de propriété intellectuelle, et permet l'attribution des contributions exceptionnelles (**Art 9**).
La Loi prévoit de différencier les types de cryptographie, et relève trois grands domaines : le domaine « principal », « commun » et « commercial » (**Art 6**). Si les deux premiers sont censés couvrir des informations confidentielles, et doivent être exclusivement gérés par les autorités, le dernier sert à la protection d'informations qui ne sont pas des secrets d'État, et peuvent être utilisées par les citoyens (**Art 7 & 8**).

En vertu de la Loi, la nouvelle autorité dénommée « Agence centrale de cryptographie » sera en charge du contrôle des acteurs du marché de la cryptographie (**Art 16**).

La Loi vise à normaliser l'application et la gestion des mots de passe. En outre, elle contribue (i) à promouvoir le développement de l'industrie des mots de passe, (ii) à assurer la sécurité des réseaux et de l'information et (iii) à améliorer le niveau scientifique, normalisé et légalisé de la gestion des mots de passe (**Art 21**).

Le problème de la responsabilité juridique est également abordé, en cas de piratage ou d'utilisation des données pour se livrer à des activités illégales (**Art 32 – 41**).

Il s'agit donc d'établir une politique nationale autour de l'utilisation de la cryptographie, et par ce biais, celle de la cryptomonnaie.

Le président Xi a indiqué lors de la publication de la Loi : « *la Chine doit considérer la blockchain comme une percée importante pour l'innovation indépendante des technologies de base. La Chine doit clarifier l'orientation principale, accroître les investissements, nous concentrer sur un certain nombre de technologies clés et accélérer le développement de la technologie de la blockchain et l'innovation industrielle* ».

C'est précisément **sur cette base qu'est développée la monnaie numérique créée en Chine, et qui sera émise par la banque centrale**. Cette nouvelle cryptomonnaie offrirait d'ailleurs quelques points de comparaison avec Libra, la monnaie virtuelle de Facebook, puisqu'elle pourrait être utilisée sur des plateformes majeures chinoises telles que WeChat ou Alipay.

Avec ce nouveau texte, la Chine se dote d'un cadre juridique bien des années après la France, laquelle s'est intéressée à la cryptologie dès 2004 avec la loi pour la confiance dans l'économie numérique, n°2004-575 du 21 juin 2004 (abrégée sous le sigle LCEN, qui est une loi française sur le droit de l'Internet, transposant la directive européenne 2000/31/CE du 8 juin 2000 sur le commerce électronique et certaines dispositions de la directive du 12 juillet 2002 sur la protection de la vie privée dans le secteur des communications électroniques).

Pour mémoire, en France, les moyens de cryptologie (science du secret englobant la cryptographie — l'écriture secrète – et la cryptanalyse – l'analyse de cette dernière) sont soumis à une règlementation spécifique.

L'utilisation d'un moyen de cryptologie est libre et il n'y a aucune démarche à accomplir.

En revanche, la fourniture, l'importation, le transfert intracommunautaire et l'exportation d'un moyen de cryptologie sont soumis, sauf exception, à déclaration ou à demande d'autorisation.

Ces démarches incombent au fournisseur du moyen de cryptologie et sont à accomplir auprès de l'ANSSI (l'agence (française) nationale de la sécurité des systèmes d'information). Le régime applicable (déclaration ou demande d'autorisation) dépend des fonctionnalités techniques du moyen et de l'opération commerciale projetée (fourniture, importation…).

Les textes en la matière en France sont :

- Articles 30 à 36 de la loi n°2004-575 du 21 juin 2004
- Décret 2007-663 du 2 mai 2007
- Arrêté du 29 janvier 2015

A rapprocher : Le texte de loi en chinois

***