



****** Lettre d'information Domainoo JANVIER 2021 ******
Toute l'actualité sur les noms de domaine

Bonjour à tous,

Puisqu'il est encore temps, nous vous présentons nos meilleurs vœux pour cette nouvelle année, ainsi qu'à vos proches et collaborateurs. Nous espérons que vous allez bien, et que la crise que nous traversons ne vous affecte pas trop, tant professionnellement que personnellement.

Dans le monde des noms de domaine, l'année 2020 devait être une année marquante au niveau de la prochaine vague de Nouvelles Extensions, avec un début de calendrier et des informations sur le guide du candidat. Pour autant, l'ICANN ne semble avoir prévu de nouvelles entrées d'argent en lien avec cette activité que dans son budget 2024 !

Chez Domainoo, l'année 2020 a été particulière à bien des égards : nous avons notamment passé le cap des 20 ans, grâce à vous, mais n'avons pas pu célébrer cet anniversaire comme nous l'aurions voulu. Nous vous remercions sincèrement pour votre fidélité, et espérons que l'année 2021 nous permettra enfin de vous retrouver, pour des réunions physiques et autres moments de convivialités !

Enfin, le contexte sanitaire nous a fait évoluer vers du télétravail généralisé jusqu'à nouvel ordre. Nous avons tout de même pu assurer tous les services habituels et continuer le développement de nouveaux outils et l'amélioration de nos process. Nous pourrions notamment présenter cette année aux équipes techniques notre outil d'audit de zone, notre outil de surveillance d'activation a terminé sa phase d'essai, et la sécurité des accès à notre interface a encore été renforcée avec la mise en place, si vous le souhaitez, d'alertes de notification pour toute connexion à votre compte.

L'équipe Domainoo vous invite à prendre connaissance, dans cette lettre d'actualité, des dernières évolutions en matière de noms de domaine !

Au sommaire de ce numéro :

ACTUALITE DES NOMS DE DOMAINE

I ACTUALITE DES EXTENSIONS CLASSIQUES

- **BREXIT ET .FR**
- **LE .LU S'AGRANDIT GRACE AUX NOMS COURTS**
- **.COM.AU : DURCISSEMENT DES REGLES**
- **RENOUVELLEMENT DES NOMS DE DOMAINE EN .XXX EN 2021**

II ACTUALITE DES NOUVELLES EXTENSIONS

- **LES CLAIMS NOTICE DE LA TMCH INCLUENT DESORMAIS LE .COM**
- **OUVERTURE ATTENDUE DES (ANCIENNES) EXTENSIONS DE L'OREAL : .BEAUTY, .HAIR, .SKIN ET MAKEUP, MAIS AUSSI DU .QUEST**
- **OUVERTURE DU .FORUM**
- **ABANDON ET REVOCATION DE DOTBRANDS**
- **2EME EDITION DU CERCLE DES .MARQUES AVEC L'AFNIC**

III BREVES

- **CLASSEMENT DES EXTENSIONS POUR L'ANNEE 2020**
- **PARTENARIAT ET AIDE AUX PME**
- **CERTIFICATS SSL : DUREE DE VIE LIMITEE A 1 AN**
- **DNSSEC : TOUS LES GTLDS SECURISES**
- **UNE NOUVELLE FORME D'ARNAQUE A L'AGENDA**
- **L'OMPI ENREGISTRE SA 50 000E PLAINTTE POUR CYBERSQUATTAGE**

ACTUALITE JURIDIQUE

I POINT DE DEPART DU DELAI DE PRESCRIPTION DANS LA CNDRP : LE REJET DE LA DATE D'ENREGISTREMENT DU NOM DE DOMAINE AU PROFIT DE LA DATE DE SURVENANCE D'UN FAIT NOUVEAU

II LA NECESSITE DE PROMOUVOIR LA MARQUE SUR LAQUELLE SE FONDE LA PLAINTTE

III QUEL SERA L'IMPACT DU DSA DANS LA LUTTE CONTRE LA CONTREFAÇON EN LIGNE ?

Les informations fournies dans le cadre de cette lettre d'information ne peuvent en aucun cas être considérées comme un conseil quelconque et doivent être vérifiées ou confirmées par des personnes habilitées avant d'être utilisées

ACTUALITE DES NOMS DE DOMAINE

I ACTUALITE DES EXTENSIONS CLASSIQUES

- **BREXIT ET .FR**

Tout comme nous l'avions présenté pour le .EU, depuis le 1er janvier dernier, les résidents du Royaume-Uni ne sont plus éligibles au .FR ainsi qu'à l'ensemble des extensions gérées par l'Afnic. En effet, peuvent demander l'enregistrement ou le renouvellement d'un nom de domaine, dans chacun des domaines de premier niveau, toutes personnes physiques résidant et toutes personnes morales ayant leur siège ou établissement principal :

- sur le territoire de l'un des états membres de l'Union Européenne ;
- sur le territoire des pays suivants : Islande, Liechtenstein, Norvège, Suisse.

Le Royaume-Uni n'étant plus membre de l'Union Européenne, ses résidents ne sont plus éligibles. Cela concerne les résidents d'Angleterre, d'Écosse, du Pays de Galles mais aussi d'Irlande du nord.

Pour autant, la Charte de nommage de l'Afnic prévoit que l'application de nouvelles règles ne peut pas avoir d'effet rétroactif, sauf cas exceptionnels. Ainsi, et cela concerne environ 34 000 noms de domaine en .FR enregistrés avant le 1er janvier 2021, ces titulaires résidant au Royaume-Uni conservent leur nom de domaine et peuvent continuer à en bénéficier sans faire de changement de propriété.

- **LE .LU S'AGRANDIT GRACE AUX NOMS COURTS**

Depuis mardi 15 décembre 2020, et après 15 semaines d'ouverture progressive et 20 années d'indisponibilité, les noms de domaine en .LU en 1 et 2 caractères sont autorisés. Cela représente environ 2400 noms de domaine.

La protection des noms à 1 ou 2 caractères, pour des raisons de sécurité et de clarté, reste cependant encore la norme.

- **.COM.AU : DURCISSEMENT DES REGLES**

A partir du 12 avril 2021, **tout nom de domaine enregistré sur la base d'une marque Australienne devra être enregistré à l'identique de la marque.** Et contrairement au .FR, la Charte de nommage australienne a un effet rétroactif !

Cela impactera donc tout nom de domaine existant enregistré sur la base d'une marque locale mais à l'approchant de la marque. Il faudra donc, pour maintenir ses noms de domaine actifs, changer la base de l'enregistrement et utiliser une présence locale.

Le Registre donne l'exemple de la marque *A Pretty Horse Carousels*. Avec celle-ci, vous pourrez prétendre uniquement au nom *aprettyhorsecarousels.com.au*, mais pas aux noms *phc.com.au*, *carousels.net.au*, *aprettyhorse.com.au*, ou encore *horsecarousels.com.au* comme cela était toléré auparavant.

Nous sommes à votre disposition pour faire l'inventaire de vos .COM.AU et modifier la base de leurs enregistrements lorsque cela sera nécessaire.

- **RENOUVELLEMENT DES NOMS DE DOMAINE EN .XXX EN 2021**

En décembre prochain, vous aurez à renouveler vos noms en .XXX déposés il y a 10 ans à titre défensif sur la base de vos marques (Sunrise B). A ce moment-là, le renouvellement à proprement parler ne sera pas possible et vos noms se transformeront automatiquement en Adultblock.

Peu d'entre vous se sont déjà positionnés sur les services Adultblock et Adultblock+, très coûteux et donc souvent privilégiés pour les marques principales. Nous surveillons donc auprès du Registre les promotions à venir pour permettre à la majorité d'entre vous de pouvoir faire évoluer votre protection vers ces services, ou pour être en capacité de couvrir même vos marques secondaires.

Pour rappel, les services Adultblock et Adultblock+ permettent aux détenteurs d'une marque inscrite à la TMCH ou déposée en .XXX en Sunrise B de bloquer tout enregistrement à l'identique ou à l'approchant sous les extensions pour adultes : .SEX, .PORN, .ADULT et .XXX.

II ACTUALITE DES NOUVELLES EXTENSIONS

- **LES CLAIMS NOTICE DE LA TMCH INCLUENT DESORMAIS LE .COM**

Si vous avez une marque inscrite à la TMCH, vous bénéficiez de mini rapports de surveillance, appelés « Claim Notices » qui listent l'ensemble des noms, contenant votre marque, enregistrés sous de nouvelles extensions depuis le précédent rapport. Domainoo vous propose depuis le début la compilation de ces résultats et leur intégration dans vos rapports de veille classique.

Sachez que la TMCH vient d'intégrer d'office à ses Claims Notices les noms enregistrés en .COM. Pour ceux d'entre vous qui n'ont pas de veille classique chez Domainoo, nous ajouterons donc très bientôt les .COM aux résultats qui vous sont présentés chaque mois. Tout cela vous sera présenté dans le cadre de la rétrospective de vos veilles menée en Mars prochain.

- **OUVERTURE ATTENDUE DES (ANCIENNES) EXTENSIONS DE L'OREAL : .BEAUTY, .HAIR, .SKIN ET MAKEUP, MAIS AUSSI DU .QUEST**

Les nouvelles extensions .MAKEUP, .BEAUTY, .SKIN, et .HAIR avaient à l'origine été demandées par L'Oréal mais ont depuis été revendues à un Registre généraliste, en charge entre autres des .XYZ, .CARS, .SECURITY etc.

Pour les .SKIN, .BEAUTY, et .HAIR, le process habituel est respecté avec un Sunrise dédiée aux marques inscrites à la TMCH jusqu'au 5 février 2021 (mais à un tarif très élevé), une Landursh avec ouverture à tous et prix dégressif sur une semaine, puis une Ouverture Générale le 2 mars 2021, sur la base du 1^{er} arrivé, 1^{er} servi, à un tarif proche d'une extension générique classique.

Pour le .MAKEUP en revanche, il s'agit d'une réouverture dans la mesure où le précédent Registre avait déjà lancé sa Sunrise (en interne). Le nouveau Registre a donc joué avec les possibilités qui

s'offraient à lui pour proposer les mêmes conditions d'ouverture que pour les autres extensions, à la différence que la phase de lancement n'est pas réellement une Sunrise et ne permet donc pas aux marques inscrites à la TMCH d'être prioritaires.

Le prix élevé dissuade nombre d'entre vous de profiter de leur droit prioritaire lors de la Sunrise. Et le tarif abordable de l'ouverture générale laisse présager un niveau élevé de cybersquattage opportuniste. Il est donc assez difficile de se positionner sur la meilleure stratégie de pré-commande, et il est encore plus difficile d'anticiper l'avenir de telles extensions : apporteront-elles une réelle valeur ajoutée dans le domaine de la Beauté sur Internet ? Ou seront-elles polluées et dévaluées du fait d'un trop fort taux de cybersquattage ?

Parallèlement, le Registre XYZ relance sur le même schéma l'extension .QUEST, destinée aux experts et spécialistes dans tous les domaines.

- **OUVERTURE DU .FORUM**

Le .FORUM a terminé sa phase de Sunrise et n'offre pas de phase de Landrush. Il sera ouvert à tous le 2 mars prochain, sans condition spécifique. Cette extension pourra être dédiée aux espaces d'échange, comme son étymologie y invite.

N'hésitez pas à nous contacter si cette extension vous intéresse.

- **ABANDON ET REVOCATION DE DOTBRANDS (OU « .MARQUE »)**

Régulièrement, de grandes marques se séparent de l'extension qu'elles avaient décidé de lancer dans le cadre de la libéralisation des extensions en 2012. L'explication à leur décision, en plus du budget conséquent nécessaire à obtenir et maintenir une extension, se trouve dans leurs courriers adressés à l'ICANN. Toutes ces marques ou presque ont en effet utilisé la même lettre type, exprimant une raison claire : « *The only domain name registered in the .brand, nic.brand, is registered to and maintained by XXX, theRegistryOperator, for its exclusive use.* »

Motivées ou fortement incitées à se défendre par leurs conseils face aux dangers potentiels de l'ouverture des dotBrands, nombre d'entre elles ont enregistré leur propre TLD dans le seul but de se protéger. Les mécanismes de protection étaient pourtant suffisamment nombreux et accessibles.

D'autre part, le 27 juin 2020, l'ICANN a révoqué le dotBrand .AIGO. La société chinoise Aigo Digital Technology Co,Ltd, fabricant de produits électroniques, avait obtenu l'accord d'exploitation de cette extension en 2016. A cette époque, la société répondait à toutes les exigences des dossiers de candidatures mais a vite montré des signes de faiblesse en n'honorant pas les factures ou en ne respectant pas les mentions légales liées au statut de Registre. L'ICANN a déclenché la procédure de révocation sans que la société AIGO ne daigne prendre parti aux débats ou ne tente de défendre son extension.

- **2EME EDITION DU CERCLE DES .MARQUE AVEC L'AFNIC**

Le 5 novembre dernier, vous avez encore été nombreux à participer au 2^{ème} rendez-vous du Cercle des .MARQUE ou à manifester votre intérêt pour le futur volet d'ouverture de Nouvelles extensions.

A noter que le calendrier prévu à ce stade a été communiqué par le Brand Registry Group lors de l'ICANN Hambourg qui s'est tenu du 17 au 22 octobre dernier. Il prévoit une validation du guide de candidature mi-2022 pour un dépôt des candidatures fin 2022. Toutefois, comme nous le disions plus tôt dans cette Newsletter, l'ICANN n'intègre des entrées financières liées aux nouveaux gTlds que dans son budget de 2024.

Rien n'est donc fixé mais la période actuelle peut être propice aux réflexions sur votre présence digitale ; n'hésitez pas à nous solliciter. Et nous pouvons relayer vos réflexions auprès de l'Afnic afin que les sujets qui vous intéressent soient traités lors du prochain rendez-vous du Cercle.

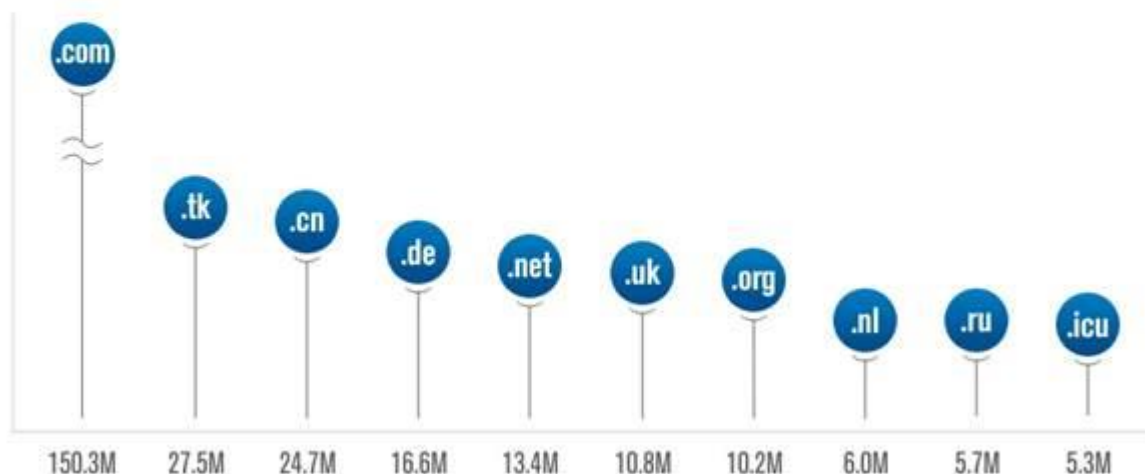
III BREVES

- **CLASSEMENT DES EXTENSIONS POUR L'ANNEE 2020**

Au 30 septembre 2020, plus de 370,7 millions de noms de domaine ont été enregistrés dans le monde, ce qui représente une augmentation de 3% sur une année. Les extensions .COM et .NET totalisent à elles seules 163,7 millions de noms de domaine, ce qui représente 6,3 millions de noms de domaine de plus qu'en 2019. Concernant les extensions nationales, le .TK pour les îles Tokelau (mais surtout gratuit) très prisé des cybersquatteurs devance le .CN avec plus de 27 millions de noms de domaine.

Top 10 Largest TLDs by Number of Reported Domain Names

Source: ZookNIC, Q3 2020; Verisign, Q3 2020; Centralized Zone Data Service, Q3 2020



Source Verisign – Données au 30/09/2020

Les Nouvelles extensions représentent 30,2 millions de noms de domaine, soit 8% du nombre total de noms de domaine déposés toutes extensions confondues. Le .ICU, qui représente 17,7% des Nouvelles extensions, a détrôné le .TOP, passé au 3^{ème} rang, après le XYZ avec 9,4%. Viennent ensuite les .SITE, .ONLINE, .WANG, .CLUB, .VIP, .APP et .SHOP.

A noter qu'au milieu des extensions géographiques appelées ccTlds (.DE, .FR, .US etc), les Nouvelles extensions géographiques percent lentement. En effet, elles représentent 1,3% des noms de domaine, et le .TOKYO est de loin le plus représenté. Le .PARIS représente quant à lui 2,6% des Nouvelles extensions géographiques.

- **PARTENARIAT ET AIDE AUX PME**

ePro Shopping, partenaire de Domainoo depuis de nombreuses années pour ses noms de domaine, propose une solution e-commerce très simple, dédiée aux commerçants, artisans, et TPE/PME, pour leur passage à l'e-commerce.

Pour soutenir les commerçants dans la crise sanitaire, ePro Shopping, en partenariat avec Domainoo et l'Afnic, a pu offrir à ses clients un nom de domaine en .FR pendant près de deux mois lors du 1^{er} confinement. L'opération a été reconduite au moment du 2^{ème} confinement et ePro Shopping a également accompagné les commerçants à mettre en place leur site de prise de commande avec livraison locale ou retrait en drive, permettant ainsi de continuer en partie leur activité, tout en s'adaptant aux protocoles sanitaires.

- **CERTIFICATS SSL : DUREE DE VIE LIMITEE A 1 AN**

Apple, Mozilla, Microsoft et Google ont modifié leur politique sur les certificats SSL/TLS. Ainsi, depuis le 1er septembre 2020, les autorités de certification SSL ne délivrent plus de certificats de plus d'1 an. Nous vous avons accompagné dans cette transformation et vous proposons dans l'interface Domainoo un espace dédié à vos certificats, y compris ceux qui ne sont pas émis par nos partenaires ; vous pouvez ainsi bénéficier d'une vision consolidée de votre portefeuille de certificats et ne pas passer à côté de vos échéances.

- **DNSSEC : TOUS LES gTLDs SECURISES**

L'ICANN a annoncé le 23 décembre dernier que l'ensemble des 1 195 domaines génériques de premier niveau (gTLD) ont déployé les extensions de sécurité du système des noms de domaine (DNSSEC). Après la signature de la zone de .AERO, 100% des gTLDs sont désormais signés DNSSEC. C'est une étape importante dans la mesure où tous les opérateurs gTLDs peuvent désormais proposer aux titulaires de noms de domaine la possibilité d'activer les DNSSEC. L'ICANN continuera à proposer la signature DNSSEC de leurs zones aux domaines de premier niveau géographiques qui ne l'ont pas encore fait. Elle encouragera aussi les opérateurs de résolveurs DNS (qui vérifient les signatures DNSSEC pour contrôler que les données n'ont pas été modifiées) à activer la validation DNSSEC.

Si vous souhaitez être accompagnés dans votre réflexion sur la mise en place du DNSSEC sur vos noms de domaine, n'hésitez pas à nous contacter.

- **UNE NOUVELLE FORME D'ARNAQUE S'ATTAQUE A L'AGENDA**

Nous vous l'avions dit dans notre dernière Newsletter : le contexte actuel, avec l'avènement du télétravail, n'a fait qu'encourager les pratiques malveillantes sur Internet. Parmi elles, une technique redoutable s'attaque aux agendas partagés. Elle existe a priori depuis plusieurs années, mais connaît une augmentation significative ces derniers temps.

Votre agenda n'a pas les filtres anti-spam dont bénéficie votre service de courrier électronique. Les spammeurs ont ainsi trouvé un moyen d'exploiter cette faille. Une invitation à une « réunion » vous est adressée à l'aide des outils collaboratifs intégrés dans Google Calendar, iCloud ou autres outils de planification en ligne. Par défaut, ces services ajoutent l'événement à votre agenda, que vous l'ayez accepté ou non. Ainsi, que ce soit pour rencontrer des célibataires de votre région ou pour une réunion « importante », le rendez-vous est inscrit dans votre agenda, sans intervention de votre part. Il y a tout de même de fortes chances que vous ne voyiez pas l'invitation du tout : Gmail, par exemple, peut automatiquement placer l'invitation dans votre dossier spam, mais Google Agenda traite toujours l'invitation, ce qui peut conduire à une mystérieuse notification sur votre téléphone, par exemple.

Les spécialistes de la cybersécurité et des antivirus travaillent donc sur l'amélioration des outils à ce niveau. Si la plupart du temps vous avez peu de risques de voir ces notifications ou de tomber dans le piège, la technique s'améliore puisque ZDNet note quelques autres utilisations néfastes, comme un spammeur qui a ciblé les employés d'une entreprise spécifique et a mystifié l'invitation pour qu'elle apparaisse comme si elle venait du CEO.

- **L'OMPI ENREGISTRE SA 50 000^{ème} PLAINTÉ POUR CYBERSQUATTAGE**

Le 30 novembre dernier, le Centre d'arbitrage et de médiation de l'OMPI a indiqué dans un communiqué de presse avoir enregistré sa 50 000^{ème} plainte UDRP pour cybersquattage. Depuis 20 ans, l'OMPI a ainsi enregistré des plaintes sur près de 91 000 noms de domaine, impliquant des parties de plus de 180 pays. Les principes directeurs de l'UDRP s'appliquent à tous les gTlds et à de nombreux ccTlds (.CH, .IO) ou servent de base à certains Registres pour leur propre procédure de résolution des litiges.

Par ailleurs, la pandémie de COVID-19 a entraîné une recrudescence du nombre de litiges pour cybersquattage, renforçant d'autant le nombre record de plaintes déposées auprès de l'OMPI en 2020 : de janvier à octobre, le Centre a traité 3 405 plaintes, soit une augmentation de 11% par rapport à la même période en 2019.

S'agissant de l'augmentation du nombre de plaintes déposées auprès de l'OMPI, Erik Wilbers, directeur du Centre d'arbitrage et de médiation de l'OMPI, a déclaré : « Avec un nombre croissant de personnes passant davantage de temps en ligne durant la pandémie, les cybersquatteurs trouvent un environnement

qui leur est de plus en plus favorable. Dans le même temps, les titulaires de droits augmentent la protection de leurs marques sur Internet à mesure qu'ils intensifient la commercialisation et la vente en ligne ».

ACTUALITE JURIDIQUE

I POINT DE DEPART DU DELAI DE PRESCRIPTION DANS LA CNDRP : LE REJET DE LA DATE D'ENREGISTREMENT DU NOM DE DOMAINE AU PROFIT DE LA DATE DE SURVENANCE D'UN FAIT NOUVEAU

PAR EMMANUEL GILLET, IP TWINS, LE 12 DECEMBRE 2020

Contrairement aux autres règlements pour la résolution extrajudiciaire des litiges relatifs aux noms de domaine, l'article 2 de la cnDRP pose un délai pour agir. Or imposer un tel délai, fondé exclusivement sur la date d'enregistrement du nom de domaine, n'est pas souhaitable :

« 197. Le Rapport intérimaire de l'OMPI recommandait de ne pas imposer de délai de forclusion pour l'engagement de procédures concernant des noms de domaine (par exemple déclarer irrecevables les plaintes déposées à l'encontre d'un enregistrement qui n'a pas été contesté dans un certain délai). Il a été considéré qu'une telle mesure ne tiendrait pas compte du fait que l'utilisation déterminante d'un nom de domaine peut évoluer avec le temps (la conséquence étant que cette utilisation peut porter atteinte à des droits par exemple par l'offre à la vente de produits différents de ceux qui étaient précédemment proposés sur le site Web), du fait que tout droit de propriété intellectuelle connexe détenu par le détenteur du nom de domaine peut s'éteindre et que la forclusion ne serait pas souhaitable dans tous les cas où des parties sont de mauvaise foi. (...)

199. Il n'est pas recommandé de soumettre à des délais le dépôt de plaintes dans le cadre de la procédure administrative » (OMPI, Rapport final concernant le processus de consultations de l'OMPI sur les noms de domaine de l'Internet. La gestion des noms de domaine de l'Internet. Questions de propriété intellectuelle, 30 avril 1999, paras. 197 et 199).

Imposer un délai pour agir reviendrait, en effet, à méconnaître ou ignorer les tactiques des cybersquatteurs. L'hypothèse est celle d'un nom de domaine dont l'utilisation ne présente aucune menace apparente jusqu'à l'expiration du délai pour agir. Par exemple, il suffit d'imaginer un nom de domaine similaire ou identique à une marque, mais dont l'utilisation, délibérément éloignée de tout risque de confusion, laisse croire que son titulaire dispose d'un droit ou intérêt légitime irréfutable. Dans de telles circonstances, toute plainte cnDRP serait vouée à l'échec. En réalité, le contenu du site peut n'être rien d'autre que de la poudre aux yeux. Le cybersquatteur est un investisseur. Il est patient et conscient qu'en l'absence de procédure extrajudiciaire et expéditive disponible, la valeur du nom de domaine décuplera du jour au lendemain. Il lui suffit, par exemple, de modifier le contenu du site de manière à générer un risque de confusion et à proposer de céder le nom de domaine contre le paiement d'une « rançon ». Or, malgré l'apparition de faits nouveaux démontrant, de manière quasi-irréfragable, la mauvaise foi du cybersquatteur, le propriétaire de la marque est démuni puisque le délai pour agir a expiré. La victime, désarmée car privée de recours, est placée, à son grand désarroi, dans une situation de déni de justice. Enfin, le seul recours possible étant la négociation, le cybersquatteur se trouve en position de force pour exiger le tribut qui lui paraît le plus approprié en fonction de l'espèce.

Au fond, en fixant la date d'enregistrement du nom de domaine comme unique point de départ du délai de prescription, l'article 2 de la cnDRP aboutit à une double peine : absence de recours extrajudiciaire expéditif

et augmentation de la valeur du nom de domaine. Certes, l'annulation du contrat de cession pourrait être envisagée ultérieurement. En effet, on pourrait considérer que ce contrat est vicié compte tenu de la contrainte exercée par le cybersquatteur sur le propriétaire de la marque. Toutefois, cela reviendrait à additionner des difficultés que l'on pourrait éviter en apportant une simple modification à la lettre de l'article 2 de la cNDRP. Pour remédier à cette situation inéquitable, pour peu que l'on s'obstine à conserver un délai pour agir, il suffirait de fixer le point de départ de la prescription à la date de survenance d'un fait nouveau.

II LA NECESSITE DE PROMOUVOIR LA MARQUE SUR LAQUELLE SE FONDE LA PLAINTÉ

PAR CABINET DREYFUS, LE 25 NOVEMBRE 2020

Au sujet de : *OMPI, centre d'arbitrage et de médiation, 22 juillet 2020, Affaire D2020-1383, Natixis Intertitres c. Super Privacy Service LTD c/o Dynadot / Fredrik Lindgrent*

Être titulaire d'une marque identique au nom de domaine contre lequel on agit est un bel atout dans le cadre d'une procédure UDRP. Mais encore faut-il en démontrer la connaissance par le défendeur. Entreprise difficile lorsque la marque en question n'est pas mise en valeur.

Natixis, dont la renommée est internationale, détient une filiale, Natixis Intertitres, titulaire de marques sur le signe « INTERTITRES ». Cette filiale a déposé une plainte UDRP en vue d'obtenir le transfert du nom <intertitres.com>, réservé par un tiers sans autorisation.

Dans le cadre de la procédure, l'anonymat du réservataire a été levé, pour révéler un titulaire en Suède.

Le requérant estime que le nom a été enregistré en référence à sa marque et non pour la définition générique du terme « intertitres » car, en langue française, le terme est généralement employé au singulier et est défini sous cette forme dans les dictionnaires. En outre, le requérant trouve « suspicieux » le paramétrage de serveurs de messagerie sur un nom de domaine qui ne renvoie vers aucun site. Ainsi, d'après Natixis Intertitres, l'objectif du défendeur serait de tirer parti de la réputation du requérant et de sa marque.

Le défendeur n'a pas formellement répondu à la plainte mais a précisé avoir réservé le nom de domaine afin de créer un site en rapport avec la littérature.

L'expert en charge de ce litige reconnaît le risque de confusion entre la marque et le nom de domaine postérieur, tout comme l'absence de preuve d'intérêt légitime par le défendeur, celui-ci n'ayant pas véritablement expliqué le choix de ce nom de domaine.

En revanche, l'expert est plus mitigé sur la question de mauvaise foi. Il avance notamment deux points importants.

En premier lieu, rien ne démontre que le réservataire, basé en Suède, avait connaissance de la marque « INTERTITRES ». Natixis est certes connue à l'échelle internationale, mais ce n'est pas le cas de sa marque « INTERTITRES » qui désigne des chèques déjeuners, principalement

disponibles en France. Ces chèques déjeuners sont plutôt commercialisés sous les noms « CHEQUE DE TABLE » ou « APETIZ ». Dès lors, il est improbable que le défendeur ait eu connaissance de cette marque.

En second lieu, « INTERTTTRES » est surtout un terme générique. Le fait que les définitions fournies dans les dictionnaires soient au singulier ne signifie pas que le terme n'existe pas dans sa forme plurielle.

La plainte est donc rejetée.

Il est essentiel, pour les titulaires de droits, d'être attentif au champ de rayonnement de leur marque. La marque est-elle suffisamment connue dans le pays du réservataire pour que l'on puisse raisonnablement penser qu'il l'avait à l'esprit lors de la réservation du nom ? Cette question doit faire l'objet d'une étude minutieuse, d'autant plus quand la marque a également une signification dans le langage courant et que le nom de domaine en cause n'est pas exploité pour une activité proche de celle de la marque. A cet égard, l'expert a justement rappelé qu'utiliser un nom principalement afin de disposer d'une messagerie n'est pas prohibé.

III QUEL SERA L'IMPACT DU DSA DANS LA LUTTE CONTRE LA CONTREFAÇON EN LIGNE ?

PAR EVE RENAUD-CHOURAQUI, HAAS AVOCATS, LE 11 JANVIER 2021

On vous en parle depuis longtemps, le voile a enfin été levé sur les tant attendus **Digital Services Act (DSA)** et **Digital Market Act (DMA)**.

Pour mémoire :

- le **DSA** vise à obliger les plateformes, réseaux sociaux et intermédiaires en ligne à **limiter les contenus illicites et à renforcer la transparence sur le fonctionnement de leurs algorithmes**;
- le **DMA**, quant à lui, a pour objectif **de lutter contre les comportements abusifs des plateformes numériques structurantes**, considérées comme des « gatekeepers ».

Dans le cadre de cet article, concentrons-nous sur le DSA et plus particulièrement sur son **impact sur la lutte contre la contrefaçon**.

1. Enjeux

Les **plateformes** sont, en l'état actuel du droit, **assimilées à des hébergeurs de contenus** dont la **responsabilité est limitée**. Ce régime a été **créé par la Directive E-commerce de 2000**. La responsabilité de l'hébergeur n'est engagée que si celui-ci, après avoir été informé d'un contenu illicite, ne procède pas à son retrait dans un prompt délai.

Ce régime conduit à une **absence de vigilance active** des plateformes dans les contenus publiés.

Des plateformes e-commerce comme Amazon, Ebay ou Le Bon Coin sont souvent montrées du doigt par les titulaires de droit comme n'agissant pas suffisamment activement contre les contrefaçons présentes sur leurs plateformes.

Les enjeux sont considérables.

Selon un rapport de la Cour des comptes de mars 2020, les **échanges de contrefaçon dans le monde auraient représenté 509 milliards de dollars en 2016** (3,3% du volume des échanges mondiaux) et représenteraient 6,8% des importations dans l'Union européenne. La contrefaçon causerait la perte de 700.000 emplois et de 16,3 milliards d'euros de recettes fiscales par an.

Les très grosses plateformes, à l'instar d'Amazon ou d'Ebay, ont **lourdement investi afin de lutter contre ce phénomène**. Amazon a lancé une unité spéciale en 2020 ayant pour but de lancer des actions en justice contre les enseignes vendant des biens contrefaisants sur sa place de marché.

Néanmoins, la contrefaçon continue de prospérer sur les plateformes, tant concernant les traditionnels secteurs du luxe, que concernant de nouveaux secteurs, notamment pharmaceutiques, ce qui n'est pas sans poser de sérieux problèmes de sécurité sanitaire.

L'Assemblée nationale a publié, en décembre 2020, un rapport d'évaluation de la lutte contre la contrefaçon, pointant la dangerosité du phénomène, tant d'un point de vue sanitaire qu'économique.

2. Les moyens conférés par le DSA

La position de la Commission européenne est la suivante : **ce qui est illégal hors ligne doit être illégal en ligne.**

Que doit-on entendre par « **contenu illicite** » ? Selon le projet de règlement, il concerne **toute information, quelle que soit sa forme, qui, en vertu de la loi applicable, est, en elle-même illégale ou se rapporte à des activités illégales.**

Le DSA a pour objectif d'**accentuer les moyens d'action à l'encontre des contenus considérés comme illicites**, en ce compris les biens contrefaisants.

Dans ce cadre, il prévoit notamment :

- un **mécanisme de signalement des contenus illicites** pour les utilisateurs des plateformes et une **coopération de ces dernières avec des « signaleurs de confiance »** (entendu comme des entités ayant une expertise spécifique dans le repérage des contenus illicites) ;
- des **obligations spécifiques en termes de traçabilité des entreprises utilisatrices** afin d'aider à identifier les vendeurs de marchandises illicites.

Toutefois, le DSA, cherchant à faire une **balance équitable et proportionnée entre les intérêts des plateformes, des utilisateurs et du respect de la liberté d'expression** :

- **ne revient pas sur la distinction hébergeur et éditeur de contenus**, telle que posée par la Directive E-commerce de 2000 (les plateformes conserveront, en conséquence, le statut d'hébergeur) ;
- **n'impose aucune obligation générale de surveillance aux plateformes.**

Pour ces raisons, beaucoup appellent à un **renforcement des moyens de lutte contre la contrefaçon.**

Le **rapport d'évaluation de la lutte contre la contrefaçon de l'Assemblée nationale formule 18 propositions visant à accentuer les moyens d'actions.**

3. La nécessité de renforcer les moyens de lutte

Le rapport d'information s'articule autour de **plusieurs grands axes** :

- **Définir une stratégie nationale** coordonnant les acteurs publics et privés (notamment les Douanes et les titulaires de droits) ;
- **Réviser le cadre législatif français et renforcer la réponse judiciaire.**

Sur ce deuxième axe, le rapport préconise de :

- **Permettre à l'administration d'adresser un avertissement, d'opérer un blocage de site de contrefaçon et d'informer le public ;**
- **Adapter le droit de la propriété intellectuelle aux nouvelles modalités de délinquance** (via l'instauration d'une procédure administrative d'avertissement et de blocage des sites internet proposant des contrefaçons, la création d'agents assermentés en droit des marques autorisés à constater une infraction commise sur le web) ;
- **Améliorer l'évaluation du préjudice subi par le titulaire de droits par les tribunaux** (la contrefaçon étant, à ce jour, au regard des dommages et intérêts alloués, plus lucrative que les condamnations prononcées) ;
- **Introduire une amende civile en complément des dommages et intérêts à l'encontre du vendeur de la contrefaçon ;**
- **Faciliter la défense des droits de propriété intellectuelle des entreprises** (et notamment des PME) via la création d'un organisme apportant conseil et aide aux titulaires de droits et pouvant constater les infractions et porter plainte ;
- **Accentuer la lutte contre la vente illicite de tabac.**

Le rapport préconise également **d'adapter l'organisation judiciaire à la délinquance propre aux plateformes et réseaux sociaux**, considérant que :

- Si les sanctions pénales sont sévères, les délais de procédure sont trop longs ;
- Les magistrats disposent d'une expertise inégale des enjeux et techniques de délinquance propres au web.

Afin de pallier à cette situation, le rapport propose de **dédier une chambre juridictionnelle spécifique dans certains tribunaux, permettre aux titulaires de droits de déposer une requête en ligne et limiter la rotation des magistrats** disposant d'une expertise spécifique en matière de délinquance sur le web.

Enfin, **au niveau européen**, le rapport pointe du doigt **l'insuffisance de l'arsenal européen dans la lutte contre la contrefaçon** au regard :

- Du caractère daté de la Directive E-commerce n'étant plus alignée à l'activité réelle des plateformes et des intermédiaires en ligne ;
- De l'inefficacité des chartes de bonnes conduites (MoU).

Le rapport propose **la mise en place de mesures européennes fortes**, telles que notamment :

- **La définition d'un nouveau régime de responsabilité pour les plateformes de commerce en ligne et les réseaux sociaux** (avec l'instauration d'une obligation de moyens pour lutter contre la vente de contrefaçon et l'utilisation de l'intelligence artificielle pour aider dans la lutte ; une obligation de connaître son client (« know your

- customer ») ; l'instauration d'un formulaire harmonisé au niveau européen et une obligation pour les plateformes de rendre accessible un bouton « contrefaçon ») ;
- **L'instauration par les Etats membres d'un cadre juridique** prévoyant que les plateformes instaurent :
 - un **dispositif de traitement des notifications et des plaintes des titulaires de droits et des autorités** ;
 - Une **procédure de retrait normalisé et un délai d'intervention** ;
 - Une **possibilité de signalement de la contrefaçon sur le site** ;
 - Une **obligation de transparence sur les moyens mis en œuvre** (en personnel) pour la lutte contre la contrefaçon et le traitement des réclamations.
 - Une **information des consommateurs** via l'obligation de rembourser les clients ayant acheté des contrefaçons sur le site.

Ces **mesures ne sont, pour l'heure, pas celles prévues par le DSA**, ce qui explique que les grands acteurs de la lutte contre la contrefaçon font part de leurs réserves quant à l'efficacité du texte dans le cadre de la lutte contre la contrefaçon.

Un important travail de lobbying par des acteurs disposant d'intérêts nécessairement opposés, va se mettre en place dans les prochains mois.

L'issue de cette démarche nous permettra de voir si le DSA, tant attendu et tant espéré, deviendra, comme le souhaite la Commission européenne, l'arme ultime de régulation du marché numérique.

Les informations fournies dans le cadre de cette lettre d'information ne peuvent en aucun cas être considérées comme un conseil quelconque et doivent être vérifiées ou confirmées par des personnes habilitées avant d'être utilisées.

Sources : afnic.fr ; nic.ar ; dns.lu ; google.com ; znet.fr ; domainnamewire.com ; iptwins.com ; verisign.com ; presse-citron.net ; icann.org ; wipo.int ; dreyfus.fr ; haas-avocats.com

L'équipe Domainoo reste à votre entière disposition pour tout complément d'information.

DOMAINOO

49, rue de Richelieu - 75001 Paris
Tél 01 47 05 87 27 - Fax 01 56 72 90 48
Email: info@domainoo.com