PANTHÉON-ASSAS
UNIVERSITÉ
PARIS

BANQUE DES MEMOIRES

Master de Propriété industrielle
Dirigé par Jean-Christophe Galloux
2024

La protection des signes distinctifs face au développement du cybersquatting

Flore David

Sous la direction de Madame le Professeur Radmila Chapuis

Avertissement

La faculté n'entend donner aucune approbation ni improbation aux opinions émises dans ce mémoire ; ces opinions doivent être considérées comme propres à leur auteur.

Remerciements

J'adresse tous mes remerciements

À Madame le Professeur Radmila CHAPUIS pour tous ses conseils, ses encouragements ainsi que son aide précieuse dans la préparation de mon mémoire.

À mon directeur de Master, Monsieur le Professeur Jean-Christophe GALLOUX, pour m'avoir admise au sein de ce Master Droit de la Propriété Intellectuelle parcours Propriété Industrielle.

Sommaire

Introduction

Le 20 novembre 2020, 22 ans après la création de l'ICANN et de la procédure UDRP, le Centre d'arbitrage et de médiation de l'Organisation Mondiale de la Propriété Intellectuelle (OMPI) a enregistré sa 50 000e plainte pour cybersquattage. Nous assistons à l'heure actuelle à une augmentation exponentielle des dépôts de plainte à l'OMPI. La pandémie de Covid-19 a marqué cette forte augmentation et le directeur du Centre d'arbitrage et de médiation de l'OMPI, M. Erik WILBERS, explique ce phénomène par la hausse de temps que nous passons en ligne, notamment avec le télétravail. En effet, l'espace numérique est devenu, pour les cybersquatteurs, un véritable terrain de jeu pour porter atteintes aux droits de propriété intellectuelle des titulaires[1].

Il est nécessaire, avant tout développement, de comprendre « comment est né le cybersquattage ? ». Tout commence à la fin du siècle dernier avec la création des noms de domaine. Il s'agit d'une « *dénomination unique à caractère universel qui permet de localiser une ressource ou un document sur internet, et qui indique la méthode pour y accéder, le nom du serveur et le chemin à l'intérieur du serveur* »[2]. Les noms de domaine trouvent leurs sources dans la création de l'*Advanced Research Projects Agency network* (ARPAnet), un réseau interuniversitaire d'échange d'informations que les chercheurs américains ont mis en place et qui n'était limité, au début, qu'à une dizaine d'ordinateurs. Le gouvernement américain, voyant le potentiel de ce projet, a demandé que le réseau ARPAnet puisse communiquer avec le réseau de la *National Science Foundation* (NSF). Mais pour pouvoir communiquer, il fallait trouver un langage commun. Cette mission a été confiée à l'*Internet Engineering Task Force* (IETF) et celui-ci va rendre des décisions techniques via le *Request for comments* (RFC), qui est un document visant à établir un standard de l'internet pouvant être perçu comme une décision technique influant la manière dont le réseau va être géré. Le principal éditeur des RFC fut Jon Postel qui a publié, lors d'une conférence de l'*International Network Working Group* en septembre 1973, pour la première fois, le TCP/IP (*Transfer Control Protocol*) qui est le langage commun entre deux machines situées sur deux réseaux différents. Pour qu'une communication entre deux machines puisse se réaliser, il est nécessaire que ces deux machines soient connectées et identifiées sur le même réseau commun et utilisent toutes deux ce langage TCP/IP. Chaque machine va être localisée par une adresse IP, qui est une suite de chiffres

[1] M. Erik WILBERS, Directeur du Centre d'arbitrage et de Médiation de l'OMPI
[2] *Vocabulaire de l'Internet et de l'informatique* publié par la Commission de terminologie française JORF n°63, 16 mars 1999

séparés par des points. Ces adresses étant difficiles à mémoriser et face à l'augmentation du nombre de machines interconnectées, Jon Postel a proposé le système des noms de domaine, le *domain name system* (*DNS*), qui prévoit que pour chaque adresse IP il existera une correspondance sous forme de suite de lettres. Ce système DNS va convertir le nom de domaine en adresse IP chiffrée. La conséquence d'une telle création est l'attrait grandissant du système Internet entrainant une multiplication exponentielle des enregistrements. Il était ainsi nécessaire de modifier la gestion du DNS. C'est pour cela que la RFC n°920 va proposer la création de 250 extensions de premier niveau que l'on va diviser en deux classes de nommage : 6 extensions « génériques », que l'on appelle les « gTLD » dans lequel on retrouve « .gov », « .edu », « .com », « .org », « .mil » et « .net », et 244 extensions « locales », que l'on appelle les « ccTLD » ou code pays et qui renvoie à la dimension territoriale d'Internet. Ces deux classes de nommage ont des finalités différentes, les extensions génériques vont servir à cibler les utilisateurs en fonction d'un intérêt particulier, renvoyant plus à une dimension commerciale, alors que les extensions locales vont servir à manifester une appartenance à une certaine localité, par exemple le « .fr » pour la France.

Initialement, la gestion du système DNS appartenait au Département du commerce américain. Cependant, il devenait indispensable de confier ce réseau à une personne morale afin que qu'il puisse évoluer et gagner en importance. C'est ainsi qu'en 1998 l'*Internet Corporation for Assigned Names and Numbers* (ICANN) est née. Il s'agit d'une entité technique indépendante du gouvernement américain qui va être régie par des principes juridiques et être subordonnée au droit californien. Son rôle est de coordonner la gestion des noms de domaine à l'international et par conséquent gérer essentiellement la stabilité d'internet. Pour ce faire, elle va coordonner 13 serveurs racine qui vont abriter les noms de domaine.

Néanmoins, la création des noms de domaine a également des zones sombres. En effet, à la fin des années 1990 et face à cet engouement autour des noms de domaine, il y a eu une nécessité de régler le problème de la protection des droits de propriété intellectuelle. Ainsi, en 1998, l'ICANN a instauré la *Uniform Domain Name Dispute Resolution Policy*, la procédure UDRP, destinée à régler les litiges issus de l'enregistrement d'un nom de domaine qui porterait atteinte au droit de marques du titulaire[3].

[3] *Noms de domaine et modes alternatifs de règlement de conflits*, Thèse de Radmila Pavlenko épouse Chapuis,

Dès lors, c'est avec la naissance des noms de domaine qu'est né le cybersquattage. Ce terme ne connait pas de définition législative. Cependant, des auteurs vont définir ce comportement comme « *l'enregistrement de mauvaise foi d'un nom de domaine similaire ou identique aux droits antérieurs d'un tiers* »[4]. Ainsi, le cybersquatting est un acte portant atteinte aux signes distinctifs.

Les signes distinctifs sont les moyens phonétiques ou visuels qui permettent à la clientèle de reconnaître les produits, les services ou les établissements qu'elle recherche et de les distinguer des produits, des services ou des établissements similaires[5]. Il existe deux catégories de signes distinctifs, nous avons d'un côté les signes distinctifs à usage individuel où l'on retrouve le droit de marques, le nom commercial, l'enseigne, la dénomination sociale, les noms de domaine, et les signes distinctifs à usage collectif où l'on retrouve notamment les indications d'origine et les appellations d'origine protégée. Notre étude se concentrera sur les signes distinctifs à usage individuel, qui constituent les principales cibles des cybersquatteurs. Cela dit, il convient de noter qu'un signe à usage collectif peut également être victime de cet acte illicite.

Ce présent mémoire va s'intéresser à la protection des signes distinctifs face au développement du cybersquatting.

En partant du droit positif, il est opportun d'étudier les atteintes aux signes distinctifs à l'ère du numérique (Partie I) avant de mettre en exergue la nécessité d'une révision pour arriver à une meilleure protection (Partie II).

[4] « Le cybersquatting est-il un acte de cybercriminalité ? » Chronique 7 octobre 2008
[5] *Droit de la propriété industrielle*, Jean-Christophe Galloux et Jacques Azéma, « Deuxième Partie : les droits sur les signes distinctifs », 8e édition, Paris, Dalloz, 2017

Partie I – Les atteintes aux signes distinctifs à l'ère du numérique

Il existe aujourd'hui une multitude d'atteintes possibles aux signes distinctifs, il peut s'agir notamment d'une reproduction d'un modèle, d'une mise sur le marché de produits non autorisée par le titulaire des droits. Cependant, avec l'émergence des noms de domaine depuis une vingtaine d'années, un nouvel acte illicite a vu le jour : le cybersquatting. Depuis 1998, la base de données de l'OMPI recense plus de 129 000 noms de domaine, parmi lesquels plus de 70 700 procédures UDRP ont été déposées. Cela signifie que plus d'un nom de domaine sur deux a porté atteinte à un droit de marques[6]. En 2020, on estime que plus de 370 millions de noms de domaine ont été enregistrés dans le monde auprès de divers bureaux d'enregistrement[7]. Ce phénomène, certes récent, ne fait que progresser au fil des années. En effet, en 2023, 6192 litiges ont été résolus devant l'OMPI grâce à la procédure UDRP contre 3447 en 2018[8]. Donc en l'espace de cinq années, le nombre de litiges a augmenté de près de 179%. Néanmoins, ce nombre ne prend en considération que les noms de domaine soumis au système DNS, or il existe aujourd'hui une autre catégorie de noms de domaine, les noms de domaine décentralisés qui sont une concurrence directe à l'ICANN et qui ne sont sous la responsabilité d'aucun organe indépendant du créateur et donc aucune procédure extrajudiciaire ne permet demander le transfert ou la suppression de tel type de nom de domaine révélant une insuffisance de protection dans le système actuel.

Les noms de domaine sont devenus, depuis leur création, un véritable fonds de commerce pour les cybersquatteurs (Chapitre 1). Néanmoins, même s'il existe un système encadrant ces signes distinctifs, il reste insuffisant face à l'environnement numérique (Chapitre 2).

[6] Voir les annexes 1 et 2 p.32, données prises du site officiel de l'OMPI
[7] « Combien existe-t-il de noms de domaine en 2020 ? », Jean-François Poussard, 4 mars 2020 Solidnames
[8] « Total Number of Domain Names by Years », site de l'OMPI

Chapitre 1 – Les noms de domaine, le fonds de commerce du cybersquatteur

Les noms de domaine peuvent être perçus comme un poste de dépenses majeur pour les ayants droits[9]. Par exemple, le 27 juillet 2016, la société Nu Dot Co a acquis le Top-Level Domain générique « web » pour la somme de 135 millions de dollars, l'objectif derrière ce rachat est celui de pouvoir vendre ou louer cette extension de domaine[10]. Cet exemple illustre non seulement l'impact financier qu'une extension de nom de domaine peut avoir, mais également la valeur économique d'un simple nom de domaine. Ainsi, pour le cybersquatteur, la revente de noms de domaine créés en violation des droits des tiers constitue une opération particulièrement lucrative. Il existe de nos jours une multiplicité de noms de domaine, que l'on va diviser en deux catégories (Section 1), ayant des conséquences néfastes (Section 2).

Section 1 – La rivalité entre les deux systèmes de nommage, DNS ou blockchain ?

Depuis la fin des années 1990, le système des noms de domaine, dit DNS, gère uniquement les noms de domaine « classiques », c'est-à-dire ceux qui permettent de transcrire la suite de chiffres que constitue l'adresse IP en une suite de lettres pour donner l'accès à un site internet. Face à eux existe, depuis plus d'une dizaine d'années, un nouveau système de nommage sur blockchain, ce sont des noms de domaine « décentralisés ». Il est opportun de présenter ces deux catégories de noms de domaine.

Tout d'abord, les noms de domaine « classiques » sont sous la responsabilité de l'ICANN, puisque c'est elle qui gère le système DNS, et doivent, par conséquent, obéir à sa politique. Même si certains auteurs sont réfractaires à cette idée, particulièrement Olivier Ricou qui considère qu'il n'existe pas de « *gouvernement de l'Internet mais quatre pouvoirs qui contribuent au bon fonctionnement de l'Internet* »[11], l'ICANN gouverne aujourd'hui le système DNS[12]. En effet, elle remplit les quatre conditions caractérisant la gouvernance : tout d'abord, il s'agit d'une personne morale régulant tout le système DNS, pouvant déléguer les extensions génériques ou locales à des registres, ayant la main mise sur les réseaux et ayant la possibilité de créer des extensions locales. Par ailleurs, les registrars, accrédités par les registres, sont

[9] Newsletter juillet 2019, Cabinet Plasseraud
[10] « Enchères record pour le.web, vendu à 135 millions de dollars », Équipe éditoriale IONOS, le 30/11/2022
[11] *Géopolitique de l'Internet*, Olivier Ricou, version 3.1 du 2 aout 2023
[12] *Democracy and its critics*, New Haven and London, 1989, Robert Alan DAHL

soumis à la politique de l'ICANN. Ensuite, toutes les décisions politiques prises par l'ICANN répondent aux problématiques spécifiques de la gestion DNS, toute l'arborescence du DNS est soumise à cette loi privée de l'ICANN, d'autant plus que c'est elle qui va imposer sa réglementation à tous les niveaux par des contrats successifs. Troisièmement, elle possède ce pouvoir de coercition qu'elle va exercer à l'encontre des registres, des registrars et des utilisateurs finaux. Et enfin, la juridiction de l'ICANN s'étend à tout le système des noms de domaine, y compris aux extensions locales.

L'ICANN va approuver un registre qui va pouvoir gérer ces extensions locales. C'est notamment le cas en France avec l'Association Française pour le Nommage Internet en Coopération (AFNIC), créée en 1997, qui gère plusieurs extensions locales nationales à savoir le « .fr », le « .re », le « .tf », le « .yt », le « .pm » et le « .wf ». Tout l'encadrement autour de ces extensions locales a été réalisé par la loi du 9 juillet 2004[13] qui a créé l'article L45 du Code des postes et communications électroniques (CPCE), censuré à la suite d'une question prioritaire de constitutionnalité le 6 octobre 2010[14]. Aujourd'hui, les conditions d'attribution des noms de domaine en .fr sont prévues aux articles L45 à L45-8 CPCE[15]. Ces dernières années ont marqué une forte croissance du .fr puisqu'en 2023, 801 427 nouveaux noms de domaine en .fr ont vu le jour, soit une augmentation de 3,4%[16]. Par ailleurs, en France l'extension nationale a gagné 0,9 point de part de marché en 2023 alors que le .com, l'extension générique, a perdu 0,8 point[17].

En 1998, l'ICANN a été créée afin de « *garantir un Internet mondial sûr, stable et unifié* »[18]. Cependant, depuis les années 2000 est née une multitude de réseaux parallèles dont le plus connu est issu de la blockchain, qui est une technologie de stockage permettant la transmission des informations. Cette blockchain présente de nombreux avantages puisqu'elle est transparente, sécurisée, infalsifiable et ne nécessite aucun organe de contrôle. Le développement de ce réseau parallèle a permis la création d'un nouveau système de nommage sur blockchain et l'arrivée de nouveaux noms de domaine décentralisés, pouvant être définis

[13] Loi n°2004-664 relative aux communications électroniques et aux services de communication audiovisuelles, JORF n°159, 10 juillet 2004, p.12483
[14] Conseil Constitutionnel, 6 octobre 2010, n°2010-45 QPC, D.2010.2285
[15] Modification par l'ordonnance n°2014-329 du 12 mars 2014
[16] « Bilan 2023 du .fr : Plus de 40% des noms de domaine en France sont en .fr » Actualité de l'AFNIC publiée le 26 mars 2024
[17] Annexe 3, p.33 : Variations des parts de marché en France (2019-2023)
[18] *Élaboration de politiques*, site officiel de l'ICANN

comme des jetons non-fongibles[19]. Un NFT, ou crypto actif, est un actif numérique stocké sur un support électronique permettant à une communauté d'utilisateurs les acceptant en paiement de réaliser des transactions sans avoir à utiliser la monnaie légale[20]. Ainsi, contrairement au système DNS, utilisé pour trouver l'adresse IP correspondant au nom de domaine, la blockchain associe un nom de domaine à l'adresse d'un contrat intelligent. Cette adresse renvoie ensuite vers un compte utilisateur identifié par des adresses cryptographiques, souvent difficilement lisibles. L'ICANN n'a aucune main mise sur ces noms de domaine décentralisés prenant de plus en plus d'ampleur. Puisqu'ils ne sont pas validés par l'ICANN, il n'existe aucune procédure extrajudiciaire permettant la récupération de ce type de noms de domaine ni de moyens techniques ou juridiques pour statuer sur de tels noms de domaine.

L'enregistrement d'un nom de domaine décentralisé correspondant à la marque du titulaire peut être un moyen pour lui de la protéger sur l'environnement numérique, le Web3[21] qui est un terme employé pour désigner l'Internet décentralisé, et d'éviter qu'un tiers ne puisse l'acheter pour le revendre au prix fort. Il existe, aujourd'hui, une multitude de systèmes de nommage basés sur la blockchain, on peut citer notamment BitDNS, Solana Name Service, EmerDNS, PeerName, Emercoin, Ethereum Name Service. Le fournisseur le plus connu est Unstoppable Domains qui propose des extensions tels que « bitcoin », « coin » ou encore « nft ». D'autres plateformes proposent des extensions notamment la plateforme ENS lancée depuis 2017 qui se développe de plus en plus puisqu'elle a enregistré 378 000 noms de domaine en .eth seulement sur le mois de juillet 2022 et a enregistré en tout plus de 2 millions de noms de domaine en blockchain vers la fin de l'année 2022[22]. Il est primordial, dès lors, de comprendre et d'encadrer ces noms de domaine décentralisés car même s'ils présentent de nombreux avantages, ils peuvent également être source d'inconvénients notamment à cause de la complexité de tracer les activités en ligne étant donné son anonymat. En outre, les noms de domaine régis par l'ICANN doivent respecter les politiques qu'elle a elle-même mises en place alors qu'un nom de domaine en blockchain, qui n'est régi par aucun organe de contrôle, n'obéit à aucune règle, même s'il existe un règlement européen pouvant être une source face à ces

[19] NFT « *non fungible tokens* »
[20] « Cryptoactifs, cryptomonnaies : de quoi s'agit-il ? » Ministère de l'Économie, des finances et de la souveraineté industrielle et numérique, economie.gouv.fr
[21] Terme utilisé pour la première fois par le fondateur de Polkadot et le cofondateur d'Ethereum, Gavin Wood en 2014
[22] « Ethereum Name Service : plus de 2 millions de noms de domaine.eth enregistrés », Le Journal du Coin le 24 août 2022

difficultés. Ainsi, aujourd'hui, il existe des milliers de noms de domaine ayant défini leurs propres règles.

Section 2 – Des actes aux conséquences néfastes

Les noms de domaine peuvent devenir un véritable danger. En effet, ils peuvent être utilisés à mauvais escient que ce soit par le registrant qui va volontairement créer un nom de domaine pour pouvoir gagner de l'argent en le revendant au titulaire légitime ou encore le requérant, c'est-à-dire le titulaire du droit lui-même, qui va abuser de la procédure UDRP pour essayer de se faire transférer un nom de domaine dont il n'est pas un détenteur légitime, c'est ce que l'on appelle le détournement de nom de domaine inversé, *reverse domain names hijacking* (RDNH). Dans le premier cas, il s'agit d'un acte de cybersquatting et dans le second, un abus de procédure.

Il est opportun de comprendre ce qu'est cet acte qui est en développement constant. Le cybersquatting est un abus de noms de domaine. Le 16 mai 2023, l'*International Trademark Association* (INTA) a défini cet abus comme « *toute activité qui utilise, ou à l'intention d'utiliser, des noms de domaine, le protocole du système des noms de domaine ou tout indicateur numérique dont la forme ou la fonction est similaire à celle des noms de domaine pour mener des activités trompeuses, malveillantes ou illégales* ». En réalité, la pratique du cybersquatting peut être associée au chantage puisque le cybersquatteur va obliger les titulaires de droits d'acheter les noms de domaine déjà enregistrés correspondant, entre autres, à leurs propres marques. Cette pratique ne vise pas à tromper l'internaute mais à priver la victime d'un nom afin de lui demander de l'argent. À cet égard, la vente de noms de domaine n'est pas une activité illégale. En effet, on parle de « *domaining* » pour faire référence à cette activité et celui qui la pratique se nomme le domaineur et celui-ci n'est pas forcément un cybersquatteur. Par exemple, en 2015 GDF Suez a racheté pour 9 999 euros le nom de domaine « engie.ru » car cette entreprise a déposé une nouvelle marque Engie sur le territoire Russe[23]. Pourtant, de nombreux cybersquatteurs vont détourner cette activité, en principe légale, pour obliger des titulaires de droit de racheter leurs noms de domaine plus particulièrement quand le prix moyen d'un rachat de nom de domaine est aux alentours de 5000 euros[24]. Parmi les secteurs les plus

[23] « Rachat nom de domaine », Solidnames
[24] Annexe n°4 p.33

touchés par le cybersquatting on peut retrouver le secteur de la banque, de la finance, de la biotechnologie, de la pharmacie, de la mode et du commerce en détail[25].

Toutefois, il n'y a pas seulement le requérant qui peut être une victime puisque le registrant lui-même peut en être une du fait du RDNH. Le principe est que le requérant va intenter de mauvaise foi une procédure UDRP notamment parce qu'il sait qu'il n'a pas de droit prioritaire à faire valoir sur le nom de domaine que le registrant a enregistré de bonne foi[26]. La victime de RDNH n'obtient que rarement la demande du requérant, à savoir le transfert du nom de domaine, fort heureusement. Néanmoins, les experts se limitent à rejeter la plainte et aucune sanction dissuasive n'est prise à l'encontre du requérant. La seule sanction qui existe en cette matière est la mention sur un site dédié aux affaires de RDNH.com comme auteur de plainte abusive[27]. Les cas de RDNH se multiplient au fil des années. Rien qu'entre janvier et juillet 2024, 29 cas de RDNH ont été recensés[28]. Par ailleurs, c'est le 2 juin 2022 qu'est rendue la 500e décision UDRP déclarant un plaignant coupable de RDNH[29]. Néanmoins, il existe des cas où l'expert UDRP va refuser d'admettre que le plaignant exerce un abus de procédure. Ne serait-ce récemment, dans une décision de l'OMPI du 12 mars 2024[30] où l'expert UDRP, pour refuser de caractériser une tentative de RDNH du demandeur s'est fondé sur la « croyance sincère » de celui-ci. Cette décision est très contestable puisque la notion de « croyance sincère » ne figure pas dans les règles UDRP. Par conséquent en retenant une telle solution, l'expert va à l'encontre de ces règles et par la même occasion permet le développement du « harcèlement » en matière de nom de domaine.

Ainsi, avec le développement d'Internet, il est de plus en plus facile, ou du moins plus accessible, de porter atteinte à un droit. Le Conseil Constitutionnel en fait état de ces constatations et s'exprime sur ce sujet « *en l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services dans la vie économique et sociale, notamment pour*

[25] « Nom de domaine – Dernières tendances chez l'OMPI : une forte croissance des litiges sur les noms de domaine en 2023 » – Propriété industrielle n°4, Avril 2024, alerte 30 – Cabinet Dreyfus
[26] WIPO Arbitration and Mediation Center, Case No D2000-1123, Teranet Land Information Services Inc. v. Verio Inc, January 25, 2001
[27] Article 15 e) des principes directeurs
[28] Reverse Domaine Name Hijacking Information, RDNH.com
[29] « The UDRP « Celebrates » Its 500th Reverse Domain Name Hijacking Case », by Zak Muscovitch, General Counseil, Internet Commerce Association, CircleID
[30] WIPO Arbitration and Mediation Center, Case No D2024-0151 Mermet SAS v. Didier Mermet, mermet.com, March 12, 2024

ceux qui exercent leur activité en ligne, l'encadrement, tant pour les particuliers que pour les entreprises, du choix et de l'usage des noms de domaine sur internet affecte les droits de la propriété intellectuelle, la liberté de communication et la liberté d'entreprendre »[31]. Par conséquent, pour répondre à ce besoin de protection, ont été mises en place des procédures afin que la victime d'un cybersquatting puisse se défendre. Néanmoins, se pose la problématique suivante : *est-ce une protection réellement efficace ?*

Chapitre 2 – Une protection existante mais insuffisante

Le titulaire, victime de cybersquatting, a le choix entre une procédure judiciaire et une procédure extrajudiciaire. Le choix de la procédure va dépendre de la complexité de l'affaire et de ce que la victime souhaite obtenir. Si la victime fait le choix d'une procédure judiciaire, elle pourra opter soit pour l'action en contrefaçon si le nom de domaine en cause porte atteinte à son droit de propriété intellectuelle, soit pour l'action en concurrence déloyale[32] ou le cas échéant l'action pour usurpation d'identité. Néanmoins, la procédure judiciaire reste plus couteuse. Ainsi, la victime peut choisir d'avoir recours à une procédure extrajudiciaire, moins couteuse et immédiatement applicable.

Dans le périmètre de ce mémoire, nous nous concentrerons sur les procédures extrajudiciaires. Il existe de nombreuses procédures internationales, la plus importante étant la *Uniform Domain-Name Dispute-Resolution Policy*, la procédure UDRP (Section 1) qui sera étudiée dans un premier temps. Puis dans un second temps, il sera intéressant de comparer cette procédure internationale avec les procédures alternatives qui ont été mises en place dans les extensions locales (Section 2).

[31] Conseil Constitutionnel, 6 octobre 2010, n°2010-45 QPC, D.2010.2285
[32] Article 1240 du Code Civil

Section 1 – La procédure UDRP

« *Les principes UDRP constituent un outil essentiel pour protéger les utilisateurs de l'Internet dans le monde entier contre la tromperie et la fraude en ligne* »[33].

Cette procédure a été instaurée dès 1998 par l'ICANN. Elle s'applique obligatoirement à toutes les extensions génériques mais pas forcément aux extensions locales qui peuvent avoir une procédure propre. Cette procédure trouve son fondement dans, tout d'abord, les principes directeurs sur la procédure uniforme de résolution des litiges en matière de noms de domaine[34], puis les règles d'application[35] et enfin les règles supplémentaires adoptées par le fournisseur administrant une procédure[36]. La procédure UDRP ne s'applique qu'au seul registrant qui viole un droit de marque[37]. À noter que la marque peut être soit enregistrée soit être une marque d'usage, signifiant ainsi que la condition est moins l'enregistrement que la commercialité du signe à protéger.

À propos de la charge de la preuve, nous notons que c'est au requérant de prouver que le nom de domaine lui porte préjudice car celui-ci porte atteinte à son droit de marque. Pour cela, il doit prouver de manière cumulative le risque de confusion entre sa marque et le nom de domaine, que le registrant n'a aucun intérêt à enregistrer le nom de domaine et enfin que l'enregistrement et l'utilisation du nom de domaine ont été faits de mauvaise foi. Il faut analyser plus en détail ces notions à prouver. Tout d'abord, l'appréciation du risque de confusion. Pour les experts UDRP il ne s'agit pas d'analyser le contenu du site[38], néanmoins, dans plusieurs décisions, certains experts ont élargi l'analyse du risque de confusion au comportement du registrant[39]. Les décisions sont contradictoires, tout dépend de l'expert UDRP chargé de l'affaire, créant ainsi une insécurité juridique. Par ailleurs, il faut prouver que le registrant n'ait

---

[33] Propos du Directeur général de l'OMPI, M. Daren Tang : https://www.wipo.int/pressroom/fr/articles/2020/article_0026.html#:~:text="Les%20principes%20UDRP%20constituent%20un,Daren%20Tang.

[34] Principes directeurs régissant le règlement uniforme des litiges relatifs aux noms de domaine, adoptés le 26 août 1999

[35] Règles pour la procédure uniforme de résolution des litiges en matière de noms de domaine, approuvées par l'ICANN le 24 octobre 1999

[36] Règles supplémentaires NAF pour la résolution de litiges UDRP, mise à jour le 31 juillet 2015

[37] Articles 1er et 4(a) des principes directeurs

[38] WIPO Arbitration and Mediation Center, Case No D2000-1698 Arthur Guiness Son&Co (Dublin) Limited v. Dejan Macesic, January 25, 2001

[39] WIPO Arbitration and Mediation Center, Case No D2001-0970, Briefing.com Inc v. Cost Net Domain Manager, September 12, 2001

aucun intérêt légitime à enregistrer son nom de domaine, en revanche le requérant n'a pas à prouver qu'il a un intérêt à agir en UDRP. Le registrant à un intérêt légitime lorsque, par exemple, il fait un usage loyal ou non-commercial du nom de domaine ou que celui-ci n'a pas eu connaissance de l'intention du titulaire de la marque d'acquérir le nom de domaine litigieux[40]. Enfin, doit être prouvée la mauvaise foi du registrant. La procédure UDRP exige une preuve indépendante de l'enregistrement et la mauvaise foi du nom de domaine. Néanmoins, les experts ont proposé une théorie, qui va à l'encontre des principes UDRP, qu'ils vont développer et qui est la théorie de la contamination rétroactive, c'est-à-dire que l'usage de mauvaise foi du nom de domaine va contaminer l'acte d'enregistrement, même si celui-ci a été effectué de bonne foi par le registrant[41]. De cette théorie découle la théorie inversée, c'est-à-dire que l'enregistrement de mauvaise foi du nom de domaine va contaminer l'usage de celui-ci par le registrant[42].

De l'analyse de ces conditions découle un fait : le déséquilibre entre les parties. En effet, le registrant est obligé, à partir du moment où la procédure est lancée d'y participer. Par ailleurs, le requérant peut démarrer la procédure UDRP à n'importe quel moment, il n'existe aucun délai de prescription. À noter qu'en général en droit de la propriété intellectuelle, l'action en contrefaçon est prescrite par 5 ans à compter du jour où le titulaire d'un droit a connu ou aurait dû connaître le dernier fait lui permettant de l'exercer[43]. Ainsi, le requérant peut prendre tout le temps nécessaire pour préparer l'instance en collectant des preuves ainsi que rédiger ses conclusions. En revanche, le registrant n'a que 20 jours[44] pour répondre et présenter son argumentaire, sans prolongation possible. La problématique face à ce court délai est que le registrant n'a pas le temps de répondre soit pour faute de temps soit parce qu'il n'a pas les moyens financiers suffisants pour pouvoir le faire. En outre, c'est le requérant qui a le pouvoir de choisir le centre de règlement de litige. Il existe 5 centres qui sont habilités à recevoir des plaintes UDRP : le Centre d'arbitrage et de médiation de l'OMPI, la Cour Arbitrale Tchèque (CAC), le National Arbitration Forum (NAF), le Centre asiatique de règlement des différends en matière de noms de domaine (ADNDRC) et le Centre arabe pour le règlement des litiges relatifs aux noms de domaine (ACDR). Ainsi, celui-ci pourra prendre le centre qui va avoir le

[40] WIPO Arbitration and Mediation Center, Case No D2000-0016, Allocation Network GmbH v. Steve Gregory, March 24, 2000
[41] WIPO Arbitration and Mediation Center, Case No D2009-0643, City Viexs Limited v. Moniker privacy Services / Xander, Jeduyu, Algebralive, July 3, 2009
[42] WIPO Arbitration and Mediation Center, Case No D2000-0021, Ingersoll-Rand Co. Vs. Gully, March 9, 2000
[43] Article L716-4-2 du CPI en matière de droit de marque
[44] Article 5(e) des principes directeurs

taux de transfert le plus élevé, c'est-à-dire les décisions qui ont donné gain de cause au requérant. En 2023, le rapport de l'OMPI mentionne un nombre de dépôt de plaintes de 6192 avec un taux de transfert du nom de domaine litigieux au requérant de 82%, sachant que 3% des plaintes ont été rejetées et 14% des plaintes ont été résolues à l'amiable[45].

Certes la procédure UDRP est essentielle pour sécuriser internet et éviter que des noms de domaine tombent dans les mains de titulaires malveillants. Néanmoins, celle-ci n'est pas parfaite notamment à cause de cette difficulté du déséquilibre entre les parties. Par ailleurs, il est nécessaire de prendre en considération les noms de domaine en blockchain qui ne peuvent être transférés via cette procédure qui ne règle que les litiges en relation avec un nom de domaine dépendant du système de nommage DNS.

Section 2 – Les procédures alternatives spécifiques aux extensions locales

Il existe, à côté de la procédure UDRP, d'autres procédures alternatives de résolution des litiges qui ont été mises en place dans les extensions locales. En effet, l'ICANN a laissé libre aux différents services qui gèrent les extensions locales de mettre en place ces types de procédures. C'est le cas notamment en France où l'AFNIC a mis en place la procédure SYRELI qui s'applique aux extensions locales nationales.

Cette procédure SYRELI demeure légèrement différente de la procédure UDRP. En effet, tout d'abord le requérant doit pouvoir être le réservataire d'un nom de domaine en .fr au regard de la charte de nommage du .fr., dont la dernière mise à jour a été réalisée le 3 juillet 2023. Par ailleurs, contrairement à la procédure UDRP, le requérant doit forcément avoir un intérêt à agir, cette condition peut notamment permettre d'éviter les actes de RNDH. En outre, il faut pouvoir prouver que le nom de domaine litigieux rentre dans l'une des hypothèses suivantes, c'est-à-dire qu'il ne doit pas être « *1° susceptible de porter atteinte à l'ordre public ou aux bonnes mœurs ou à des droits garantis par la Constitution ou par la loi ; 2° susceptible de porter atteinte à des droits de propriété intellectuelle ou de la personnalité, sauf si le demandeur justifie d'un intérêt légitime et agit de bonne foi ; 3° identique ou apparenté à celui de la République française, d'une collectivité territoriale ou d'un groupement de collectivités territoriales ou d'une institution ou service public national ou local, sauf si le demandeur*

[45] Rapport de l'OMPI pour l'année 2023

justifie d'un intérêt légitime et agit de bonne foi »[46]. Ainsi, contrairement à la procédure UDRP qui exige une atteinte à un droit de marque, la procédure SYRELI a un champ plus vaste. L'AFNIC a, par exemple, pris une décision de transmission du nom de domaine « entiledefrance.fr » au profit du requérant, la RÉGION ILE DE FRANCE. Dans cette affaire, le requérant a soulevé que « *l'enregistrement ou le renouvellement du nom de domaine entiledefrance.fr par le titulaire est susceptible de porter atteinte à des droits de PI ou de la personnalité* » mais également est apparenté à celui d'une collectivité territoriale, à savoir la région Ile de France[47]. Il s'agit d'une procédure rapide car le collège de l'AFNIC rend ses décisions dans un délai de 21 jours calendaires à compter de l'expiration du délai de réponse laissé au titulaire, qui est également de 21 jours. Les décisions sont adoptées à la majorité par un Collège de l'AFNIC composé de 3 membres, qui statuent sur la demande au vu des seules écritures et pièces déposées par les parties. Les décisions de l'AFNIC sont exécutées une fois écoulé le délai de 15 jours civils à compter de la notification de celles-ci aux parties. Les décisions prises par l'AFNIC sont susceptibles de recours devant le juge judiciaire[48].

La France n'est pas le seul pays ayant mis en place ce type de procédure alternative pour les extensions locales. Il existe, au Royaume-Uni, le service de médiation et d'arbitrage du registre NOMINET qui a mis en place le Dispute Resolution Service, DRS, ouverte à toute personne démontrant que l'enregistrement ou l'utilisation abusive d'un nom de domaine en « .uk » a porté atteinte à un quelconque droit de propriété intellectuelle[49]. En effet, dans de nombreuses décisions, l'expert anglais a affirmé que « *le requérant a des droits sur un nom ou une marque identique ou similaire au nom de domaine* », ce qui a permis, sur ce fondement, le transfert du nom de domaine « record-power.co.uk » à la société Record Power Ltd par exemple[50]. Contrairement à la procédure UDRP, celle-ci permet à ce que le requérant soit sanctionné en cas de RDNH puisque que l'article 18.8 du Dispute Resolution Service Policy dispose que « *si le plaignant est reconnu à trois reprises au cours d'une période de 2 ans comme ayant procédé à un détournement inverse de nom de domaine, NOMINET n'acceptera plus de plaintes de ce plaignant pendant une période de deux ans* ». Par ailleurs, il existe la procédure cnDRP en Chine où il est indiqué que cette procédure est ouverte à toute personne dont un nom

[46] Article L45-2 du CPCE
[47] Décision de l'AFNIC, entiledefrance.fe, Demande n°FR 2024-03882, 7 juin 2024
[48] Article L45-6 du CPCE
[49] Article 1 « Abusive Registration » - Dispute Resolution Service Policy
[50] DRS No 04849, record-power.co.uk du 19 septembre 2007

de domaine porte atteinte à ses droits ou intérêts légitimes[51], une formulation large qui peut englober de nombreuses hypothèses. Cette procédure est également intéressante et tente à combattre le déséquilibre existant entre les parties puisque celle-ci rejette toute plainte relative à un nom de domaine enregistré depuis plus de 3 ans[52]. Dès lors, à côté de la procédure UDRP, il existe d'autres procédures qui certes sont très proches de la procédure uniforme mais s'en écarte sur certains points, un écart appréciable et qui tente à combattre les lacunes de cette procédure.

La législation actuelle ne prend pas assez en compte les développements technologiques. Nous sommes entrés dans une ère où le numérique a une place majeure et où se développent de nouveaux moyens, de nouvelles techniques aux fins de porter atteinte aux droits des titulaires. Aujourd'hui, en 2024, il est nécessaire de revoir la législation sur les noms de domaine. L'ICANN, créée en 1998, a réussi à dompter l'émergence du www et protéger les titulaires des droits avec la création d'une procédure de règlement des litiges. Une mise à jour du système des noms de domaine est indispensable afin de prendre en compte toutes ces évolutions pouvant devenir des menaces si elles ne sont pas maîtrisées …

[51] Article 5, China ccTLD Dispute Resolution Policy
[52] Article 2, China ccTLD Dispute Resolution Policy

Partie II – Une révision nécessaire pour une meilleure protection

Face à l'émergence de ces différents noms de domaine et aux diverses conséquences qui en découlent, on assiste, aujourd'hui, à une perte de contrôle de la part de l'ICANN. Il s'agit du seul organe central existant à ce jour pour les noms de domaine et celui-ci ne prend pas en compte l'ensemble des difficultés que l'on rencontre. Dès lors, l'un des défis majeurs est la révision du système des noms de domaine. En effet, le système actuel n'envisage pas les noms de domaine en blockchain, signifiant que les cybersquatteurs peuvent porter atteinte à ces signes distinctifs sans qu'il existe de procédure pouvant les en empêcher (Chapitre 1). Par ailleurs, une harmonisation des législations des États membres de l'Union Européenne pourrait être un moyen d'étendre la protection dans les diverses législations européennes afin d'avoir un encadrement commun (Chapitre 2).

Chapitre 1 – Les noms de domaine en blockchain, les grands oubliés

La création du système de blockchain est apparue en 2008 permettant ainsi l'émergence d'un nouveau système de nommage avec la création des noms de domaine décentralisés. Néanmoins, c'est un système qui n'est soumis à aucun contrôle d'un organe indépendant laissant place à un vide législatif qui peut s'avérer néfaste face à la menace du cybersquatting. Toutefois, même s'il n'existe aucune législation spécifique à ce système de nommage, il y a eu quelques évolutions notables qui sont certes insuffisantes mais qui marquent un début d'évolution (Section 1). Il serait envisageable d'imaginer une situation future dans laquelle des aménagements seraient pris (Section 2).

Section 1 – La situation actuelle

Il est intéressant de se d'analyser, même s'il n'est pas directement fait référence aux noms de domaine enregistrés sur une blockchain, à la loi PACTE de 2019[53] et au règlement européen 2023/1114 sur les marchés de crypto-actifs, autrement appelé le règlement MiCA, publié au Journal officiel de l'Union Européenne le vendredi 9 juin 2023. Toutefois, ce cadre harmonisé européen ne va venir remplacer les cadres nationaux mis en place qu'à compter du

[53] Loi n°2019-486 relative à la croissance et la transformation des entreprises, 22 mai 2019

30 décembre 2024. Cela signifie, que pour l'instant l'offre au public et l'admission aux négociations de jetons, la fourniture de services sur crypto-actifs par des prestataires et la prévention des abus de marché sur cryptos actifs sont encore régis par les législations nationales[54]. Ce règlement rend l'agrément des prestataires de services sur actifs numériques obligatoire afin qu'ils puissent fournir leurs services dans toute l'Union européenne.

Ce règlement européen peut être un tremplin et une inspiration pour la réglementation de la création et de l'utilisation des noms de domaine créés sur les blockchains. En effet, en plus de la nécessité d'obtenir l'agrément, ces prestataires de crypto-actifs vont être soumis à une série d'obligations. À titre d'exemple, ils auront l'obligation d'agir de manière honnête, loyale et professionnelle « *au mieux des intérêts des clients* »[55], c'est-à-dire que ceux-ci doivent fournir « *des informations loyales, claires et non trompeuses, y compris dans leurs communications commerciales* » et ils doivent également avertir leurs clients des risques liés aux transactions portant sur des crypto-actifs. De cette obligation, on peut y voir un moyen de défense pour le titulaire du droit de marques. Si un nom de domaine décentralisé porte atteinte à un droit de marques, le prestataire qui détient ce nom de domaine frauduleux et qui le revend fait preuve de déloyauté envers son client ou de négligence si celui-ci ne savait pas qu'il s'agissait d'un nom de domaine frauduleux.

Outre ce règlement européen et ces dispositions du droit commun classique, il existe des décisions récentes qui peuvent avoir une influence sur la création de jetons non fongibles et leur réglementation au vu de la protection fournie par la propriété intellectuelle. À titre de référence, il faut mentionner l'affaire Metabirkin, M. Rothschild contre Hermès[56], une décision de la Southern District Court of New York. En l'espèce, Mason Rothschild avait émis et commercialisé en 2021 une série de 100 NFTs intitulés « MetaBirkins » liés à des images digitales représentant des sacs « Birkin », sac iconique de la marque Hermès, déclinés en plusieurs couleurs et recouverts de fausse fourrure. C'est en janvier 2022, qu'Hermès a initié une action judiciaire devant la Cour de New York sur plusieurs fondements et notamment la contrefaçon des marques verbales « BIRKIN », la reproduction illicite du design du sac et le cybersquatting du nom de domaine « metabirkins.com » portant atteinte à la marque

[54] « Marchés de crypto-actifs : publication du règlement européen MiCA », 12 juin 2023, Autorité des Marchés Financiers
[55] Article 66 du règlement MiCA
[56] United States District Court of the Southern District of New York, Hermes Int'I v. Rothschild, No. 22-CV-384-JSR, 2023 WL 1458126 du 2 février 2023.

« BIRKIN ». Le défendeur faisait valoir sa liberté d'expression, à savoir que cette collection numérique de jetons a été créée en vue d'être une reproduction artistique de ce sac emblématique de la maison Hermès et par conséquent que cette création « artistique » tombait sous la protection du premier amendement de la Constitution Américaine. Néanmoins, la Cour n'a pas retenu cette défense et un jury composé de 9 personnes a tranché en faveur d'Hermès International et à condamner l'artiste américain coupable des différents griefs. Du point de vue de la propriété intellectuelle, cette décision est très intéressante car, d'une part, les jetons non fongibles ne peuvent être vus comme détenant un aspect artistique supplantant sa nature intrinsèquement transactionnelle et d'autre part que l'on soit dans l'univers physique ou dans le Metavers, tout usage non autorisé dans la vie des affaires peut constituer un acte de contrefaçon au sens de l'article L711-2 du Code de la propriété intellectuelle (CPI).

Dès lors, en 2024, l'utilisation d'un nom de domaine sur blockchain portant atteinte à la marque d'un titulaire pourra être condamnée par le chemin classique de la contrefaçon.

Pourtant, en 2023, le système ENS qui est le système de nommage sur blockchain le plus utilisé dans le mode, comptait 2,8 millions de noms de domaine en .ETH détenus par 648 000 titulaires différents[57]. Ce chiffre ne prend pas en compte les autres systèmes de nommage sur blockchain, donc il existe à l'heure actuelle des millions de noms de domaine sur blockchain et aucune organisation n'a été fondée pour faire face à cet engouement. Il est dès lors indispensable de considérer l'ensemble des systèmes de nommage basés sur la blockchain, actuellement non soumis au contrôle d'un organe indépendant. Pour cela, il serait opportun d'anticiper une évolution future où ces systèmes seraient encadrés, afin de garantir leur compréhension, leur stabilité et de prévenir toute dérive.

Section 2 – La situation future

L'ICANN a été créée pour réguler et gérer la stabilité d'internet. Néanmoins, aujourd'hui, en 2024, nous sommes face à la croissance exponentielle des noms de domaine sur blockchain. Ils ne sont pas reconnus par l'ICANN et par conséquent, il n'existe aucune procédure extrajudiciaire de règlement des litiges permettant la récupération de ce type de nom de domaine. Ainsi, une question majeure se pose actuellement : l'ICANN reste-t-elle suffisante

[57] « Noms de domaine NFT », Solidnames

pour assurer la stabilité d'internet en 2024 ? La non-reconnaissance des noms de domaine décentralisés fait que la réponse à cette question bascule vers la négative. Néanmoins, des solutions peuvent être trouvées. En effet, dans un futur proche, nous pourrions envisager deux possibilités : la première est la création d'un nouvel organe et la seconde est l'élargissement des compétences de l'ICANN. La première possibilité semble être la plus envisageable et la plus intéressante.

Tout d'abord, la plus envisageable puisque l'ICANN gère déjà tout le système DNS, toute une nomenclature a été créée autour de cette organe qui gère en tout 13 serveurs racine, rajouter en plus le système de nommage sur blockchain risquerait de compromettre l'objectif premier de cet organe qui est la stabilité d'internet puisque cela additionnerait tout un système inconnu à l'heure actuelle. Par ailleurs, l'ICANN n'est pas familière avec l'esprit de la blockchain, elle ne connaît pas ses enjeux et ses contours. Enfin, il est important de rappeler la raison principale : les noms de domaine en blockchain ont été conçus précisément pour être indépendants et échapper aux exigences de l'ICANN. Confier cet écosystème à l'ICANN irait donc à l'encontre même de l'idée fondatrice de la blockchain.

Il s'agit également de l'hypothèse la plus intéressante puisque, à ce jour, on peut faire un parallèle avec une évolution déjà observée en 1998. En effet, à la fin des années 1990 il y a eu un tel emballement autour des noms de domaine qu'est née la nécessité de confier la gestion de ce système DNS à un organe personne morale afin que ce réseau puisse évoluer et gagner en importance. De là, a découlé la création d'une procédure applicable à ces noms de domaine qui est la procédure UDRP. Ainsi, en 2024, nous nous retrouvons dans la même configuration à savoir la nécessité de créer un organe à qui on va confier la gestion du système de nommage sur blockchain et ainsi on pourrait envisager la création d'une procédure UDRP spécialisée, applicable aux noms de domaine enregistrés sur une blockchain.

Certains auteurs proposent également une collaboration entre les plateformes de NFT et certains centres de médiation et d'arbitrage reconnus. Néanmoins, pour arriver à une telle solution, il faudrait que ces plateformes de NFT adoptent des principes de résolution des litiges

et que ces centres reconnaissent les principes mis en place par ces plateformes et les mettent en œuvre[58].

Par ailleurs, le règlement MiCA peut servir de pilier pour une éventuelle création d'un nouveau règlement européen spécifique aux noms de domaine en blockchain. Un tel règlement peut, potentiellement par la suite, servir de modèle pour une harmonisation internationale. Nous reviendrons ainsi à la même situation que dans les années 1990, c'est-à-dire que face à l'émergence des noms de domaine en blockchain, il devient nécessaire de mettre en place un système de gestion des noms de domaine en blockchain, regroupant ceux existant et qui se multiplient au fil des années, pour que l'ensemble de ces registres obéissent à une politique commune qui pourrait être inspirée du règlement MiCA. Tout cet écosystème autour des noms de domaine en blockchain peut être certes craint, comme la création de l'ICANN en 1998, néanmoins nous sommes aujourd'hui face à une insécurité puisque chaque registre proposant des noms de domaine décentralisés sont soumis à leur propres règles et lois et aucune procédure ne permet de protéger les titulaires de droit.

Outre la nécessité de prendre en compte de tels noms de domaine, une harmonisation européenne des noms de domaine en générale est une étape importante afin d'arriver à un système plus sûr.

Chapitre 2 – Une harmonisation des législations des États membres de l'Union européenne

Un début d'harmonisation est en cours au sein de l'Union européenne (Section 1) mais ce ne sont que de timides débuts. Il faut s'interroger sur la manière dont elle est appréhendée, perçue et sur les possibles obstacles que ce projet d'harmonisation peut rencontrer (Section 2).

[58] « La règlementation des NFT à la lumière du droit international privé : réglementation étatique ou extra-étatique ? » Yves El Hage, maître de conférences à l'université Jean Moulin Lyon 3 – Revue droit bancaire et financier n°4 Juillet-Aout 2022

Section 1 – Les timides débuts d'une harmonisation européenne

Cette harmonisation a débuté par l'adoption d'une réglementation spécifique aux noms de domaine en « .eu » qui s'est faite au travers de deux règlements : le règlement n°733/2002 du 22 avril 2002 concernant la mise en œuvre du domaine de premier niveau .eu et le règlement n°874/2004 du 28 avril 2004 établissant les règles de politique d'intérêt général relatives à la mise en œuvre et aux fonctions du domaine de premier niveau .eu et les principes applicables en matière d'enregistrement. Initialement, uniquement les détenteurs de marques déposées et les organismes publics pouvaient enregistrer un nom de domaine en .eu. Cependant, à partir du 7 février 2006, cette possibilité a été élargie aux titulaires de droits antérieurs, notamment aux personnes détenant des enseignes par exemple. À partir du 7 avril 2006, cette faculté a été ouverte à tous, c'est à dire aux entreprises, associations, particuliers. La seule condition à respecter pour obtenir un nom de domaine en .eu est d'être établie ou de résider dans l'Union européenne[59]. Ces deux règlements ont été abrogés par le règlement n°2019/517 du 19 mars 2019 concernant la mise en œuvre et le fonctionnement du nom de domaine de premier niveau .eu. Il est entré en vigueur le 18 avril 2019 et est applicable depuis le 13 octobre 2022.

Une organisation privée, indépendante, à but non lucratif a été créée, dès l'adoption du règlement de 2002, afin de gérer ces noms de domaine .eu. Il s'agit du registre européen des domaines Internet, EURid. La Commission Européenne, le 25 octobre 2021, a adopté une décision désignant ce même registre en tant que registre TLD .eu de 2022 à 2027.

Pour contester l'enregistrement d'un nom de domaine en .eu, l'article 22 du règlement de 2004[60] organise une procédure alternative de règlement extrajudiciaire de litiges spécifique à ces noms de domaine que l'on va présenter comme la procédure ADR, *Alternative Dispute Resolution*. Cette procédure est proposée par deux centres accrédités : le centre d'arbitrage et de médiation de l'OMPI et en 2005, la Cour d'arbitrage tchèque désigné par l'EURid. Cette procédure a été initialement posée par l'article 5 du règlement concernant la mise en œuvre du domaine de premier niveau .eu de 2002[61].

---

[59] *Cyberdroit : le droit à l'épreuve de l'Internet*, Section 4 – Extensions géographiques, linguistiques ou culturelles, Christiane Féral-Schul, 7e édition, Dalloz, 2018-2019

[60] Règlement (CE) n°874/2004 de la Commission du 28 avril 2004 établissant les règles de politique d'intérêt général relatives à la mise en œuvre et aux fonctions du domaine de premier niveau .eu et les principes applicables en matière d'enregistrement

[61] Règlement (CE) n°733/2002 du Parlement européen et du conseil du 22 avril 2002 concernant la mise en œuvre du domaine de premier niveau .eu complété par le règlement (CE) n°874/2004

Ses principes de fonctionnement s'inspirent de ceux retenus par l'ICANN dans le cadre de la procédure UDRP. Toutefois, il existe quelques différences entre les principes UDRP et les règles ADR. Tout d'abord, en ce qui concerne les droits protégés, les principes UDRP se limitent à la protection du droit de marques alors que les règles ADR vont plus loin et visent à protéger des dénominations faisant l'objet d'un droit reconnu ou établi par le droit national d'un État membre et/ou le droit de l'Union Européenne. Et notamment, il est intéressant de constater que dans le nouveau règlement 2024/1143[62] spécifique aux indications géographiques en matière industrielle et artisanale, son article 35 dispose que « *les registres de noms de domaine de premier niveau nationaux établis dans l'Union garantissent que toute procédure de règlement extrajudiciaire des litiges relative aux noms de domaine reconnaissent les indications géographiques enregistrées comme un droit pouvant être invoqué dans le cadre de ces procédures* ». En outre, en ce qui concerne les conditions, les principes UDRP demandent d'établir cumulativement les 3 conditions suivantes : la mauvaise foi du registrant, le manque d'intérêt légitime du registrant et le risque de confusion alors que selon les règles ADR, le requérant doit démontrer pourquoi le nom de domaine litigieux est identique ou similaire au nom sur lequel porte le droit reconnu ou établi en vertu du droit national et/ou communautaire ou d'un titre légitime portant sur le nom de domaine litigieux ou pourquoi le nom de domaine litigieux devrait être considéré comme étant enregistré ou utilisé de mauvaise foi. Et enfin, en ce qui concerne la mauvaise foi, la procédure UDRP exige un enregistrement et une utilisation de mauvaise foi tandis que les règles ADR ne demandent de prouver que l'un des deux, même si en pratique on constate que les experts UDRP développent des théories permettant de ne prouver que l'un des deux.

Par ailleurs, il existe aujourd'hui la recommandation (UE) 2024/915 de la Commission du 19 mars 2024 relative à des mesures visant à lutter contre la contrefaçon et à renforcer le respect des droits de propriété intellectuelle. Il s'agit d'une grande étape dans le renforcement des défenses contre la contrefaçon puisque celle-ci introduit des mesures pour renforcer la coopération entre les titulaires de droits, les prestataires de services intermédiaires et les autorités compétentes. En effet tout un chapitre est dédié à « *favoriser la coopération, la coordination et le partage d'informations afin de protéger l'innovation et les*

[62] Règlement (UE) 2024/1143 du Parlement européen et du Conseil du 11 avril 2024 concernant les indications géographiques relatives au vin, boissons spiritueuses et aux produits agricoles, ainsi que les spécialités traditionnelles garanties et les mentions de qualité facultatives pour les produits agricoles

investissements »[63] dans lequel on retrouve un point consacré aux fournisseurs de noms de domaine et qui vise à « *garantir la protection des droits de propriété intellectuelle dans le système des noms de domaine* ». Pour assurer cette mission, elle recommande notamment aux registres de noms de domaine de premier niveau établis dans l'UE et/ou proposant des services dans l'UE de « *coopérer et à collaborer avec l'EUIPO sur la base d'accords volontaires afin de reproduire pour les noms de domaine de premier niveau qu'ils gèrent le système d'information et d'alerte existant actuellement exploité par l'EUIPO et EURid pour les marques de l'Union européenne et le nom de domaine de premier niveau « .eu » et d'élargir la couverture aux indications géographiques enregistrées* »[64], cette mesure est intéressante puisqu'elle permet au titulaire d'indication géographique de lutter contre un potentiel cybersquatteur qui use de l'indication géographique pour en faire un nom de domaine. Et avant même cette recommandation, le 4 décembre 2023, le directeur exécutif de l'EUIPO, João Negrão, et le directeur général de l'OMPI, Daren Tang, ont exprimé leur volonté de renforcer la coopération entre leurs organisations. À cette fin, ils ont signé un mémorandum d'accord lors d'une réunion virtuelle[65].

Dès lors, même s'il s'agit de timides débuts vers une harmonisation européenne, il est tout de même opportun de prévoir la mise en place et le futur d'une telle harmonisation.

Section 2 – La mise en place et le futur de l'harmonisation européenne

Il est intéressant de s'interroger sur les aspects positifs d'une telle harmonisation. Tout d'abord, celle-ci permet de mettre en place un registre spécifique pour les noms de domaine en .eu, une initiative plus qu'appréciable au vu de l'augmentation des noms de domaine en .eu ces dernières années. En effet, 3,72 millions de noms de domaine en .eu ont été enregistrés en octobre 2023 faisant le TLD.eu le neuvième plus grand TLD de code de comté au monde. Il a été, dès lors, indispensable de mettre en place un tel registre. Par ailleurs, la Commission le dit elle-même « *le domaine de premier niveau .eu donne à l'Europe sa propre identité Internet, renforçant la visibilité de l'UE, élargissant le choix des noms de domaine par les utilisateurs*

[63] Chapitre 2 de la recommandation (UE) 2024/915 de la Commission du 19 mars 2024 relative à des mesures visant à lutter contre la contrefaçon et à renforcer le respect des droits de propriété intellectuelle
[64] Point 14-b) de la recommandation (UE) 2024/915
[65] « L'EUIPO et l'OMPI renforcent leur coopération dans des domaines clés » site de l'EUIPO, https://www.euipo.europa.eu/fr/news/euipo-and-wipo-to-strengthen-cooperation-in-key-areas

et promouvant le commerce électronique »[66] d'autant que le TLD .eu permet aux utilisateurs de créer une identité Internet paneuropéenne pour leurs sites Web et leurs adresses e-mail, tout ce système permet ainsi de rendre l'Union européenne attractive dans le monde. Enregistrer un tel nom de domaine permet à la marque du titulaire d'avoir une visibilité paneuropéenne unique, à savoir que l'on compte en 2023 près de 448,4 millions d'habitants dans l'Union européenne[67].

En outre, une telle harmonisation pourrait inciter d'autres pays de l'Union européenne, qui ne disposent pas de procédure alternative de règlement des litiges en dehors de l'UDRP, à adopter des principes similaires. C'est notamment le cas de l'Allemagne, la Roumanie ou le Monténégro par exemple[68]. Cette démarche pourrait non seulement encourager la création de telles procédures, mais également la mise en place de centres accrédités, afin d'éviter de surcharger les centres existants, comme celui de l'OMPI.

Enfin, la mise en place d'une procédure locale spécifique pourrait s'avérer utile, notamment pour combler les lacunes de la procédure UDRP, qui ne s'applique qu'en cas d'atteinte à un droit de marque. On peut également se demander si l'existence d'une telle procédure locale contribue à rendre un nom de domaine plus attractif. À titre d'exemple, pour le domaine en .eu, l'Union européenne a instauré une procédure ADR, et on note une croissance constante du nombre de noms de domaine européens enregistrés.

[66] « Bâtir l'avenir numérique de l'Europe », Commission Européenne
[67] Annexe 5, p.34- https://european-union.europa.eu/principles-countries-history/key-facts-and-figures/life-eu_fr
[68] « Service de règlement des litiges relatifs aux noms de domaine pour les domaines correspondant à des codes pays (ccTLD) », site de l'OMPI - https://www.wipo.int/amc/fr/domains/cctld/index.html

Conclusion

La protection des signes distinctifs face au développement du cybersquatting est un enjeu majeur à l'échelle internationale. Le développement de nouvelles technologies, de nouvelles méthodes de stockage telle que la blockchain est venu complexifier le système DNS prouvant la nécessité d'améliorer et de modifier ce qui existe aujourd'hui. Le système DNS n'est plus suffisant, ne signifiant pas pour autant son inefficacité. En effet, il est toujours utile pour les litiges entre un titulaire d'une marque et un nom de domaine enregistré dans ce système de nommage et portant atteinte à ses droits. La difficulté réside dans une prise en compte timide de son système rival qui est celui de la blockchain qui de nos jours n'obéit à aucune politique commune créant par conséquent une insécurité pour les titulaires de droits de marques. Certes, il existe un début d'harmonisation, tels que le règlement MiCA, mais ceux-ci ne sont pas, d'une part, spécifiques aux noms de domaine et d'autres part, ils ne sont pas internationaux mais européens. Néanmoins, ils peuvent être utiles pour la création d'un système de nommage sur blockchain qui doit indubitablement être international.

En outre, il est nécessaire également de sanctionner plus sévèrement le cybersquatting inversé, c'est-à-dire la pratique consistant à un titulaire d'une marque d'acquérir un nom de domaine légitimement enregistré par un tiers en utilisant la procédure UDRP mais de manière abusive. Comme constaté, les sanctions mises en place à l'heure actuelle ne sont pas dissuasives et nécessitent dès lors une révision.

Par ailleurs, pour lutter contre le cybersquatting, des outils commencent à voir le jour tels que GlobalBlock et GlobalBlock+ qui sont des dispositifs permettant « *d'obtenir, en une opération, le blocage automatique, au niveau des registres, de la réservation de noms de domaine identiques ou similaires à un signe distinctif éligible sur plus de 500 extensions* »[69]. Parmi ces 500 extensions, on compte des extensions géographiques, telles que « .barcelona », de nouvelles extensions, telles que « .gifts » ainsi que des extensions de noms de domaine décentralisés, telles que « .crypto ». De nombreuses extensions ne sont pas couvertes par ces dispositifs, notamment les extensions génériques de premier niveau, telles que le « .com », sachant que ces catégories de noms de domaine correspondent à plus de 36% de tous les noms

[69] « GlobalBlock : un nouveau dispositif de lutte contre le cybersquatting », Fabrice Bircker et Mira Haddag, 13 mars 2024, Cabinet Plasseraud

de domaine enregistrés dans le monde en 2024[70]. Néanmoins, si ces dispositifs répondent correctement à cet objectif de protection, ils pourront dans un futur proche couvrir davantage d'extensions. De plus, ces dispositifs de blocage ont un champ d'application plutôt large puisqu'ils sont ouverts aux titulaires de marques enregistrées, de marques d'usage, de dénominations sociales et de noms de célébrités.

Enfin, l'intelligence artificielle peut également être une aide dans la surveillance de marques. En effet, des outils de surveillance basés sur l'IA pourraient permettre aux titulaires de marques de surveiller un grand nombre de noms de domaine en continu, détectant rapidement toute tentative de cybersquatting.

[70] « GlobalBlock : analyse des avantages et des limites de ce nouveau système de blocage pour les noms de domaine », Nathalie Dreyfus, 12 mars 2024

Bibliographie

a. Dictionnaires

Vocabulaire de l'Internet et de l'informatique publié par la Commission de terminologie française JORF n°63, 16 mars 1999

b. Ouvrages et thèses

Cyberdroit : le droit à l'épreuve de l'Internet, Section 4 – Extensions géographiques, linguistiques ou culturelles, Christiane Féral-Schul, 7e édition, Dalloz, 2018-2019

Democracy and its critics, New Haven and London, 1989, Robert Alan DAHL

Droit de la propriété industrielle, Jean-Christophe Galloux et Jacques Azéma, 8e edition, Paris, Dalloz, 2017

Géopolitique de l'Internet, Olivier Ricou, version 3.1 du 2 aout 2023

Noms de domaine et modes alternatifs de règlement de conflits, Radmila Pavlenko épouse Chapuis, Université Paris 2 Panthéon-Assas, 2021

c. Revues et articles

« Bâtir l'avenir numérique de l'Europe », Commission Européenne

« Bilan 2023 du .fr : Plus de 40% des noms de domaine en France sont en .fr » Actualité de l'AFNIC publiée le 26 mars 2024

« Combien existe-t-il de noms de domaine en 2020 ? », Jean-François Poussard, 4 mars 2020 Solidnames

« Cryptoactifs, cryptomonnaies : de quoi s'agit-il ? » Ministère de l'Économie, des finances et de la souveraineté industrielle et numérique, economie.gouv.fr

« Élaboration de politiques », site de l'ICANN

« Enchères record pour le .web, vendu à 135 millions de dollars », Équipe éditoriale IONOS, le 30/11/2022

« Ethereum Name Service : plus de 2 millions de noms de domaine .eth enregistrés », Le Journal du Coin le 24 août 2022

« GlobalBlock : analyse des avantages et des limites de ce nouveau système de blocage pour les noms de domaine », Nathalie Dreyfus, 12 mars 2024

« GlobalBlock : un nouveau dispositif de lutte contre le cybersquatting », Fabrice Bircker et Mira Haddag, 13 mars 2024, Cabinet Plasseraud

« La règlementation des NFT à la lumière du droit international privé : réglementation étatique ou extra-étatique ? » Yves El Hage, maître de conférences à l'université Jean Moulin Lyon 3 – Revue droit bancaire et financier n°4 Juillet-Aout 2022

« Le cybersquatting est-il un acte de cybercriminalité ? » Chronique 7 octobre 2008

« L'EUIPO et l'OMPI renforcent leur coopération dans des domaines clés » site de l'EUIPO

« Marchés de crypto-actifs : publication du règlement européen MiCA », 12 juin 2023, Autorité des Marchés Financiers

« Nom de domaine – Dernières tendances chez l'OMPI : une forte croissance des litiges sur les noms de domaine en 2023 » – Propriété industrielle n°4, Avril 2024, alerte 30 – Cabinet Dreyfus

« Noms de domaine NFT », Solidnames

« Rachat nom de domaine », Solidnames

« Service de règlement des litiges relatifs aux noms de domaine pour les domaines correspondant à des codes pays (ccTLD) », site de l'OMPI

« The UDRP « Celebrates » Its 500th Reverse Domain Name Hijacking Case », by Zak Muscovitch, General Counseil, Internet Commerce Association, CircleID

« Total Number of Domain Names by Years », site de l'OMPI

d. Jurisprudences

1. AFNIC

Décision de l'AFNIC, entiledefrance.fe, Demande n°FR 2024-03882, 7 juin 2024

2. Centre d'arbitrage et de médiation de l'OMPI

WIPO Arbitration and Mediation Center, Case No D2000-0021, Ingersoll-Rand Co. Vs. Gully, March 9, 2000

WIPO Arbitration and Mediation Center, Case No D2000-0016, Allocation Network GmbH v. Steve Gregory, March 24, 2000

WIPO Arbitration and Mediation Center, Case No D2000-1698 Arthur Guiness Son&Co (Dublin) Limited v. Dejan Macesic, January 25, 2001

WIPO Arbitration and Mediation Center, Case No D2000-1123, Teranet Land Information Services Inc. v. Verio Inc, January 25, 2001

WIPO Arbitration and Mediation Center, Case No D2001-0970, Briefing.com Inc v. Cost Net Domain Manager, September 12, 2001

WIPO Arbitration and Mediation Center, Case No D2009-0643, City Viexs Limited v. Moniker privacy Services / Xander, Jeduyu, Algebralive, July 3, 2009

WIPO Arbitration and Mediation Center, Case No D2024-0151 Mermet SAS v. Didier Mermet, mermet.com, March 12, 2024

3. Conseil Constitutionnel

Conseil Constitutionnel, 6 octobre 2010, n°2010-45 QPC, D.2010.2285

4. Nominet

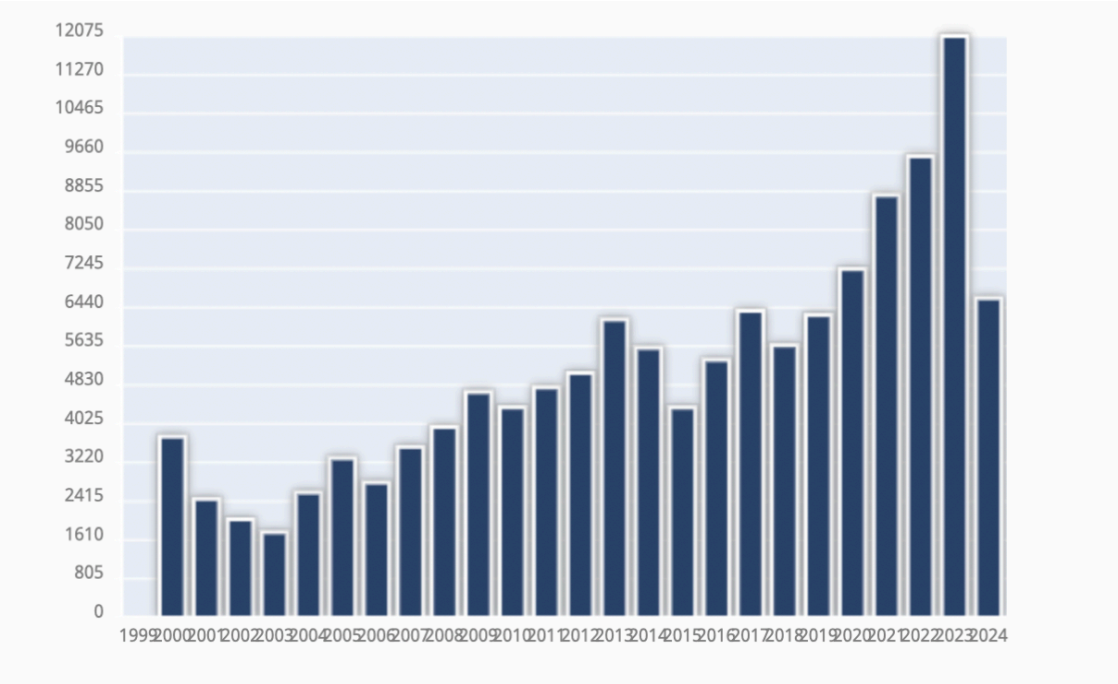
DRS No 04849, record-power.co.uk du 19 septembre 2007

5. United States District Court

United States District Court of the Southern District of New York, Hermes Int'I v. Rothschild, No. 22-CV-384-JSR, 2023 WL 1458126 du 2 février 2023.

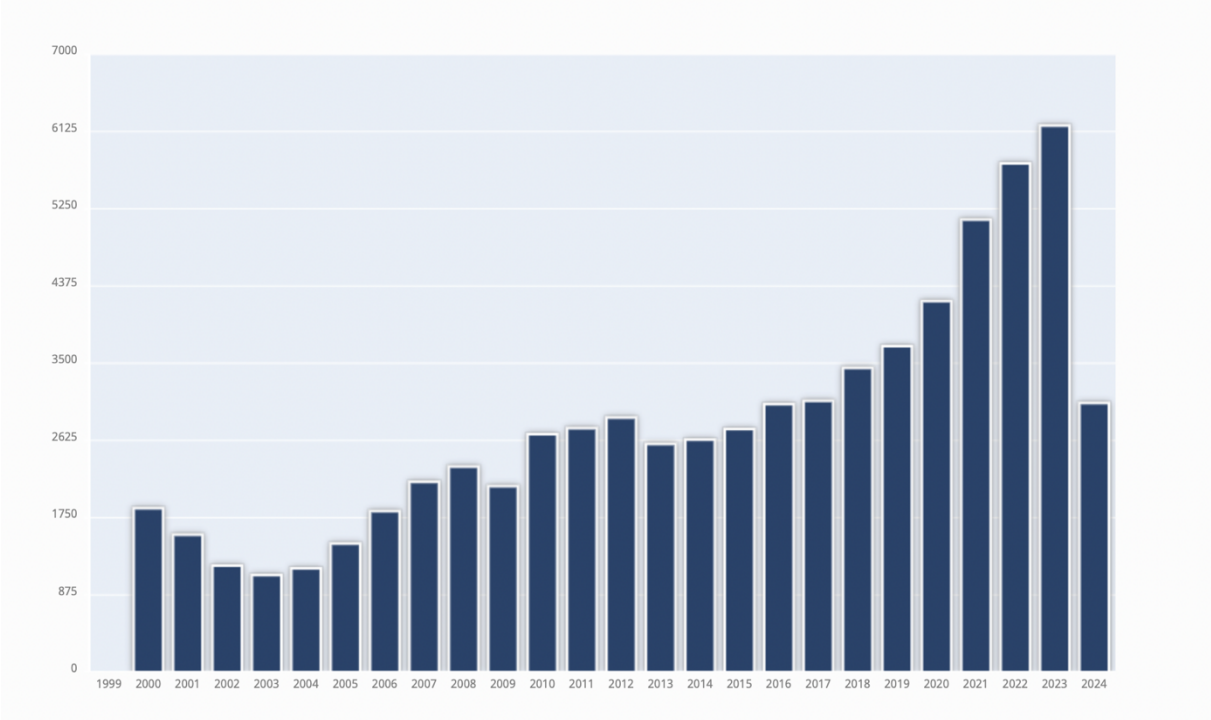
Annexes

Annexe 1 :



Nombre totale de noms de domaine par an – Site de l'OMPI

Annexe 2 :



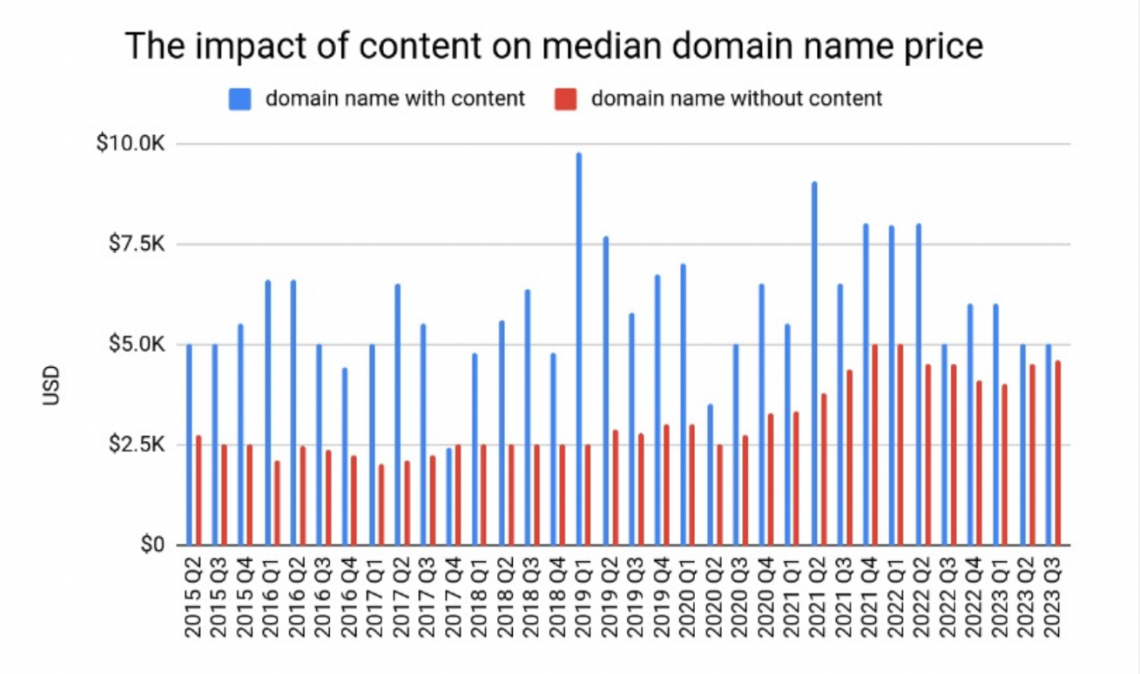
Nombre totale de litiges par an – Site de l'OMPI

Annexe 3 :

	2019	2020	2021	2022	2023	Total
.FR	0,5	0,3	0,8	0,6	0,9	**+ 3,1**
.COM	0,6	– 0,6	0,6	– 0,5	-0,8	**-0,7**
Autres Legacy	-0,8	– 0,3	– 0,3	– 0,3	-0,2	**– 1,9**
Autres ccTLD	– 0,2	– 0,4	– 0,2	– 0,1	0,0	**– 0,9**
nTLD	– 0,1	1,0	– 0,9	0,3	-0,4	**– 0,4**

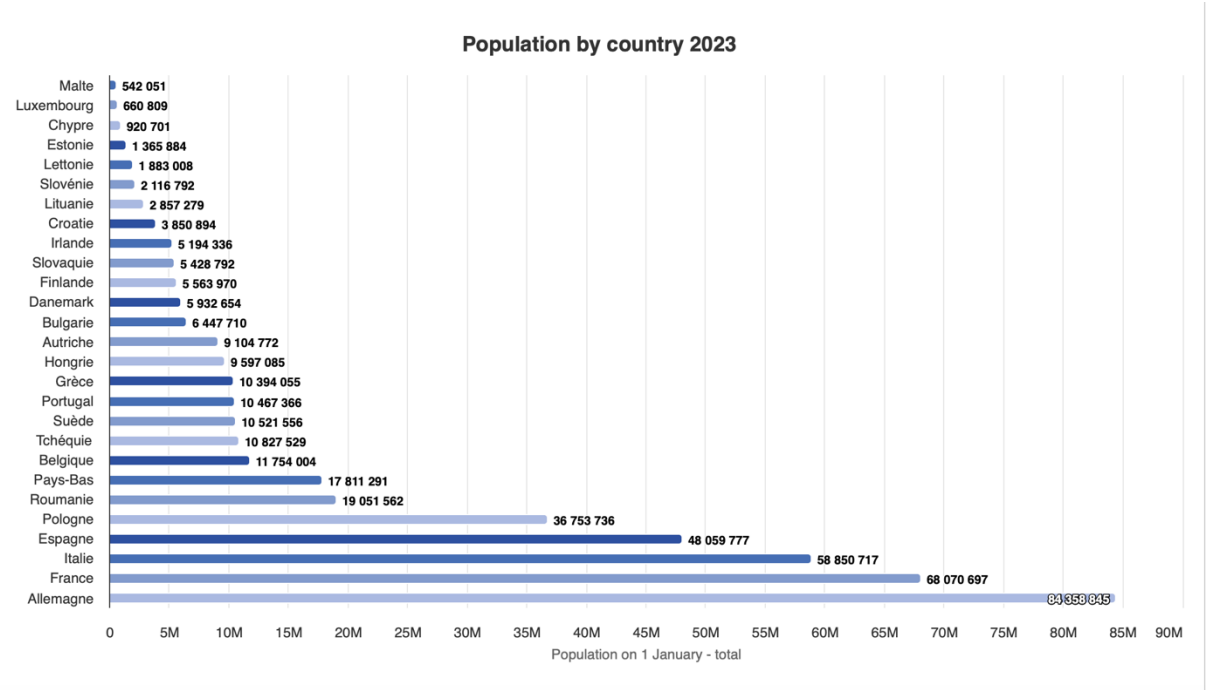
Variations des parts de marché en France (2019 – 2023)

Annexe 4 :



Prix moyen d'un rachat de noms de domaine chez Escrow au fil des années

Annexe 5 :



Population de l'Union européenne par État membre en 2023