DOCTORAL THESIS

DOMAIN NAME VS. TRADEMARK AND PROBLEMATIC ISSUES IN CYBERSPACE

MARTON GÉZA DOCTORAL SCHOOL OF LEGAL STUDIES
DEBRECEN UNIVERSITY

Supervisor
A.P. Bartha Ildikó

Candidate:

Fahed Wahdani

Doctoral Program: Changes in State and Law in Central and Eastern Europe
Head of the Doctoral School: Prof. Dr. József Szabadfalvi, DSc, Professor of Law
The manuscript was completed on July 31, 2023
DEBRECEN
2023

NYILATKOZAT

Alulírott, Fahed A. Fahed Wahdani (név), büntetőjogi felelősségem tudatában kijelentem, hogy a Debreceni Egyetem Marton Géza Állam- és Jogtudományi Doktori Iskolában a doktori fokozat megszerzése céljából benyújtott, „Domain Name vs. Trademark and Problematic Issues in Cyberspace" című értekezésem saját önálló munkám, a benne található, másoktól származó gondolatok és adatok eredeti lelőhelyét a hivatkozásokban (lábjegyzetekben), az irodalomjegyzékben, illetve a felhasznált források között hiánytalanul feltüntettem.

Kijelentem, hogy a benyújtott értekezéssel azonos tartalmú értekezést más egyetemen nem nyújtottam be tudományos fokozat megszerzése céljából.

Tudomásul veszem, hogy amennyiben részben vagy egészben sajátomként mutatom be más szellemi alkotását, vagy az értekezésben hamis, esetleg hamisított adatokat használok, és ezzel a doktori ügyben eljáró testületet vagy személyt megtévesztem vagy tévedésben tartom, a megítélt doktori fokozat visszavonható, a jogerős visszavonó határozatot az egyetem nyilvánosságra hozza.

Debrecen, 2023/08/20

aláírás

SUPERVISOR'S OPINION

on Mr. Fahed Wahdani's dissertation to be submitted for preliminary defense

Debrecen, 31 August 2023

Mr. Fahed Wahdani's dissertation focuses on regulatory questions of the domain names as digital trademark in cyber space, and some recent challenges related to this issue. In his approach, in the light of the digital revolution, the need for protection of rights of domain name owners emerges as a new challenge for intellectual property rights (IPR) regulatory regimes in Europe and all over the world. The main scientific question of Fahed's PhD research is the applicability of IPR to domain name disputes, i. e. whether the legislative instruments of IPR and related conflict resolution mechanisms are able to follow the development of information technology and risks in cyber space, and whether they can provide an effective protection for domain name (as digital trademark) owners' rights.

Recent challenges in the protection of intellectual property rights are among the most contested issues in international trade relations and also a key issue from the point of view of EU economic law. The importance of the research topic is thus undeniable, both in the international context and from a European perspective.

The thesis is built on a multidisciplinary approach, sociological and economic analysis thus supplement the strict legal dimension of the research. Fahed examines these legal and regulatory problems in the context of the relevant international legislation (in particular the WIPO and TRIPS agreements), the laws and policies of the European Union and the rules of the United States. After introducing the conceptual framework of domain names and trademarks, the thesis discusses the mechanism of the conflict between domain name owners and trademark holders (including the cybersquatting and reverse domain hijacking phenomena). Then, it examines the instruments (both the available judicial procedures and alternative dispute resolutions mechanisms) to resolve the conflict between owners of domain names and holders of trademarks. The thesis also devotes a detailed analysis for the impact of the COVID-19 pandemic on the domain names industry, highlighting recent problems of domain names

registration triggered by the coronavirus crise, the illegal use of domain names and the financial effect of the pandemic.

The final conclusions of the dissertation are based on a creative and comprehensive analysis.

In the preliminary defense of the dissertation, the candidate received critical regards and suggestions for revisions concerning the structure of the work, its language and the content of some parts. I believe that along these critics, the previous shortcomings have been corrected accordingly.

All in all, Fahed's work is convincing about his ability to identify the main research problems of the examined topic, to carry out in-depth research and to communicate the research result to the scientific community at a high level. The complex approach of the research theme proves the novelty of the present work. As the supervisor of the research, I support the acceptance of the dissertation for the final defense.

Dr. Ildikó Bartha, habil., Ph.D., supervisor
Professor of Law
University of Debrecen

Contents

Contents 1

Abbreviations 7

INTRODUCTION 9

1. The hypotheses of the thesis 9

2. Methodology 10

3 Thesis structures 11

4. Main concepts 13

4.1. Domain Name Cybersquatting 13

4.2. Reverse Domain Name Hijacking 14

4.3. In Rem Jurisdiction 15

5. The legal and regulatory environment examined in the dissertation 15

5.1 The relationship between the Lanham Act and the ACPA 16

5.2 ICANN as a non-governmental organization 16

5.3 UDRP rules 17

5.4 The relationship between WIPO and ICANN 17

5.5 WIPO regulatory instruments 18

5.6 Laws relating to jurisdiction conflict resolution 18

FIRST PART: THE LEGAL NATURE OF DOMAIN NAMES AND RECENT REGULATORY CHALLANGES 20

Chapter 1: Domain names as a digital trademark: the legal nature of domain names 20

1. The legal nature of domain names 20

1.1 Service contract 20

1.2 Stock ticker 23

1.3 Security interest 23

1.4 Address 24

1.5 Property rights 24

1.6 Domain name as a digital trademark 25

2. Can the domain name be registered as a trademark? US PTO v. Booking.com: A case study 27

2.1. The decision in the Booking.com case 27

2.2 Importance of the Booking.com Decision 28

2.3 Generic terms understanding 29

3. The European and American courts' case-law regarding the legal nature of domain names' cybersquatting 30
3.1 Unfair competition 31
3.2 Blackmail and commercial ransom 34
3.3 Passing off 35
Chapter 2: Search Engines and Domain Names 36
1. Background 36
1.1 Search engines definition 37
1.2 Search engines submerged 37
2. Area of the conflict between search engines and trademark 37
3. Metatags 38
3.1 Metatags concept 39
3.2 Usage of trademarks as meta tags 40
4. Keywords 41
4.1 Keywords, trademarks and consumer protection 42
4.2 The concept of the average consumer related to keyword ads 45
4. Metatags and trademark infringements in other jurisdictions 47
5. Conclusion 48
Chapter 3: Domain names immune against international crises: COVID-19 as a case study 49
1. The interaction between COVID-19 and the domain names industry 49
1.1 COVID-19 in the online space 50
1.2 Increase in domain name registration related to COVID-19 50
2. The COVID-19 pandemic's illegality in the domain names industry 52
2.1 COVID-19 Scam websites 53
2.2 COVID-19 domain names virus: Worm and Ransom 55
2.2.1 Worms and Malware 55
2.2.2 Ransom 56
2.3 COVID-19 pandemic impact on trademark counterfeiting 57
2.4 COVID-19 domain names and misleading information 58
3. COVID-19's financial effect on the domain name industry 62
3.1 COVID-19 domain names' registration cost 62
3.2 COVID-19 domain names' trade cost 62
3.3 COVID-19, investments and ethical questions 63
3.4 COVID-19 domain names advertisement cost 64
3.5 Covid-19 related domain names conflict cost 66

4. COVID-19 pandemic effect on government domain names 67
5. COVID-19 pandemic impact on the conflict in the domain names industry: The legal issue related to Covid trademark 68
SECOND PART: DOMAIN NAMES VS. TRADEMARK CONFLICT MECHANISM 71
Chapter 1: The role of registry agencies in generating conflicts between domain name owners and trademark holders 71
1. Competition over domain names 71
2. Bad management of domain names by formal registrar's institutions 74
Chapter 2: Cybersquatting and reverse domain hijacking phenomena 76
1. Domain names Cybersquatting institutions 76
2. The emergence of cybersquatting 77
3. The legal nature of domain name cybersquatting 77
3.1 First-come, first-served: Legitimizing of cybersquatting 77
3.2. First-come, first-served principle in light of trademark registration rules 79
3.3. Level of protection, granted by the first comes, first served principle 81
3.4. Trademark holders' behaviours 83
4. Reverse domain hijacking (RDNH) 83
4.1 Theoretical Framework for Reverse Domain name Hijacking 84
4.2 Mechanism of Reverse domain name hijacking 84
4.2.1 Reverse domain name hijacking under UDRP rules 85
4.2.2. Bad faith criteria 85
4.2.3. ACPA rules on Reverse domain name hijacking 87
4.2.4. Compensation for damages 89
5. Effects of Reverse domain hijacking 90
THIRD PART: RESOLVING DISPUTES UNDER DOMAIN NAME DISPUTE RESOLUTION POLICY (UDRP) 91
Chapter 1: ‘Uniform domain names dispute resolution policy: the ICANN's role 91
1. Mission 94
2. ICANN’s functions 94
3. ICANN nature and structure 95
4. ICANN accountability 96
Chapter 2 Domain name dispute resolution procedures 98
1. The aim of UDRP procedures 98
2 The scope of UDRP procedures 99
3. The operation of UDRP procedures 99

4. UDRP rules conditions 101
4.1 Domain is confusingly similar or the same as a trademark 101
4.2 Establishing rights to a domain name identical or confusingly similar to a trademark. 103
4.3 The registrant has no legal rights or interests in the registered domain name 104
4.4 Bad faith 106
5. UDRP rules “in partice” – the example of bpost.com 107
Chapter 3: ICANN Extra remedies 108
1. Right Protection Mechanisms 109
1.1 Legal right objection procedure 109
1.1.1 The criteria to determine the legal rights objection 111
1.1.2 Dispute settled under the legal rights objection 112
1.1.3 LRO remedies 112
1.1.4 Retain the Court options 112
1.2 Trademark Clearinghouse 112
1.2.1 Clearinghouse Mechanism and Functions 113
1.2.2. Clearinghouse importance 114
1.3 Uniform Rapid Suspension (URS) System 116
1.4. Post-delegation dispute resolution procedure (PDDRP) 117
1.4.1 Trademark Post-Delegation Dispute Resolution Procedure (TM-PDDRP) 117
1.4.2 Public interest commitments dispute resolution procedure (PICDRP) 118
1.4.3 The registration restriction dispute resolution procedure (RRDRP) 119
2. Remedies and Liability 119
Chapter 4: The domain name economy: Domain names’ value and their financial impact on domain name conflicts 120
1. Background 120
2. Financial effect of domain name conflict and the financial cost 121
2.1 Cybersquatting as the prototype to evaluate the financial effect of domain name conflict over stakeholders 121
2.2 Financial effect of domain name conflict resolution cost under UDRP rules 122
2.2.1 The financial cost of conflict resolution under UDRP rules 124
2.2.2 UDRP rules’ fee 124
2.3 Financial cost of conflict resolution under ACPA 125
PART FOUR: RESOLVING DOMAIN NAME DISPUTES BY JUDICIAL FORUMS (IN PARTICULAR IN AMERICAN JURISDICTION) 127
Chapter 1: Domain Names vs. Trademark in judicial proceedings 127
1. Anticybersquatting Consumer Protection Act (ACPA): a new legal framework 127

2. Conflict ground according to the ACPA (dilution and confusion) 129
2.1 Confusion 129
2.1.1 Confusion definition and criteria 130
2.1.2 The extent of the similarity of the domain name to the trademark 130
2.1.3. Offline trademark confusion vs. online domain names confusion 132
2.1.4 Generic top-level domain Names and Confusion 134
2.1.5. Criticism suffix vs. free speech right 134
2.1.6. Domain name confusion according to "gripe site." 135
2.1.7. Cybersquatting and Confusion 138
2.2 Domain names dilution 139
Chapter 2: Domain Names vs. trademark jurisdiction 141
1. Background 142
2. The causes of *in rem* jurisdiction conflict over domain names 143
2.1 ICANN lacking policy 143
2.2 Permit the Court to initiate the conflict 144
3. Types of jurisdiction 144
3.1 Personal Jurisdiction of domain names 144
3.2 In Rem jurisdiction 147
4. Practical issues over domain names *in rem* jurisdiction 148
5. Practical challenges in the choice of jurisdiction 149
6. The reality of in rem jurisdiction 152
6.1 In rem jurisdiction and territorial links 152
6.2 In rem jurisdiction challenges 154
6.3 In rem jurisdiction over the domain names: website content approach 156
6.4 Bad faith and in rem jurisdiction 156
6.5. In rem Jurisdiction and reverse jurisdiction 157
6.6 In rem jurisdiction and stakeholders' interests 157
6.7 In rem jurisdiction in the USA 158
6.7.1 Sanctions of the ACPA 159
6.7.2 Jurisdiction conflicts 159
6.7.3 Applicable law 160
6.8 In rem jurisdiction in the EU 163
6.8.1 Conflicts of Jurisdiction 163
6.8.2 Applicable law 164
6.8.3 Rome regulation mechanism related to in rem jurisdiction 165
6.9 In rem jurisdiction in Latin America 165

7. The alternative for the jurisdiction dilemma and the main challenges. 166
7.1 Challenges 166
7.2 Disadvantages of UDRP rules 167
7.3 UDRP rules as possible framework for the operation of an international Court 168
CONCLUSIONS 170
REFERENCES 179

Abbreviations

ACPA	Anticybersquatting Consumer Protection Act
ADR	Alternative Dispute Resolution
ALAC	At-Large Advisory Committee
ARPANET	Advanced Research Project Agency Network (the US Defense Advanced Research Project Agency.
ASO	the address supporting organization
ccNSO	Country Code Names Supporting Organization
ccTLD	country code Top Level domains
CIRA	Canadian Internet registry Authority
DARPA	US Defense Advanced Research Project Agency
DNS	domain names system
EEA	Agreement on the European Economic Area
EFTA	European Free Trade Association
ETSI	European Telecommunications Standards Institute
EU	European Union
EUTMR	European Union Trademark Policy
FTAs	A free trade agreement
GAC	Global Advisory Council
GNSO	The generic names supporting the organization
gTLDs	General top-level domain names
IAB	Interactive Advertising Bureau
IANA	Internet Assigned Numbers Authority
ICANN	The Internet Corporation for Assigned Names and Numbers
IDN	internationalized country code top-level domains
ccTLD	country code top level domain
IGO	intergovernmental" institutions
IPRS	Intellectual Property Rights
ITU ITU-T	The Telecommunications Standardization Sector of the International Telecommunications Union
ITU	the International Telecommunication Union
LRO	The legal rights objection
MCAD	rules on misleading and comparative advertising
PDDRP	Post-Delegation Dispute Resolution Procedure
PICDRP	Public Interest Commitments Dispute Resolution Procedure
RDNH	reverse domain hijacking
RECSAT	Research Centre for Applied Science and Technology
REFIT	the Regulatory Fitness and Performance Programmed
RPMs	Rights Protection measures
RRDRP	the Registration Restriction Dispute Resolution Procedure
SDM	single digital market
SSAC	The Security and Stability Advisory Committee
TCHM	trademark Clearinghouse
TCS	Trademark Claims Service.
TFEU	the Treaty on the Functioning of the European Union
TLD	top-level domain
TLG	Technical Liaison Group

TMPDDR	trademark Post-Delegation Dispute Resolution Procedure
TRIPS	Trade-Related Investment Measures Agreement
TTAB	trademark trial and Appeal board
UCPD	Unfair Commercial Practices Directive No 2005/29
UDRP	Uniform dispute resolution policy
UN-CIRP	United Nations Committee for Internet-Related Policies
URS	the Uniform Rapid Suspension System."
USPTO	United State Patent and Trademark Office's
W3C	World Wide Web Consortium
WIPO	World intellectual property organization
WTO	The World Trade Organization

INTRODUCTION

Intellectual property issues date back at least as far as the Venetian Patent Statute of 1474[1]. However, the concept of an international framework for IP policy, or at least, a forum to that end, has only taken shape relatively recently, with the formation of the World Intellectual Property Organisation in 1967[2]. Since then, the intellectual property field has been transformed from the traditional sense of geographical space, to the still-evolving concept of cyberspace, driven by the digital revolution.

Crucially, intellectual property rights in cyberspace are evidently more vulnerable to security threats and conflicts than in the traditional geographical environment. Hence, the relationship between intellectual property and cyberspace must be clarified with the common understanding of cyberspace as a 'container' or 'store' which contains the website network. Furthermore, this transition is from the limited or finite geographical level to the unlimited, infinite realm of cyberspace, with its attendant overlaps and continuous, rapid iterations..

Meanwhile, the internet, as a means of storing, transferring, and disseminating information, has largely superceded traditional means, which have failed to keep pace. The same might justifiably be said of policy and policing: ironically, cyberspace, which helps to spread news, exchange knowledge, and facilitate trade, is, at the same time, a haven for rogue traders, hackers, and IP theft.

Defining the relationship between intellectual property and cyberspace stems from the need to find a legislative development that goes hand in hand with technical development to ensure the ongoing necessary protection in a rapidly innovative, fluid environment. The current relationship between intellectual property and cyberspace can be incarnated in the competitive situations between trademark holders and domain name owners, which are described chiefly as unstable.

1. The hypotheses of the thesis

There are several hypotheses that this study seeks to test. The first hypothesis is based on the legal nature of the domain name in the context of the digital revolution having broken the barriers of place, time and the traditional unit of labour, moving from a limited geographical reality to a virtual reality (which has become a virtual market). In this respect, the study assumes that the legal nature of a domain name is a digital trademark and that domain names can be registered as trademarks.

The second hypothesis is presented in the relationship between search engines and trademarks. In this regard, the author will examine whether the emergence of the search engine phenomenon has led to a reduction in the conflict between trademark owners and domain name owners; furthermore, whether search engines could infringe trademark rights in cyberspace. The third hypothesis relates to the legal nature of domain name cybersquatting;

[1] *Poni, C.; Berveglieri, R. (1982). Three Centuries of Venetian Patents: 1474–1796 Resumé.*

[2] *https://www.wipo.int/portal/en/index.html*

in this respect, this study assumes that cybersquatting amounts to more than merely unfair competition or passing off, and should rather be qualified as a financial crime because of the threat posed to all communities.

The fourth hypothesis relates to whether the UDRP rules are effective in resolving reverse domain name hijacking and whether this policy was formulated to resolve conflicts based on cybersquatting and reverse domain name hijacking equally. This study assumes that the UDRP rules were not primarily designed to address reverse domain name hijacking effectively.

The fifth hypothesis is related to ICANN's additional remedies: can these remedies be effective separately? Or, do they need to be combined?

The sixth hypothesis is that the registration and use of a domain name identical to a trademark is not sufficient to establish initial interest confusion, especially for a weak trademark at the basis of the conflict, based on the Lanham Act. The seventh hypothesis is presented in the legal administrative instruments offered in the UDRP Rules. The judicial tools offered by the court do not fully resolve the *in rem* conflict because the UDRP Rules give the parties the right to go to court. The court may not always have the power to enforce the decision outside the local territory if one of the parties is a foreigner, or it may not be able to recognise the ownership of the disputed domain names. This study assumes that the court can exercise in rem jurisdiction if the domain name is considered to be property. Furthermore, the analysis in the eighth hypothesis assumes that the domain name industry does not have sufficient immunity against global crises; to support this point of view, the author has examined the impact of COVID-19 on the domain name industry.

2. Methodology

This study takes a multidisciplinary approach, incorporating history, ethics, sociology, and other approaches. The ethical phenomena of cybersquatting are analysed in Chapter 3, in relation to the using of domain names related to the COVID-19 pandemic to gain benefits. The sociological aspect, such as the dominance of social media platforms, is observed in the examples of COVID-19 domain names that spread misleading information, ignore COVID-19, or urge people not to take the vaccine (often based on a conspiracy mentality.

In addition, the financial approach is also evident, for example, in terms of the value of the domain name and the cost of the conflict between the main stakeholders. The legal approach, meanwhile, appears at various levels, from statutes and other legislation to arbitration and court decisions. For example, the Lanham Act is essential in resolving conflicts based on confusion and dilution rules. Likewise, legal agreements form another legal dimension, with examples such as the TRIPS Agreement giving international protection to domain names and the Rome Convention in terms of jurisdictional rules.

In terms of framework, the methodology will employ different (multidisciplinary) approaches to engender a precise and comprehensive understanding of the conflict, its mechanisms and dilemmas and pinpoint the reasons behind it. In the same multidisciplinary context, this study will also attempt to offer a practical solution. Accordingly, the quantitative approach in terms of statistics will be used alongside the qualitative approach in the collection of documents for this study. In this respect, the study will rely on normative legal research, as the primary data

will be legal data, including laws, legislation, regulations and case law. Furthermore, the empirical legal approach will focus on how the law resolves and enforces this conflict.
This study will largely use the case analysis approach in terms of the legal arguments used by judges to make the decision. At the same time, this study will use the comparative approach to understand how some different legal systems in some countries deal with the core of the domain name conflict in different ways. The author will use the analytical tool of the legal texts and their consistency with the protection of the rights of the holder. The comparative approach will also be applied to the international legislation related to this conflict. The inductive approach will be used to analyse the decisions of the courts and the direction taken by the courts to resolve this dispute. In addition, this study will rely mainly on secondary data.

3 Thesis structures

The thesis is divided into three parts and consists of 12 chapters. The first part of the study focuses on the issue of domain names versus trademarks. In the first chapter, the author presents a new vision of the legal nature of domain names and the importance of this new vision in protecting and stabilising the relationship between domain name owners and trademark holders. In this context, the author analyses the legal nature of domain names on the basis of recent court decisions. In this regard, the author examines the court's decision in US PTO v. Booking.com on whether the domain name is registered as a trademark. An explanation of the court's decision is essential in order to understand the legal nature of the domain name as a digital trademark. The second chapter of this part examines the relationship between search engines and trademarks, that is, whether it violates trademark law or shrinks the conflicts between the main actors in cyberspace. In the third chapter, the author sheds light on the impact of international crises on the domain name industry and its immunity. Here, the author has chosen the COVID-19 pandemic as a recent and well-documented global international crisis. The author explains the relationship between the domain name industry and COVID-19, demonstrating an association between the increase in domain name registrations and the proliferation of the COVID-19 pandemic. The author then explores illegal activities in the domain name industry related to the COVID-19 pandemic, including fraudulent websites, malware, and ransom.
In the second part of the dissertation, the author discusses the mechanism of the conflict between domain names and trademarks. This part consists of six chapters. The first chapter examines the reasons behind the conflict based on the role of registration agencies and the degree of mismanagement by these agencies. In the second chapter, the author discusses the phenomena of cybersquatting and reverse domain hijacking and how cybersquatting deals with the unstable relationship between the main stakeholders in cyberspace. Moreover, the author examines the legal character of cybersquatting and illustrates the importance of the legal character according to legal aspects such as first-come-first-served principle, legitimising cybersquatting, and the behaviour of trademark holders in response to legal trends and court decisions. This chapter also explains the emergence of reverse domain hijacking, illustrates the mechanism based on bad faith issues, and shows the extent to which

the Lanham Act deals with this phenomenon. Finally, this chapter will detail the effects of reverse domain hijacking.

In the third chapter, the author explains the domain name registration system and how it has affected the conflict based on the first-come, first-served principle. In addition, the deposit system based on the development of the first-come, first-served regulation is explained in more detail in accordance with the trademark registration rules.

As for the third part of this thesis, the author has examined the mechanism for resolving the conflict between the domain name holders and the trademark holder through the UDRP rules. In this part, the author reviews the mechanism for resolving the dispute between domain names and trademarks under the Uniform Domain Name Dispute Policy (UDRP), focusing on ICANN's core mission and ICANN's accountability and criticism in the first chapter. The author then reviews the scope of domain name dispute resolution procedures and the functioning of its mechanism, analysing the main conditions of confusion and bad faith in the second chapter. As for the third chapter of the first section, the author reviews ICANN's additional remedies, including the legal rights objection procedure and the criteria used by the panel to determine this objection, besides analysing the Trademark Clearinghouse Mechanism (TCHM), functions, remedies and liability. In Chapter 4, the author focuses on the economics of domain names, because the main motivation behind the conflict is the financial value of domain names; in order to resolve the dispute, it is necessary to encode this financial conflict in a legal framework. To this end, the cybersquatting prototype is used to evaluate the economic impact of the problem between domain names and stakeholders and to show the economic impact of resolving domain name conflicts under the UDRP rules, including the fee and financial cost of applying the ACPA.

As in the fourth part, the author envisages the resolution of conflicts between the main stakeholders through a judicial device. The author divides this section into two chapters. With reference to the Lanham Act, the first chapter is devoted to the grounds of conflict, going through confusion criteria and problems such as confusion of generic top level domain names, criticism suffix, free speech right, dilution of domain names and dilution of cybersquatting.

The second chapter of this section discusses in rem jurisdiction in terms of jurisdictional requirements and causes of in rem jurisdictional conflicts over domain names. This chapter also examines the jurisdiction of courts over persons and property in addition to in rem jurisdiction. It reviews jurisdiction, stakeholders' interests, conflicts of jurisdiction and in rem jurisdiction in the EU. The author discusses the alternative proposal for the jurisdiction of the dilemma and the main challenges, including the disadvantages of the UDRP rules as an international tribunal.

..

4. Main concepts

4.1. Domain Name Cybersquatting

Cybersquatting is the extraction of payment from the trademark owner[3]. The essence of the cybersquatting problem is complacency over the emergence of domain name registration phenomena.[4] Naturally, the cybersquatting problem can be expected to continue and grow as long as the incentive remains to buy extra or expired domains for malicious or profitable purposes.[5] Creating a new generation of Top Level Domains (TLDs)[6] requires the understanding that the goal beyond creating new generic Top Level Domains gTLDs is to reduce the cybersquatting problem.[7] Furthermore, understanding this phenomenon means understanding the exact meaning of domain names and their nature, so that the determination of domain name cybersquatting fighting will be conducted according to a rational and solid protocol based on the legal nature of cybersquatting. Defining the concept of cybersquatting is essential in order to shed light on how this phenomenon was understood at the early stage of its emergence from a legal point of view before the enactment of the ACPCA in 1999 and before the holding of the WIPO conference in 2001 that established best practices to deal with domain name cybersquatting. This concept has thus far largely depended on the understanding of legal scholars. For example, both Lemanski and Majca have defined cybersquatting as registering a domain name by a third party in bad faith.[8] This definition is considered absolute, including in other cases where any bad faith may not qualify as cybersquatting. In their definition, cybersquatting might occur if the registration is made in bad faith without reselling the domain name. This issue reflects the scope of domain name cybersquatting in the early days of its emergence.

Another point that challenges this definition is the registration process, which means that the competent authority has approved ownership of the domain name. However, this fails to consider whether the domain name has been taken by force, and that cybersquatting involves a ransom element.[9] From a legal perspective, legislators generally assume that cybersquatting is limited to domain names registering another trademark holder for profit or offered for resale.[10] In the widely-reported Toeppen case mentioned earlier, the court recognised that the

---

[3] *Lee A. Bygrave, Jon Bing, Internet Governance: Infrastructure and Institutions, PublisherOUP Oxford, 2009,p82.*

[4] *Kenneth W. Clarkson, Roger LeRoy Miller, Business Law: Text and Cases Publisher Cengage Learning,USA,15th edition, 2021 ,p171.*

[5] *ibid ,p171.*

- Misty E. Vermaat, Susan L. Sebok, Steven M. Freund, Discovering Computers ©2018: Digital Technology, Data, and Devices, Publisher Cengage Learning, 2017, p 2-10

[6] *Jennifer T. Campbell, Steven M. Freund, Mark Frydenberg, Shelly Cashman Series Discovering Computers & Microsoft Office 365 & Office 2016: A Fundamental Combined Approach, Publisher Cengage Learning, 2016, p64.*

[7] *Kenneth W. Clarkson, Roger LeRoy Miller, Business Law: Text and Cases ibid ,p171.*

[8] *Karla Lemanski-Valente and Timothy Majka, domain Names and Trademark Issues in the European Union on http://egov.ufsc.br/portal/sites/default/files/anexos/29452-29470-1-PB.htm*

[9] *Robert Wegenek, Ged O'Neill, Jonathan Moore, E-commerce: a guide to the law of electronic business, ibid, p206.*

-Peter K. Yu, Intellectual Property and Information Wealth: Issues and Practices in the Digital Age, Volume 3, Greenwood Publishing Group, 2007, p379.

David P. Twomey, Marianne M. Jennings, Stephanie M Greene, Anderson's Business Law & The Legal Environment - Comprehensive Edition,Cengage LearningUSA, 24TH edetion, 2021,,p169.

[10] *Michael Wallace, Larry Webber, IT Governance: Policies and Procedures, 2021 Edition, Wolters Kluwer Law & BusinessUSA,,1st edition, 2021,p22-34.*

-Kenneth W. Clarkson, Roger LeRoy Miller, Business Law: Text and Cases, ibid, P171.

- Roger LeRoy Miller,,Business Law Today, The Essentials: Text and Summarized Cases Cengage Learning ,13th edition , 2021,p163.

defendant was attempting to force the plaintiff to pay a ransom to secure the return of the domain name to its original 'commercial use.'[11] From a broader point of view, this definition only requires bad faith without the need for the domain to have been resold to a trademark holder. An advantage of this definition is that cybersquatting is not only associated with selling domain names and making a profit. At the same time, it is also conceivable that the aim of a particular cybersquatting scenario could be to harm others (the competitors) by preventing them from using that domain.

Reverse domain name hijacking is a conflict between domain name owners and trademark holders over trademark rights first and domain name rights second. In cyberspace, the conflicts between trademark holders and domain name owners have been seen to overlap. Finally, there is the cybersquatting conflict in which domain name owners have violated the rights of the trademark holders.

4.2. Reverse Domain Name Hijacking

The purpose of registering the trademarks of famous companies is to profit from reselling them.[12] The financial motivation behind domain name hijacking[13] means that millions of dollars' worth of domain names are at risk from this new source of profit, and there has been a sharp increase in reverse domain name hijacking.[14] Domain name hijacking is the illegal seizure of domain names by changing the domain name registration without the permission of the original registrant. Initially, this was done by blocking access to the DNS web server and placing their web server at its location.[15]

Reverse Domain Name Hijacking is defined in paragraph 1 of the UDRP Rules as "using the [UDRP] Policy in bad faith to attempt to deprive a registered domain name holder of a domain name." Reverse domain name hijacking (also known as reverse cybersquatting) happens when a trademark owner tries to secure a domain name by making false cybersquatting claims against a domain name's rightful owner through legal action or UDRP.[16]In contrast to domain name hijacking, cybersquatting involves registering domain names that are related to another person's trademark or personal name in order to market them for a high profit,[17] and is defined as "the practice of registering and using a well-known name or trademark as a domain to keep it away from its owner or to extort a substantial profit

---

[11] *The John Marshall Journal of Computer & Information Law, John Marshall Law School, 2001 Volume20, ibid, p562.*

[12] *Orin Hargraves, New Words, Oxford University Press, 2004, P 70*
- Jerry Pournelle, Erin McKean, 1001 Computer Words You Need to Know, Oxford University Press, 2004, p36.
- Angus Stevenson, Maurice Waite, Concise Oxford English Dictionary: Luxury Edition Publisher OUP Oxford, 2011, p356.
- Susie Dent, The Language Report Publisher Oxford University Press, 2003, Page 31.
- Richard Lindsay, Ad Law: The Essential Guide to Advertising Law and Regulation, Kogan Page Publishers, 2016, P46,
- Berkeley Technology Law, Journal University of California Press, 2005,2005 Volume 20, Issue 1 - Page 185.

[13] *James Van Roekel, MaryAnn Bell, Bobby Ezell, Cybersins and Digital Good Deeds: A Book About Technology and Ethics, CRC Press, 2006, p51.*

[14] *What's in a Name: Reverse domain Name Hijacking and Cybersquatting, https://hutchersonlaw.com/reverse-domain-name-hijacking-cybersquatting*

[15] *Nam H Nguyen, 2018 Essential Cyber Security Handbook in English, Publisher am H Nguyen, 2018*

[16] *Definition of Reverse Domain Name Hijacking. In: Domain Name Dictionary, https://www.domainsherpa.com/domain-name-dictionary/reverse-domain-name-hijacking*

[17] *Jacqueline D. Lipton, Internet domain Names, Trademarks and Free Speech, ibid, p12.*

from the owner".[18] Cybersquatting differs from regular trademark infringement because the primary goal of cybersquatting is to force the trademark owner to pay to get their trademark back.[19] This also distinguishes cybersquatting from cyberpiracy, which relates to copyright infringement on the website. In contrast, cybersquatting is related to domain name registration infringements.[20]

4.3. In Rem Jurisdiction

The legal term "*in rem* jurisdiction" indicates that a court can exercise its power over property or a "status" against a person not within *in personam* jurisdiction, which is called "*in rem* jurisdiction". This concept came into practice for situations when the property was located but the owner was not. Courts accepted this method as simple "*ex parte* property". However, this type of jurisdiction is controversial because it is more often used in circumstances where the party in possession is known - making them the legal presumed owner. Nevertheless, the prosecutor and the judge proceed as if he were not the owner. Instead of personal obligations, which are not always linked to the property, the primary target of an *in rem* action is the property itself.[21].

5. The legal and regulatory environment examined in the dissertation

The assumptions of this thesis depend on the legal and regulatory environment. The emergence of domain names in digital space has created new challenges that most states have attempted to address through traditional trademark laws. These customary laws cannot efficiently serve the rights of domain name owners and stakeholders. Therefore, it is crucial to identify the legal systems studied in this dissertation.

The legal environment of the assumptions of this thesis is mainly related to legal challenges, in addition to conflict resolution mechanisms. The regulations can be divided into governmental legislation, such as the Lanham Act; non-governmental regulations related to ICANN, such as the UDRP rules; and international legislation, such as treaties and conventions (TRIPS Agreement and the Rome Convention). The Internet Corporation for Assigned Names and Numbers (ICANN) is an American multi-stakeholder group and non-profit organisation responsible for coordinating the maintenance and procedures of several databases related to the names and numbering spaces of the Internet, ensuring the stable and secure operation of the network. It was founded in 1998.

Consequently, the thesis will examine American law (Lanham Act and ACPA) because it is considered to be a large market for domain names worldwide. Moreover, this law is a very advanced instrument compared to other state laws. These laws were formulated to deal with legal challenges related to domain names.

---

[18] *Munindar P. Singh, The Practical Handbook of Internet Computing Publisher CRC Press, 2004, p 1302*

[19] *Lee A. Bygrave, Jon Bing, Internet Governance: Infrastructure and Institutions, Publisher OUP Oxford, 2009, p82.*

[20] *Ibid, p 96*

[21] *https://en.wikipedia.org/wiki/In_rem_jurisdiction*

In this context, the US legislator developed its legal instruments to deal with these new legal challenges, which led to the creation of the Act of 1999, which can be considered a watershed. This act encountered new legal challenges, including the dilution and confusion of domain names, as well as the phenomena of cybersquatting. In terms of international legislation, the author examines the TRIPS Agreement to confirm the assumption that international intellectual property protection can protect the domain name. With regard to jurisdiction, the author tries to examine the extent to which jurisdiction and *in rem* jurisdiction over domain names can be exercised under the Rome Convention. In this context, the author has focused on two geographical areas for *in rem* jurisdiction: the US and the EU. The USA represents the largest market for domain names. Although the USA is a country with federal laws and regulations, the diversity of state laws has led to significant conflicts regarding *in rem* jurisdiction. Meanwhile, the EU comprises the world's largest geo-economic and political bloc, governed by a single political unit. Despite its composition of 27 independent states, the EU is able to manage *in rem* jurisdiction relatively smoothly, in comparison to the USA.

5.1 The relationship between the Lanham Act and the ACPA

The Anticybersquatting Consumer Protection Act (ACPA) is a legislation enacted in 1999 to prevent cybersquatters from registering Internet domains containing trademarks for the purpose of offering them back to the trademark owner.[22] The ACPA is an extension of the Lanham Law through an amendment (15 USC § 1125(d) (the critical federal trademark law in the US). It allows for civil proceedings to address bad faith registration of domain names that are confusingly similar or identical to (or dilutive of) famous or unique marks.[23] The Lanham Act is the umbrella under which other legal instruments are grouped (ACPA). The Cybersquatting Act deals with the registration of domain names and the trademark rights of others in order to resell them at a high profit. In addition, the Lanham Act has developed dilution and confusion tools to deal with domain name infringement based on dilution and confusion.

5.2 ICANN as a non-governmental organization

As part of the conflict-resolving mechanisms, the legal environment of this thesis was examined under the World Intellectual Property Organization (WIPO) legal umbrella through administrative legislation, which ICANN approved to solve the conflict between the main stakeholders in cyberspace. WIPO is a global organization established to develop and

[22] *Tamara Kurtzman, CYBER CENTER: The Continued Hijacking and Ransoming of the Domain Name System by Modern-Day Corporate Privateers,AMERican bar assocation, June 20, 2016, https://www.americanbar.org/groups /business _law/ publications/blt/2016/06/cyber_center_kurtzman/#:~:text=Specifically%2C%20the%20ACPA%20is%20an,of)%20distinctive%20or%20famous%20marks.*

[23] *ibid*

implement intellectual property policies on an international scale.[24] It provides free access to legal information on intellectual property (IP), including IP laws and regulations, and is one of the 15 specialized agencies of the United Nations. The Headquarters of WIPO is Geneva (Switzerland) and it was founded in 1967. The ICANN supports managing the authority role of the Internet's assigned numbers.[25] Besides providing specialized operations of vital Domain Name System (DNS) sources, ICANN specifies procedures for exactly how the "numbers and names" of the internet need to run, and provides areas for Internet policy concerns[26]. DNS is the system of global navigation within the Internet.[27]

5.3 UDRP rules

Uniform dispute resolution policy (UDRP)[28] is a process established by ICANN to resolve disputes regarding the registration of Internet domain names. UDRP currently applies to all generic top-level domains (.com, .net, .org), some country codes' top-level domains, and all new generic top-level domains (.xyz, .online, .top). UDRP rules represent the uniform domain name resolving policy and were the primary instrument used to solve the conflict between trademark holders and domain name owners, alternatively in the early stage of domain name emergencies. ICANN has practically taken on UDRP rules in all gTLD dispute processes arising from violent enrolments of domain names (cybersquatting). The UDRP rules are limited policies between the client and the registrar. They are also included in the enrolment contracts for all ICANN-accredited registrars[29].

5.4 The relationship between WIPO and ICANN

WIPO, operating through the WIPO centre, played a significant role in providing expertise to ICANN. WIPO experts assisted in preparing the board responsible for establishing the policies and procedures of the Uniform Dispute Resolution Policy (UDRP). Their expertise was instrumental in shaping and finalizing the UDRP policy. It has established WIPO supplemental rules for UDRP, which supplement the UDRP policy.[30] In this context, the UDRP rules establish a legal structure for resolving conflicts between a domain registrant and a third party over abusive enrolment and using an Internet domain in the GTLDs. General top-level domain names (GTLDs) are a category of top-level domains maintained by the Internet Assigned Numbers Authority for use in the Domain Name System of the Internet. The top-level domain is the last level of every fully qualified domain name. On October 24, 1999, the ICANN board embraced the UDRP rules, laying out procedures and other

---

[24] *aaron upcroft*trade marks as domain names: an australian perspective, 3 mac lr,p54.*

[25] *Welcome to ICANN!, https://www.icann.org/resources/pages/welcome-2012-02-25-en*

[26] *ibid*

[27] *Murray, Andrew D. "Internet Domain Names: The Trade Mark Challenge." International Journal of Law and Information Technology, vol. 6, no. 3, 1998, pp. 285-312.*

28 Murray, Andrew D. "Internet Domain Names: The Trade Mark Challenge." International Journal of Law and Information Technology, vol. 6, no. 3, 1998, pp. 285-312.

[29] *ICANN,Domain Name Dispute Resolution Policies, https://www.icann.org/resources/pages/dndr-2012-02-25-en*

[30] *https://www.wipo.int/amc/en/domains/guide/#a*

conditions for each conflict resolution administrative procedure. ICANN provides this rule, while the WIPO centre is simply a service provider.

5.5 WIPO regulatory instruments

This thesis examines the efficiency of resolving disputes between the main stakeholders through the ICANN legal and regulatory regime, to address issues concerning the dispute and how the procedures could be situated and enhanced. Under the pressure of the new legal challenges, the WIPO presented in ICANN attempted to develop legal administrative instruments and regulations to encounter such new challenges; hence, ICANN adopted many regulatory and legal acts, and instruments such as Legal Rights Objection (LRO) which empowers a trademark holder to challenge an appeal for a gTLD chain. LRO is an objection made because the applied-for gTLD string infringes the existing legal rights of the objector.

Furthermore, ICANN adopted other legal instruments such as the Trademark Clearinghouse (TMCH) and Uniform Rapid Suspension System (URS). URS is a rights protection mechanism that complements the existing UDRP by offering a lower-cost, faster path to relief for rights holders experiencing the most clear-cut cases of infringement. TMCH is a centralized database of verified trademarks that are connected to every new TLD, it started to operate on June 28, 2013. TLD is the domain at the highest level in the hierarchical Domain Name System of the Internet after the root domain. The top-level domain names are installed in the root zone of the namespace.[31] ICANN established the "Post-Delegation Dispute Resolution Procedure"(PDDRP) as a preventive mechanism that enables trademark holders to enrol marks pre-emptively. The PDDRP is a rights protection mechanism (RPM) designed to provide trademark holders (whether or not their marks are registered) with a means of disputing the actions of a gTLD registry operator.

Another legal instrument is the Public Interest Commitments Dispute Resolution Procedure (PICDRP). The PICDRP is a device that addresses complaints that a registry operator may not comply with the Public Interest Commitment(s) in Specification 11 of their registry agreement (RA). Public Interest Commitments (PICs) are binding obligations that generic top-level domain (gTLD) registry operators have made to the Internet community, with their agreement to comply included in their contracts with ICANN org. They are subject to compliance oversight and enforcement by ICANN org, which stands for PICDRP and the Registration Restriction Dispute Resolution Procedure (RRDRP) as of February 1, 2020.

5.6 Laws relating to jurisdiction conflict resolution

There are two main areas of jurisdiction: the USA and the EU. Among other areas of conflict in the EU, is the lack of choice in terms of applicable law concerning cyberspace. On the constructive side, the EU has put in place mechanisms to deal with new forms of conflict, such as Council Regulation (EC) No 44/2001 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (hereinafter Brussels I Regulation)

[31] *https://www.google.jo/search?q=top-level+domain&hl=en&sxsrf=AJOqlzXYcWgHG3BMQByv1EycHzecJ_1XZQ:1676740175624&source=lnms&sa=X&ved=2ahUKEwiap7H0x5_9AhXPgP0HHSFEBo0Q_AUoAHoECAEQAg&biw=1227&bih=657&dpr=1*

and the Regulation (EC) No. 593/2008 of the European Parliament and the Council on the law applicable to contractual obligations (hereinafter Rome I Regulation). The jurisdiction rules in the Brussel I Regulation govern jurisdiction in civil and commercial matters, mainly where the defendant is domiciled in an EU Member State. In addition, Rome I Regulation applies to contractual obligations and determines which national law applies to contractual obligations in civil and commercial matters involving more than one EU country. Rome I Regulation also promotes party autonomy and freedom of choice. Article 3(1) of this Regulation provides that "a contract shall be governed by the law chosen by the parties".

This is not the case in the United States. The Anticybersquatting Consumer Protection Act (ACPA) provides for *in rem* jurisdiction, which is based on the location of the registry or the owner of the domain name. In terms of EU jurisdictional rules, the EU has developed effective legal instruments to deal with domain name conflicts in EU cyberspace, including the Rome I Regulation and Regulation (EC) No. 864/2007 of the European Parliament and the Council (hereinafter Rome II Regulation). The Rome II Regulation deals with non-contractual obligations and develops the principle that the law applicable to non-contractual obligations is undoubtedly the law of the country where the damage occurs. According to this explanation, the analysis of Rome I and Rome II can be applied to cyberspace conflicts beyond the traditional geographical borders governed by national laws and policies. As far as jurisdiction in the EU is concerned, it is quite interesting because it consists of several countries and at the same time represents a geographical and political block.

FIRST PART: THE LEGAL NATURE OF DOMAIN NAMES AND RECENT REGULATORY CHALLANGES

In this part, the author will illustrate the main challenges related to domain name in the cyberspace. First, the author examines the legal nature of the domain name. In this regard, the author will examine the hypothesis related to domain name characters and how these characters would affect the stability of the domain name industry. Then, the relationship between domain names and search engines will be analysed. Finally, the author chooses the COVID-19 pandemic as an example of a potential threat to the domain name industry, while bearing in mind that such a threat would backfire on both the domain name industry and trademark holders.

Chapter 1: Domain names as a digital trademark: the legal nature of domain names

Since the emergence of cyberspace, new phenomena have shaped, among other things, the relationships between the stakeholders of digital communities. The relationship between the two main stakeholders of the digital society (domain name owners and trademark owners) has often been described as an unstable relationship with conflicts over potential interests, profits, and the commercial dignity of trademarks. In the early days of the digital revolution, the so-called 'cobweb' was seen as a double-edged sword in commercial, legal and technical terms. The colossal technical and legal contrasts created a deep divide between the parties, shaping the conflict over disputed rights. This conflict manifested itself in the form of unique legal challenges, providing a constant headache for legislators and legal entities. One of these challenges was embodied in domain names. The main obstacle to dealing with this issue, apart from the absence of relevant legal rules, was the ambiguity of the legal nature of domain names, at least in the early stages of the emergence of cybersquatting as a legal issue.

1. The legal nature of domain names

1.1 Service contract

A trend has emerged that rejects the premise that domain names can be classified as part of intellectual property. To this point, there is agreement that intellectual property rights cannot be physically owned, but can be regulated and exploited. It is rather a different subtlety that the court can correlate in integrity.[32] The author argues that looking at domain names from a functional point of view leads to a misunderstanding of the nature of the domain name from a legal point of view. Some links between the functions of domain names as access to a particular site are based on the detailed technological features of the domain name system, for example, a separate address for each area of the Internet. The domain name is a purposeful way of enabling an individual to access a particular

[32] *Eva-Maria Kieninger, Security Rights in Intellectual Property, Publisher Springer Nature,swizerland, 2020, p189.*

website and, on the basis of these prior facts, one might reasonably conclude that a domain name, once assigned, is not a trademark, and that a domain, necessarily, may only identify an isolated area.[33]

As regards the ownership question, we will examine the example of the registration procedure in Canada. The Canadian internet registry authority (CIRA) is the domain name authority responsible for administering the .ca domain name registry. CIRA establishes the rules for registering .ca domain names, certifies .ca registrars, maintains the WHOIS service for .ca domain names, and establishes the policy for resolving disputes regarding .ca domain names[34]. For the purpose of registration, the applicant must complete a registrar agreement[35]. The CIRA Registrant Agreement contains a non-proprietary clause. The Registrant acknowledges and agrees that domain names are not property; the registration of a domain name does not create any exclusive property rights as to the Registrar, the Registrar of Record, or any other person in any name used as a domain or in any domain name registration. Access to the domain names in the WHOIS database registry shall not be construed as evidence of ownership of any domain name registration. The Registrant shall not in any way transfer any exclusive privilege in any domain name registration or give as protection or in any other way encumber or pledge any domain name registration. This condition has been considered by a UDRP panel since 2013. However, the conflict has not been resolved on the basis of security interests.

The author has elsewhere recommended that such an agreement is likely to prevent an exclusive claim between the parties to such an agreement and is likely to protect against a proprietary interest between the parties. However, a condition in the overhead terms would expressly prohibit the grant of a charge or security by a registrant.[36.]

On the one hand, some argue that the domain must be considered as an agreement for a service contract[37], which stems from the legal arrangement between the registrar and the registrant. On the other hand, another strong school of thought disagrees, arguing that domain names are the property rights of the domain name's owner[38].

The relevant judicial case-law seems to confirm the former view. In its denial of the property's claims for the domain name, the Virginia Supreme Court decided that a domain name is a contractual service between domain registrars and the proprietors of the domain names[39]. It is interesting to analyse the court's view of the nature of domain names and whether registrants have property rights over their domain names. In *Dorer v Arel*'s case[40], the plaintiffs DORER filed a suit against Mr. Arel under infringement on trademark over the contested domain name *writeword.com.* The complainant likewise desired to possess his allotment of the earnings that could come from using the disputed domain name. However,

---

[33] *Carlos Correa, Trade Related Aspects of Intellectual Property Rights: A Commentary on the TRIPS Agreement, Publisher Oxford University Press,2nd edition, 2020,p36.*

[34] *Borden Ladner Gervais LLP, Trade-Mark Practice in Canada, 9780973075052, p126.*

[35] *Eva-Maria Kieninger, Security Rights in Intellectual Property , ibid, ,P170.*

[36] *ibid 171*

[37] *Konstantinos Komaitis, The Current State of domain Name Regulation: domain Names as Second-Class Citizens in a Mark-Dominated World, Publisher Routledge, 2010, p51.*

[38] *Graham J. H. Smith, Internet Law and Regulation, Publisher Sweet & Maxwell, 2007, p171.*

[39] *Jeffrey H. Matsuura, Managing Intellectual Assets in the Digital Age, Artech House, 2003, p64*

[40] *Dorer v Arel, 60 F. Supp. 2d. 558 (E.D. Va.1999).*

the court refused that demand as there was no relationship between the domain name and the commercial property. In this particular instance, the domain name was a service contract from NSI[41]. The Court decided that the domain name should certainly not be evaluated by money in the market[42]. The court reinforced this point of view in the case *Umbro International v 3263581 Canada*[43]. In this case, *Umbro* considered NSI an official garnishee and asked NSI to maintain these domain names until the most significant customers used them. NSI complained, supposing the legal frame of this relationship was more than just an agreement or contract to provide services, believing it contained a property right. The court decided to ignore any potential right of property in the contested domain names[44].

Furthermore, the court confirmed the registrar agreement as a contract offered to the registrant by the registrar to provide a service. The previous decision by the court raised one more question regarding the actual owner[45], that is, whether the registrant agency might be qualified as genuine proprietors of the domain name or not. In answer to this question, the court examined this concern in a case concerning a person who had registered the domain name with NSI. The Court argued that the registration company had a contract with the government to offer the domain name registration, stipulating that NSI was primarily responsible for doing the best for the domain names, and fairly.[46] It is clear that this agency is the regulatory agency, and not the owner;[47] moreover, it is the sole authorised custody of the domain name registry[48].

The argument that the domain name is limited to service contracts would have threatened the interests of stakeholders and investors in the cyberspace community and would have potentially led to the collapse of this vital area. If the contract allows such use, the trademark as a domain name should cease when the service contract is terminated. Thereafter, the reseller must cease any claim to that domain name upon termination of the contract.[49] In addition to this assumption that the registrant is the real owner, the door is opened to many legal issues if the owner has the right to share the benefits of domain names with trademark holders (as the real owners). Let us assume that someone has suffered damage from the use of the domain name. In this case, the registrant (as the real owner) should be responsible for civil compensation. Moreover, the contractual service does not mean to deny the ownership of the domain name; this applies to the telephone number, the car licence and even the trademark itself towards the other party. From different points of view, the registration of a trademark by the registrant can be understood as a contractual service in order to give the necessary legitimacy, full protection against others, and authorisation of this domain name.

---

[41] *Duksh K. Koonjoobeeharry, Are domain Names Contract of Services or Property Rights? ibid*

[42] *Gerald M. Levine, Garnishing domain Names: Are They Contracts or Property? New York Law Journal, :http: // www.newyorklawjournal.com/printerfriendly/id=1202722864976, April 8, 2015,p1.*

[43] *Umbro International v 3263581 Canada, 48 Va. Cir. 139 (1999).*

[44] *Street, F. Lawrence, and Mark P. Grant.. Law of the Internet. LexisNexis.2001, 4-80.*

[45] *D.Koonjoobeeharry, Ibid.*

– L Street and M. Grant, 4-80.

[46] *Miller, Roger, and Gaylord Jentz. Cengage Advantage Books: Business Law Today: The Essentials. New York: Cengage Learning.2007, 278.*

[47] *Ibid p278*

[48] *The Computer Law Association Bulletin, Publisher the Association, 1998 Volume 13 - Page 85*

[49] *David Lindsay, International domain Name Law: ICANN and the UDRP, Publisher Bloomsbury Publishing, 2007, p 316.*

However, if it is not saleable, there is no possibility to claim cybersquatting, mainly based on the (non-) ability to resell this domain name. The majority of domain name registrars seem to recognise that domain names are not service contracts but intangible property.[50] They have mentioned that third parties have used their publicly offered WHOIS information to register domain names.[51] The NSI may certainly allow the registration of domain names for business purposes that may infringe the trademark rights of third parties. [52] The domain name could be similar to the bank account or licence medium.[53] The rejection of the principle of ownership of domain names in favour of other ideas, such as the contract for services, will reduce the protection necessary to guarantee the stability of the cyberspace community.

1.2 Stock ticker

There is a strong similarity between domain names and stock ticker symbols. Because ticker symbols are limited to a few characters, a company may sometimes find that someone else has already taken its ticker symbol. As with domain names, stock ticker symbols are primarily allocated on a first-come, first-served basis. In perhaps the only published case involving stock symbols, MDT v. New York Stock Exchange, plaintiff MDT Corp. wanted the MDT bar code, only to find that Medtronic, Inc. was already using it. The District Court of California ruled against the plaintiff. Notably, the ticker symbol had been in use for approximately twelve years, a factor the court found appropriate given MDT Corp's late filing. Thus, the Holiday Inns and MDT cases suggest that while attempts to compare domain names to other property rights may yield insights, the legal and Internet communities should be prepared for such an eventuality.[54]

1.3 Security interest

Security interest theory appeared in a famous Canadian judgment; *Lojas Renner SA v Tucows.com Co.* The Ontario Court of Appeal found the domain name in question to be proprietary in order to establish individual jurisdiction in Ontario. The Supreme Court of Canada overturned the Court of Appeal's decision, stating that the characterisation would be used in contexts beyond the jurisdiction of the district. On the other hand, Andrew Cochran provides an examination of the assumption of the domain name as a security interest. The author contends that the situation is more complex: recognising a property interest for a particular purpose is one thing; however, the assumption that the property character of domain names should be involved in all contexts, based on the global nature of domain names, needs to be further explored.[55]

---

[50] *The Hastings Law Journal - Volume 56, Issues 1-3 , Hastings College of Law, 2005, Page 41*

[51] *Miroslaw Kutylowski, Jaideep Vaidya, Computer Security - ESORICS 2014: 19th European Symposium on Research in Computer Security, Wroclaw, Poland, September 7-11, 2014. Proceedings, Part 1, Publisher Springer, 2014, p19.*

[52] *The Computer Lawyer - Volume 13, Publisher Law & Business Incorporated, 1996 Page lv*

[53] *M. Mueller, "Why ICANN can't [failings of Internet Corporation for Assigned Names and Numbers]," in IEEE Spectrum, vol. 39, no. 7, pp. 15-16, July 2002.*

[54] *carl oppedahl, remedies in domain name lawsuits: how is a domain name like a cow?, 15 j. marshall j. computer & info. l. 437 (1997),p443*

[55] *Miroslaw Kutylowski, Jaideep Vaidya, Computer Security - ESORICS 2014: 19th European Symposium on Research in Computer Security, ibid, p19.*

1.4 Address

Some legal commentators have argued that domain names are no more than street addresses, suggesting that courts should ignore domain name claims because people do not litigate over street addresses. This argument fails because people cannot choose their street addresses in the same way; every domain name is decided upon and chosen by its owner.[56]

1.5 Property rights

As mentioned previously, an additional, substantial school of thought holds that domain names have intellectual property rights under the domain name's owner[57].
In the case of *Kremen v Cohen*[58] , which was mentioned earlier, the District Court for the Norther District of California gave its opinion based on property rights in favour of the trademark's holder by holding that the domain name must establish ownership or right to possession of the property[59]**.** This case differs from the classic cybersquatting cases in that the direct owner of the domain name found that his domain name had been forcibly taken over by a third party in a fraudulent manner while his domain name was in use.[60] The Court considered that the defendant's behaviour was an illegal disposition of the property right and triggered statutory damages[61], and decided that the domain name shaped inviolable ownership under the Public Property Act of California and was subject to transfer[62]. The court considered the domain holder was qualified to possess the property of the domain name (sex.com)[63].
In another case, Jews for Jesus sued for infringement of the registered domain name. They won the case over the domain name www.jews-for-jesus.org. The court recognised legal ownership of the disputed domain.[64] Under the Lanham Act, the domain name was considered to be similar to trademarks.[65] In the United States, in such circumstances, the trademark owner may file an *in rem* action against the disputed domain name in the jurisdiction of the domain name registry, registrar, or various other domain name authorities.[66]

---

[56] *carl oppedahl, remedies in domain name lawsuits: how is a domain name like a cow?, 15 j. marshall j. computer & info. l. 437 (1997),p443*
[57] *Smith, Graham J. H. Internet Law and Regulation. Sweet & Maxwell.2007, 171.*
[58] *Miroslaw Kutylowski, Jaideep Vaidya, Computer Security - ESORICS 2014: 19th European Symposium on Research in Computer Security, ibid, Ibid, p90.*
[59] *Casenotes, Property: Casenote Legal Briefs, Publisher Aspen Publishers Online, 5th edition, 2004, p40*
[60] *Ibid, p40.*
[61] *, Ibid, p40.*
[62] *- David John Harvey, Collisions in the Digital Paradigm: Law and Rule Making in the Internet Age, Publisher Bloomsbury Publishing, 2017, p142.*
- Casenotes, Property: Casenote Legal Briefs, ibid, p40.
[63] *Irene Calboli, Jacques de Werra, The Law and Practice of Trademark Transactions: A Global and Local Outlook, 2016, Publisher Edward Elgar Publishing, Cheltenham, UK • Northampton, MA, USA, 1st edetion,2016, p95.*
[64] *Richard Spinello, Cybernetics: Morality and Law in cyberspace Publisher Jones & Bartlett Publishers,4th edition, 2010, P 129.*
[65] *(Lanham Trade- Mark Act 43(d)(2)(A), 15 USC*
[66] *Carlos Correa, Trade Related Aspects of Intellectual Property Rights: A Commentary on the TRIPS Agreement, ibid,,p36.*

1.6 Domain name as a digital trademark

Most legal texts and legislation are consistent with legal doctrine regarding the definitions of trademarks, whether legislation belongs to common-law doctrines or non-common-law doctrines. We found that German law[67] defined a trademark[68] as: "any signs, particularly words, including personal names, designs, letters, numerals, sound marks, three-dimensional configurations, including the shape of goods or their wrapping as well as another packaging, including colours and combinations of colours, which are capable of distinguishing the goods or services of one undertaking from those of other undertakings may be protected as trademarks."[69.] On the other hand, American legislation defined a trademark as: "any word, name, symbol or sign, or any kind of combination[70] thereof, used in business to recognize and differentiate the product of one manufacturer or vendor from those of an additional and also suggest the origin of this good."[71] The term 'trademark' includes any word, symbol, device, name, or combination thereof, used by an individual or a person with a legitimate intent to use it in business. It also requires the primary registrant to identify and differentiate their product(s), consisting of one or more unique items, distinguished from those made or marketed by others and to suggest the resource of the products, even if that resource is unknown.

In addition, the term 'service mark' implies any word, symbol, name, device, or any combination thereof, used by a person, or the particular person with a good faith intent to use in business, and additionally associated with register on the primary record developed by this stage, to identify and differentiate the services of a particular person, consisting of specific service, from other services and likewise to demonstrate the source of this operator services, even if that source is unknown.[72] Titles, personality names, and other differentiating features of tv or radio shows might be considered as a service mark, considering that they may sell the sponsor's items and goods.[73]

The question as to whether domain names can be considered trademarks has ignited a vigorous debate. Contrary to the mainstream, trademark holders have lobbied for adoption of the doctrine that domain names shall somehow assume a trademark's full property rights[74]. As long as numerous domain names contain trademarks, it is rational to assume that domain names can be shielded under trademark laws[75]. The domain should be used to 'differentiate and determine' the items or services to be qualified as a trademark. Since the Web domain name must be utilised in a hallmark manner, merely using the domain name as a URL address for a Web page or e-mail address determining the cyberspace area of the services

---

[67] *Act on the Protection of Trademarks and Other Signs (Trademark Act, as amended up to Act of July 17, 2017).*

[68] *The original text: Als Marke können alle Zeichen, insbesondere Wörter einschließlich Personennamen, Abbildungen, Buchstaben, Zahlen, Hörzeichen, dreidimensionale Gestaltungen einschließlich der Form einer Ware oder ihrer Verpackung sowie sonstige Aufmachungen einschließlich Farben und Farbzusammenstellungen geschützt werden, die geeignet sind, Waren oder Dienstleistungen eines Unternehmens von denjenigen anderer Unternehmen zu unterscheiden.*

[69] *Article 3. -(1) Act on the Protection of TradEMarks and Other Signs (Trade Mark Act, as amended up to Act of July 16, 1998)*

[70] *Timothy Lee Wherry, The Librarian's Guide to intellectual property in the Digital Age Copyrights, Patents, and Trademarks, American Library Association Chicago and London 2002, P117.*

[71] *See 15 U.S.C. § 1127.*

[72] *U.S. Code › Title 15 › Chapter 22 › Subchapter III › § 112*

[73] *ibid.*

[74] *John G. Sprankling, International Property Law, Ibid, p90*

[75] *"The Legal Nature of domain Names." Lawteacher. LawTeacher.net, November 2013. Web. 24 June 2019. <https:// www lawteacher. net/free- law-essays/copyright-law/the-legal-nature-of-domain-names.php?vref=1>.*

might not suffice. The domain name should be utilized to 'distinguish and determine' the service, the source, or the sponsorship of the service. Additional promotion, such as promoting the domain name or conspicuously using it, for instance, using the trademark somewhere on the internet page apart from the address, might suffice to reveal the usage of a domain as a trademark.[76]

It is reasonable to revise the legal character of domain names. Among other legal points of view, one vision has emerged: domain names might present a digital trademark because they can distinguish websites, whether services or products in cyberspace, as equivalent to traditional trademarks in the geographical world. Despite the differences between the respective 'worlds' they inhabit, the similarities between the posited digital and non-digital trademarks are notable; besides their ability to protect the reputation of goods or services, they can also distinguish between different businesses and clarify the genuine goods or services.

Trademarks are, therefore, highly valued by all parties, and domain names and trademarks are targeted by bad-faith parties in both physical and virtual markets[77]. The primary advantage of this digital trademark, is that only one domain name can be registered as one of its kind within the same level of gTLD worldwide. To this point, Roberto Moro Visconti (in his book "Startup Valuation: From Strategic Business Planning to Digital Networking) considers that the digital brand name provides an informatic expansion of the trademarks operating internet systems and is linked to other intangibles as a domain name. The trademark, in terms of law, suggests any sign at risk of graphical appropriation, especially words (consisting of the name of an individual), drawings, letters, numbers, symbols, the form of a combination, product packaging, or colour if it appropriates to differentiate the services or products of a firm from those of others.[78.] Understanding the essence of domain names could facilitate the recognition of the legal nature of these domain names, while in turn, an understanding of this legal nature could help determine the best legal way to protect domain names and all rights related to them, whether by trademark holders or domain name owners. As mentioned, as long as domain names contain - more often than not - a real trademark within its serial, then reloading the registered trademark and replacing it with a website sequel turns that traditional geographical trademark into its equivalent digital form in cyberspace (domain name), in other words, this process defines 'domain name' as the digital equivalent of the geographical trademark. Some opinions roundly reject that domain names can be considered trademark[79]. Duksh K. Koonjoobeeharryas argues that a domain

---

[76] G. Peter Albert, Jr., Right on the Mark: Defining the Nexus Between Trademarks and Internet Domain Names, 15 J. Marshall J. Computer & Info. L. 277 (1997),p279.

[77] Gerald M. Levine, Esq., Understanding the legal options used to fight cybersquatting Cybersquatters jeopardize your exclusive trademark rights, and there are multiple ways to fight back. January 14, 2015, Network World, the website https://www. networkworld. com/article /2868398/understanding-the-legal-options-used-to-fight-cybersquatting.html

[78] Roberto Moro-Visconti, Startup Valuation: From Strategic Business Planning to Digital Networking, Publisher Springer Nature,swiszirland, 1st edition 2021, p86

[79]Duksh K. Koonjoobeeharry, Are domain Names Contract of Services or Property Rights? Feb 02, 2017, http://www.circleid.com/ posts/20170202_are_domain_names_contract_of_services_or_property_rights/

name cannot be a trademark as nobody possesses the domain name; it is merely certified to be utilised as an address by the registrar to the registrant for a specific period of time.[80]

2. Can the domain name be registered as a trademark? US PTO v. Booking.com: A case study

As it becomes increasingly difficult to find a domain name that accurately reflects the purpose or subject matter of the website, so it becomes more inevitable that trademark issues will arise.[81] In this regard, the Supreme Court of the United States made a quantum leap in its determination of the legal nature of a domain name in the case of *US PTO v. Booking.com*.

2.1. The decision in the Booking.com case

Booking.com operates a website that allows customers to book hotel rooms and organise travel. The operating company filed applications with the US Patent and Trademark Office (the PTO or USPTO) in 2011 to register four trademarks.[82] The USPTO is an agency of the US Department of Commerce that serves as the national patent office and trademark registration authority in the United States. The USPTO rejected the proposed mark on the basis that it was too broad and generic, and that the top level of a domain name does not add anything of trademark significance and does not affect its registrability. The USPTO stated that generic and descriptive domain names would be rejected if they did not pass the Section 2 Lanham Act test. In addition, if the term used is confusingly similar to another mark, the entire mark will also be rejected.[83] The USPTO took the view that when a general term is integrated with a common domain-name suffix like .com, the resulting combination is always generic, even though such a stubborn legal guideline entirely disregards customer assumption and is inconsistent with the Lanham Law.[84] Companies typically prefer an internet domain name representing or resembling their company name, brand name, or services and items for apparent reasons. In addition, a business may register a generic domain that suggests or describes some element of their products or services[85]. The PTO followed its guidelines that the assortment of common terms (like 'reservation' for hotel and airline flight arrangements) with *.com* was too common to be eligible for trademark protection. The PTO's primary issue was that a trademark guard for a phrase like *Booking.com* would unfairly prevent competitors from using generic terms.[86]

In 2016, Booking.com went to the District Court of the Eastern District of Virginia in support of its motion; Booking.com argued that there was new evidence in a study that found

---

[80] *Ibid*

[81] *Genelle Belmas, Jason M. Shepard, Major Principles of Media Law, 2023 edetion ,Publisher Cengage Learning, 2022, p316.*

[82] *ibid, p1-3.*

[83] *g. peter albert, jr., right on the mark: defining the nexus between trademarks and internet domain names, 15 j. marshall j. computer & info. l. 277 (1997),p286*

[84] *David J. Byer, Eric W. Lee, U.s. supreme court allows booking.com to register its domain name as a trademark, ibid, p1-3.*
- Genelle Belmas, Jason M. Shepard, Major Principles of Media Lawibid, p316.
-Jesse Dukeminier, James E. Krier, Gregory S. Alexander, Michael Schill, Lior Jacob Strahilevitz, Property: Concise Edition,ibid , p120.

[85] *g. peter albert, jr., right on the mark: defining the nexus between trademarks and internet domain names, 15 j. marshall j. computer & info. l. 277 (1997),p293*

[86] *Stephen F. Reed, Entrepreneurship Law: Cases and Materials Publisher Wolters Kluwer Law & Business, 2nd edetion, ,2021, P147.*

74.8% of customers identified Booking.com as a brand name rather than a generic service.[87] According to the District Court, Booking.com had already met its burden of proof that the recommended mark had acquired an alternative description and was a protectable service for booking hotels and resorts.[88] On 4 February 2019, the US Court of Appeal for the Fourth Circuit confirmed that the mark was eligible for registration.[89] The court established that the mere acquisition of a domain name does not create trademark rights[90] unless the domain name is also capable of being registered as a trademark.[91] On 30 June 2020, the Supreme Court ruled that a domain name can be registered as a trademark, thereby clarifying the legal nature of the domain name and placing it in its proper designation. The court annulled the USPTO's 'virtually in itself' policy of assuming a term to be generic when resulting from the integrationa of a generic term like *reservation* with a top-level domain as *.com*, no matter consumer assumption. The court discovered that just one (physical) entity could simultaneously inhabit a particular domain name in cyberspace; therefore, a customer might reasonably ascertain that *booking.com* directs to some distinct entity[92].

This groundbreaking decision is likely to pave the way for further new legislation, in line with the inferred new position of domain names.

2.2 Importance of the Booking.com Decision

The author believes that the US Supreme Court's decision can be considered a paradigm shift from the previously established mainstream positionthat held that a domain name registration cannot confer any rights related to a questionable trademark[93]. In addition, the court resolution allows the official domain name owner to obtain governmental protection of trademarks. In addition, it establishes that customers generally view the mark as a means of distinguishing specific goods in trade, not as a classification of a generic category of goods. In this regard, the court noted that "*whether any given 'generic.com' term is generic . . . depends on whether consumers perceive that term as the name of a class or, instead, as a term capable of distinguishing among members of the class."*[94]

In addition, the Supreme Court's ruling will preserve the ability of generic.com domain owners to rely on the ACPA and the Uniform Domain Name Dispute Resolution Policy (UDRP) to protect their domain name assets.[95.] The effectiveness and strong sanctions brought to bear by the ACPA bestow on all domain names registered trademarks. Effective

---

[87] *Daniel V. Davidson, Lynn M. Forsythe, Business in the Contemporary Legal Environmentibid,,p254.*

[88] *David J. Byer, Eric W. Lee, u.s. supreme court allows booking.com to register its domain name as a trademark, , 7 July 2020, https://www.klgates.com/us-supreme-court-allows-bookingcom-to-register-its-domain-name-as-a-trademark-07-07-2020, p1-3.*

[89] *Cory Hauser, Supreme Court Ruling Protects Registered domain Names, Preserving an Import Tool in the Fight Against Cybercrime, June 30, 2020, https://www.wiley.law/alert-Supreme_Court_Ruling _Protects _Registered_domain _Names _Preserving _an_Import_Tool_in_the_Fight_Against_Cybercrime#:~:text=On%20June%2030%2C%202020%20the, for%20combatting%20Internet%2Dbased%20fraud.&text=Such%2 0protection%20is%20critical%20to% 20preventing%20domain%20name%20abuse.*

[90] *theodore l. banks frederick z. banks, Corporate Legal Compliance Handbook, , Publisher Wolters Kluwernewyork, 3rd Edition, 2022,P9-18.*

[91] *Rupert M. Barkoff, Andrew C. Selden, Fundamentals of Franchising, Publisher American Bar Association, 2008, p 29.*

[92] *Dana Shilling, Lawyer's Desk Book, Publisher Wolters Kluwer New York., , 2nd Edition, 2022,p 10-53.*

[93] *theodore l. Banks frederick z. Banks, Corporate Legal Compliance Handbook, , ibid,P9-18.*

[94] *Cory Hauser, Supreme Court Ruling Protects Registered domain Names, Preserving an Import Tool in the Fight Against Cybercrime, ibid.*

[95] *Ibid.*

complainants in matches brought under the verdict can gather real damages and revenues or choose to receive statutory damages varying from $1,000 to $100,000.[96] The unique decision of the Supreme Court, in a sense, supports the assumption that domain names can be adopted as a digital trademark by acknowledging that a suffix domain name added to even a generic term grants this entity's trademark protection and trademark registration-applications. It is the opinion of this author that this judgement paved the way to giving these entities the position they deserve among intellectual property rights, finally defining the domain name as a digital trademark, in accordance with the court's decision.

2.3 Generic terms understanding

Using the criteria to examine the term Booking.com, which represents the bulk of the term for travel booking services, the court explained: "if 'Booking.com' were generic, then it might expect that the customers recognise a traveling service to be a 'Booking.com.'" Nonetheless, because the evidence showed that customers "do not sense the term 'Booking.com' in this way," the mark qualified for federal trademark registration. In a key part of the decision, the court recognised that trademark registration gives domain name owners a stronger defence under the umbrella of the Anticybersquatting Consumer Protection Act, 15 USC § 1125(d) (ACPA). Such a protection is essential to avoid domain name abuse.[97] It is important to emphasise that a generic mark cannot be protected as a trademark.[98] Trademark law allows for descriptive phrases and terms only under certain circumstances. For example, suppose the phrase has acquired sufficient 'secondary or additional meaning' through use in the marketplace that the public is likely to recognise it as a resource indicator rather than as a term used to define services or products.[99]

The court noted that such a mark has narrow protection. This doctrine is a defence against the anticompetitive consequences of the PTO's practice, and confirms that registration of Booking.com would certainly not give its owner a monopoly on the term 'reservation'. The Booking.com case shows that Booking.com would certainly be a 'weak' mark. A generic and common mark makes it possible to use the same label for the classification of the underlying services and goods.[100] The Supreme Court indicated that Booking.com was not a generic term for hotel reservation services, so that a small addition to the generic term could make the mark descriptive and thus potentially protectable.[101] The Court's decision that Booking.com did not meet the criteria of being a generic term for a travel reservation service was based on the ultimate consideration that consumer recognition of a term as a name is what determines the legitimacy of the mark, even though Booking.com contains a pair of generic elements and

---

[96] *Roger LeRoy Miller, Business Law Today, Comprehensive: comprehensive edition text and cases, Publisher Cengage Learning, 13rd edition,2021, city p200*

[97] *Cory Hauser, Supreme Court Ruling Protects Registered domain Names, Preserving an Import Tool in the Fight Against Cybercrime, ibid.*

[98] *Hovenkamp, Janis, Lemley, Leslie, Carrier, IP and Antitrust: An Analysis of Antitrust Principles Applied to Intellectual Property Law, Publisher Wolters Kluwer, 3rd Edition,2022, p2-84.*
- david j. byer, eric w. lee, u.s. supreme court allows booking.com to register its domain name as a trademark,ibid,, p1-30

[99] *ibid, p1-3.*

[100] *Stephen M. McJohn, Examples & Explanations for Intellectual Property, Publisher Wolters Kluwer Law & Business, new york, 7th edetion,2021, p444*

[101] *Ibid,.p 444.*

also the fact that the same textual string can also function as a URL. The Court also made clear that the mark containing a generic phrase must not itself be generic,[102.] but the entire mark must be evaluated.

This case differs from others where phrases like *Booking.com* rank as inclusive, and numerous assisting principles are common ground. First, a generic term names a category of services or items rather than any certain function or exemplification of the category. Second, for a combination term, the diversity questions train on its significance as an entire phrase, not on its components alone. Third, the pertinent definition of a term is its perception by the customers. Qualification for registration activates the mark's capacity to distinguish [h] goods in commerce. Confirming the Lanham Act's concentration on customers' perception, the area controlling registration cancellation provides that the authorised mark's main relevance to the appropriate public will be the examination for identifying whether the accepted mark has ended up being the inclusive name of products or services. Under these concepts, *Booking.com* generally turns on whether that phrase or term symbolises the category of online hotel reservation services to customers. Hence, if *Booking.com* were common and generic, we might anticipate customers to recognise travel between cities as an additional service to *Booking.com.* We might similarly expect that a customer looking for a reliable resource for online hotel reservation services might ask an experienced traveller to recommend their preferred Booking.com service provider. As the courts established, consumers do not regard the term Booking.com this way.

3. The European and American courts' case-law regarding the legal nature of domain names' cybersquatting

In light of this new vision of the domain name, the main difference is that trademarks take their places within a geographical place and within narrow borders. In contrast, domain names as digital trademarks will take place in cyberspace, taking advantage of being one of a kind because the system of DNS does not allow more than one entity to be registered. Furthermore, domain names as digital trademarks can benefit from the trademark field experience in legislation, registration, or examination.

The dishonest behaviour of cybersquatters undermines the integrity of domain names.[103] When it comes to dealing with cybersquatters, court actions alternate between dilution, trademark infringement and unfair competition.[104] In cases of cybersquatting, it is often observed that the domain name registrant is not using the website.[105] In this regard, the main task of the courts to solve this issue has been presented in unfair competition such as extortion, commercial ransom and passing off, as follows.

---

[102] *Stephen M. McJohn, Examples & Explanations for Intellectual Property, ibid, p444*

[103] *ICANN internet governance: is it working? ibid p26*

[104] *Gregory J. Battersby, Charles W. Grimes, Trademark & Copyright Disputes: Litigation Forms and Analysis, Publisher Wolters Kluwer,USA, 4th edition,2021,, p 2-6.*

[105] *Khuran, Reema, Rashmi Aggarwal, Interdisciplinary Perspectives on Business Convergence, Computing, and Legality, Publisher IGI Global,USA,1st edetion 2013, p203.*

3.1 Unfair competition

Since most registration authorities in the EU do not provide an alternative dispute resolution procedure, the claimant must seek the protection of a court to protect his right to the disputed domain name from cybersquatters. As in the United States, European courts have to apply a variety of laws governing domain names, including trademark and competition laws.[106] As in the United States, courts throughout Europe have generally held that the use of domain names that are substantially identical or similar to trademarks constitutes trademark infringement if the defendant has used them in bad faith or in connection with the purchase of competing goods or services. As an example, we can mention Italian case law, where cybersquatting has been considered unfair competition and an infringement on a trademark if there is a violation of trademark value and reputation[107]. Accordingly, Genova's court of first instance established the existence of unfair competition in the famous cybersquatting case of *Compaq vs. A.B.X* concerning the Altavista search engine's market position. In this case, there was an implicit appropriation of the Altavista name's worldwide importance by the means of the altavista.it domain, whose home page returned information related to the real search engine to make users believe they were browsing the real thing. As the victim of a bad faith registration, Altavista suffered an unjustified and immediate damage not fully mendable, consisting in the prevention of Altavista from registering its own domain name to the Italian Registration Authority.[108]

However, there are exemptions to this general rule. For instance, in the case of *British Telecom plc. v. One in A Million Ltd*, the British Court of Appeal considered that the registration of popular trademarks did not amount to trademark violation, even when the domain names were non-active and the registrant did not offer the domain for sale[109].
The Danish courts represented an approach which was different from both the general (European) judicial approach and the British courts' case-law. These courts did not consider whether registration or reselling a domain's name was an infringement on a trademark as long as the domain name was not involved in any commercial practice.[110] For example, in the case *belogic vs. Deniss Willard zewillis*[111], as a defendant, Deniss zewillis registered over 200 domain names related to the famous Danish trademark[112]. The Danish capital (Copenhagen)

---

[106] Karla Lemanski-Valente and Timothy Majka ,domain Names and Trademark Issues in the European Union,ibid.
- Claudia Costa Pederson, Gaming Utopia: Ludic Worlds in Art, Design, and Media, Publisher Indiana University Press,usa1st edetion, 2021,p155-156.
- Matthew David Brozik, domain Names Here And Abroad :Superhighway Widens, But Hazards Remain: More Internet Addresses Will Not Address Trademark and Unfair Competition Concerns, New York State Bar Association, NYSBA Bright Ideas | Spring/Summer 2001 | Vol. 10 | No. 1,p13.
[107] Nicoletta Galizia, Trade mark litigation in Italy: overview at: https://uk.practicallaw.thomsonreuters.com/w-010-0167?transitionType=Default&contextData = (sc.Default)&firstPage=true&bhcp=1 01-Nov-2018
[108]The article:" Italian court solves a cybersquatting case over Altavista search engine" on the web site http://www.searchenginelaw.net/domain-names/100-italian-court-solves-a-cybersquatting-case-over-altavista-search-engine
- Stephen Fishman, Trademark: Legal Care for Your Business & Product Name, Publisher Nolo,USA, 11th edition,2016,P58.
[109] Ian Walden, Julia Hörnle, E-commerce Law and Practice in Europe, Publisher Woodhead Publishing Limned ,England1st edition, 2001, P5.
- Karla Lemanski-Valente and Timothy Majka, domain Names and Trademark Issues in the European Union,ibid.
[110] ibid
[111] Raymond Chan Internet Framing , Complement or Hijack? The "What If" Scenario to the Case, The Trade-mark Reporter, Publisher United States Trademark Association, 1999 Volume 89, p520
[112],i bid p520

court ruled that the act constituted unfair marketing[113] under Danish marketing law.[114] As confirmed, the defendant did not violate Danish trademark law[115].

In the USA, although several cybersquatting conflicts have been resolved by courts, the high cost and prolonged duration of the court procedures have pushed main stakeholders to protect their trademarks by using different approaches based on UDRP rules, unfair completion, or trademarks infringing against cybersquatters.[116] Without knowing the main stander that can specify the legal nature of domain names' cybersquatting, courts have regularly maintained that such cybersquatting comprises trademark dilution, which might violate the trademark per se[117]. In many cases, courts have also approved the trend of adopting the legal character of cybersquatting based on dilution grounds.[118] The trademark holders have been most effective in bringing cases against cybersquatters under the Federal Dilution Act and have succeeded in winning these cases.

Some argue that considering the legal nature of cybersquatting on the basis of dilution has shown the limited effectiveness of remedies against cybersquatting.[119] In this view, American courts generally rely on other approaches, such as passing off and unfair competition,[120] to solve the cybersquatting problem. Preferring such approaches is more reasonable because the claim of cybersquatting can be proven if the contained trademark is popular or different from the need for protection.[121]

One of the earliest cases of cybersquatting was *Panavision vs. Toeppen.* Toeppen registered the trademark of the legal holder as the domain name *panavision.com*. As a result, Panavision submitted legal action of cybersquatting against Toeppen under three different legal approaches: unfair competition, infringement on trademark, and trademark dilution[122].

In an earlier case with the same defendant, i.e. in the case *Intermatic Inc. v. Toeppen*, the US District Court rejected Toeppen's assertion that the absence of use safeguarded him from dilution insurance claims because of the non-commercial use exemption of the Dilution Act. In this context, the Court explained that holding his domain marketing business to be a business work within the competence of the law prevented him from future usage of the domain. The Court considered the intent to profit from the domain name as business usage,

---

[113] *Karla Lemanski-Valente and Timothy Majka ,domain Names and Trademark Issues in the European Union, ibid.*

[114] *Raymond Chan Internet Framing , Complement or Hijack? The "What If" Scenario to the Case, The Trade-mark Reporter, Ibid p520*

[115] *Ibid p 520.*

- Diane Cabell, Foreign domain. Disputes,The Computer & Internet Lawyer, Publisher Aspen Law & Business, 2000, Volume 17, P 7.

[116] *Peri Pakroo, The Small Business Start-Up Kit: A Step-by-Step Legal Guide , Publisher Nolo,USA,10th edition, 2018 P 41*

[117] *Sreenivasulu N.S, Law Relating to Intellectual Property, Publisher Partridge Publishing, India,1st edition,2013, p138.*

[118] *Margreth Barrett, Intellectual Property, Publisher Aspen Publishers Online, 2008, p274.*

- christopher j. Schulte,the new anticybersquatting law and uniform dispute resolution policy for domain names,tort & insurance law journal - the university of california, American Bar Association Vol. 36, No. 1, fall 2000 , p 105.

-Mark E. Plotkin, F. Lawrence Street, Solving the legal issues affecting B2B transactions, Publisher Practicing Law Institute, 2001, p433.

-Chris Reed, Internet Law: Text and Materials, Publisher Butterworths,Oxford,UK, 2000, p54.

- Hossein Bidgoli, The Internet Encyclopedia, Volume 2, ibid, Page 339.

[119] *Computer Law Reporter, Volume 29 Publisher Computer Law Reporter Incorporated, 1999, P 505.*

- Robert P. Merges, Peter Seth Menell, Mark A. Lemley, Intellectual property in the new technological age, Publisher Aspen Publishers/Wolters Kluwer Law & Business,4th edition, 2007, Volume 1, Page 759

[120] *Chris Reed, Internet Law: Text and Materials, ibid. p54.*

[121] *Cybersquatting, on the website: https://www.klemchuk.com/cybersquatting*

[122] *Patrick J. Flinn, Handbook of Intellectual Property Claims and Remedies, Publisher Aspen Publishers Online, 1999, p 8-39*

-Julian S. Millstein, Jeffrey D. Neuburger, Jeffrey P. Weingart, Doing Business on the Internet: Forms and Analysis, law journal press, new york, 7thedetion ,2003,p18.

- Julia Hörnle, Internet Jurisdiction Law and Practice, ,ibid, P305.

which must comprise dilution[123]. That principle was emphasised again in *Panavision, Int'l, L.P. v. Toeppen*[124]. The Court discovered that the respondent's enrolment of a domain name, which corresponded to the complainant's trademark, offered the domain's selling to the trademark holder, thus comprising a dilution. On this basis, the court rejected his claims that non-use would exempt him from the Dilution Act[125].

According to the Toeppen case, considered classic cybersquatting criteria, the Court established its decision under dilution rules[126]. Furthermore, the Court stipulated that domain name registration in commercial practice should be accepted as cybersquatting cases under dilution rules.[127]

Unfair competition is presented by any competitor's unjust and dishonest commercial practice[128]. Additionally, it was observed that cybersquatting was considered a trademark violation outside the U.S.A. based on unfair competition[129]. In very early situations, the American Court discovered that registering a famous trademark as a domain name for commercial use constitutes unfair competition, whereby the domain's registrant takes advantage of the trademark's fame[130]. In line with this issue, the trademark does not need to be creative, but simply distinctive[131].

Before Congress enacted the ACPA, most of the earliest Anticybersquatting instances were accepted based on dilution rules[132]. The ACPA has drawn attention to the need to provide courts with an effective alternative to simply expanding federal dilution law to deal with cybersquatting under the Lanham Act.[133] The key issue in these claims was determining whether the mark in the case being asserted as cybersquatting under the dilution rules was 'wellknown.'[134] In this regard, Apple has taken multiple legal actions against cybersquatters for enrolling items as domain names, such as *iphone4s.com* and *ipods.com*[135].

---

[123] *, Mark j. Thronson ,gabrielle s. Roth, jon d. Grossman, Intellectual Property Legal Opinions , ,ibid, p5-59.*

[124] *945 F. Supp. 1296, 40 U.S.P.Q.2d (BNA) 1908 (C.D. Cal. 1996)*

[125] *, Mark j. Thronson ,gabrielle s. Roth, jon d. Grossman, Intellectual Property Legal Opinions ibid, p5-59.*

[126] *Julia Hörnle, Internet Jurisdiction Law and Practice,ibid, P411.*

[127] *Peter K. Yu, Intellectual Property and Information Wealth: Issues and Practices in the Digital Age, Volume 3, Publisher Greenwood Publishing Group, 2007, p380*

[128] *World Intellectual Property Organization. International Bureau, Protection Against Unfair Competition: Analysis of the Present World Situation, Publisher WIPO, Issue 725 of WIPO publication, 1994, p23*

[129] *Claudia Costa Pederson, Gaming Utopia: Ludic Worlds in Art, Design, and Media, ibid,,p155-156.*

- Computer Law Reporter, Volume 29, Publisher Computer Law Reporter Incorporated, 1999, P 505.

- Daller, Daller, Business Torts: A Fifty-State Guide, 2021 Edition, Publisher Wolters Kluwer Law & Business,NEWYORK1St edetion, 2021,P473..

[130] *Michael D. Scott ,Scott on Multimedia Law ,ibid 2021,ibid p 5-111.*

- Irwin Gilbert, Harley S. Tropin, LexisNexis Practice Guide: Florida Business Torts, Publisher LexisNexis USA,,ist edetion, 2021,ibid,p 9-67

[131] *Niklas Bruun, Graeme B. Dinwoodie, Marianne Levin, Ansgar Ohly, Transition and Coherence in Intellectual Property Law: Essays in Honour of Annette Kur, Publisher Cambridge University Press,UK,1st edetion, 2021,p308.*

[132] *Bruce P. Keller, D. Peter Harvey, Strategies for litigating copyright, trademark and unfair competition cases, Publisher Practicing Law Institute, 2001, p239*

[133] *Ohio Lawyer, Publisher Ohio State Bar Association, 2000 Volume 14, P 434.*

- Irwin Gilbert, Harley S. Tropin, LexisNexis Practice Guide: Florida Business Torts, ibid,,p 9-68.

- Graeme B. Dinwoodie, Mark D. Janis, Research Handbook on Trademark Law Reform, Publisher Edward Elgar Publishing UK & USA, ist edetion, 2021,P356.

[134] *Practising Law Institute,Understanding Basic Trademark Law, Publisher, Practicing Law Institute, 2000 p798*

-David P. Twomey, Marianne M. Jennings, Stephanie M Greene, Anderson's Business Law & The Legal Environment - Comprehensive Edition, ,ibid, p169.

[135] *Roger LeRoy Miller, Cengage Advantage Books: Fundamentals of Business Law Today: Summarized Cases, ibid,, p109.*

In feedback to a legal conflict between Etoy.org, and eToys.com, a lawsuit was submitted in California following Etoy.org's rejection of a monetary deal for the Etoy.org domain. The toy firm implicated the other party in 'unfair competition and trademark dilution[136]. In this context, changes to China's Anti-Unfair Competition Act have robustly supported trademark holders by giving them a more powerful device to challenge cybersquatting[137].

According to cybersquatting domain names' disputation, the Chinese People's Court considered using or preserving domain names by the complainant as unfair competition[138]. It is noticeable that the Chinese People's Court's judges favour the trademark holder. Accordingly, in the case *of IKEA v Cinet* submitted to Beijing Second Intermediate Courts of People, the Court required CINET to modify its own website's enrolment.

Moreover, to quit using the domain name and terminate the registration it created in Nov 1997, the complainant submitted a lawsuit based on trademark violation and unfair competition[139].

Similarly, the Japanese courts have ruled on cybersquatting cases according to unfair Competition[140], while, the French courts have sued cybersquatters[141]. One of the ordinary pictures of the unfair competition used on large scopes occurs when the cybersquatter's website displays pornography or offers gambling, and acquires marketing profits from advertising based upon the website's number of visits, called 'hits'[142]. The unfair competition is based on directing traffic to a specific website[143] .

In the case *of Audi AG and Volkswagen of America Inc. v. Bob D'Amato,*[144] the Court decided that using the trademark and Audi's company slogan illegally in the domain name constituted an infringement on the trademark[145]. However, trademark infringement is considered an aspect of unfair competition, a tort, and certainly not criminal[146].

3.2 Blackmail and commercial ransom

One of the exciting visions related to the legal character of domain name cybersquatting relates to cybersquatting entails being adopted according to the demands of commercial

---

[136] *Claudia Costa Pederson, Gaming Utopia: Ludic Worlds in Art, Design, and Media, ibid,,p155-156.*

[137] *Niklas Per Fridman, A Remedy Against Cybersquatting, the article was previously published in Asia IP magazine: http://www.asiaiplaw.com/article/39/3167/.*

- Dan Prud'homme, Taolue Zhang, China's Intellectual Property Regime for Innovation: Risks to Business and National Development, Publisher Springer,swiszrland ,1st edetion, 2019,p31.

[138] *the John Marshall Journal of Computer & Information Law, Volume 20, 2001, p576.*

- Dan Prud'homme, Taolue Zhang, China's Intellectual Property Regime for Innovation: Risks to Business and National Development, ibid,,p31.

[139] *The Computer & Internet Lawyer, Aspen Publishers, 2000 Volume 17, Issue 9, Page 23.*

Zhou Lin, China Court Cases on Intellectual Property Rights, Publisher Kluwer Law International B.V ,ntherland,1st edetion, 2011,p 329.

[140] *Vanderbilt Journal of Transnational Law, Volume 34, Issue 1, Publisher Vanderbilt University, School of Law, 2001, p893.*

[141] *Dennis Campbell, Susan Woodley, E-Commerce: Law and Jurisdiction: Comparative Law Yearbook of International Business - Special, Issue 2002, Volume 24, Part 1 of Comparative Law Yearbook, Publisher Kluwer Law International B.V., 2003, p79.*

[142] *Deborah E. Bouchoux, Intellectual Property: The Law of Trademarks, Copyrights, Patents, and Trade Secrets, 5th Edition, Publisher Cengage Learning, 2016, p150.*

[143] *Cybersquatting and consumer protection: ensuring domain name integrity: hearing before the Committee on the Judiciary, United States Senate, One Hundred Sixth Congress, first session, on S. 1255, a bill to protect consumers and promote electronic commerce by amending certain trademark infringement, dilution, and counterfeiting laws, and for other purposes, July 22, 1999, Volume 4, Publisher U.S. G.P.O., 2000,p60.*

[144] *Audi AG and Volkswagen of America Inc. v. Bob D'Amato 469 F.3d 534, No. 05-2359 (6th Cir., November 27, 2006).*

[145] *Karla Lemanski-Valente and Timothy Majka, domain Names and Trademark Issues in the European Union, ibid.*

[146] *Boston University Journal of Science & Technology Law, Publisher Boston University, School of Law, 2000, Volume 6, p36,*

blackmail and ransom[147]. Courts have realised this[148], and accordingly, if the reason behind the domain name is cybersquatting, then it will be considered another matter called 'domain name grabbing,' defined as when a trademark is intentionally registered as a domain name to prevent the trademark's legal holder from using the domain name[149]. In one of the first cybersquatting cases (Avon Products), the Court recognised that the avon.com domain name had been registered by a third party who tried to hold up the title for extorting ransom[150]. The Court never characterised cybersquatting as blackmail or ransom. presents For the ideal cybersquatting case, the trademark holder must show evidence that the cybersquatter has demanded ransom[151] .

3.3 Passing off

Passing off is a cause of action that can apply very widely where there is a deliberate misrepresentation that a person's products or services are those of somebody else[152]. In reasonable application, the passing off offered a trademark owner the ability to control the use of the mark within its marketplace; however, the common law view influenced the law of passing off. In practice, the action for passing off is a rather troublesome procedure and can be prolonged, pricey, and unpredictable,[153].

The enrolment of a false domain name is not passing off *per se*[154]. In this regard, Unfair Competition is considered a passing off or an attempt to pass off [155]. However, passing off is considered a tort under the U.K. courts [156].

According to British courts, the legal nature of cybersquatting has been considered a tort of passing off in the context of the infringement on trademark rights[157] related to *Harrods Limited vs. United Kingdom Network Services*, which was the first case submitted to a British court based on passing off[158]. In another case, *British Telecommunication vs. One in a million*

---

[147] *Boston University Journal of Science & Technology Law, Volume 6, Boston University, School of Law, 2000, p36*

[148] *Berkeley Technology Law Journal, Publisher University of California Press, 2002 Volume 17, Pages 1-952 - Page 161.*

- United States. Congress. House. Committee on the Judiciary, Trademark Cyberpiracy Prevention Act: report (to accompany H.R. 3028), Volume 106, Issue 412 of Report, United States Congress, Publisher U.S. G.P.O., 1999 p5.

[149] *g. peter albert, jr., right on the mark: defining the nexus between trademarks and internet domain names, 15 j. marshall j. computer & info. l. 277 (1997),p312*

[150] *Susan P. Crawford, Representing the e-commerce company: a satellite program, Practicing Law Institute 2000, p64.*

- David H. Bernstein, Protecting your intellectual property assets, Practicing Law Institute 2000, p268

- Berkeley Technology Law Journal, Volume 16, Publisher University of California Press, 2001, P 218

[151] *Mark T. Carroll, ALI-ABA's Practice Checklist Manual on Advising Business Clients III: Checklists, Forms, and Advice from The Practical Lawyer, Publisher ALI-ABA, 2004, P359.*

- ICANN internet governance: is it working? hearing before the Subcommittee on Commerce, Trade, and Consumer Protection and Subcommittee on Telecommunications and the Internet of the Committee on Energy and Commerce, House of Representatives, One Hundred Ninth Congress, second session, September 21, 2006, Publisher U.S. G.P.O., 2006 Volume 4, p 28.

- Anthony Corrado, The New Campaign Finance Sourcebook, Publisher Brookings Institution Press, 2005, P 255.

[152] *Kundharu Saddhono, Deny Tri Ardianto, M. Furqon Hidayatullah, Vita Ratri Cahyani, seword fressh 2019: Proceedings of the 1st Seminar and Workshop on Research Design, for Education, Social Science, Arts, and Humanities, seword fressh 2019, April 27 2019, Surakarta, Central Java, Indonesia, Publisher European Alliance for Innovation, p468.*

[153] *dawson, n. m. "trade mark law and the creation and preservation of well-known brands." northern ireland legal quarterly, vol. 49, no. 4, winter 1998, pp. 343-362.p351*

[154] *Robert Wegenek, Ged O'Neill, Jonathan Moore, E-commerce: a guide to the law of electronic business, Publisher Butterworth, s3rd edition, 2002, p220.*

[155] *Daller, Daller, Business Torts: A Fifty-State Guide, 2021 Edition, Publisher Wolters Kluwer Law & Business,New York,1St edetion, 2021,ibid,p 344.*

[156] *Andrew Murray, Information Technology Law: The Law and Society, Publisher Oxford University Press,UK, 4TH edition 2019 P 373,*

[157] *Jenny Ng, The domain Name Registration System: Liberalization, Consumer Protection, and Growth, Publisher Routledge, 2013, p75.*

[158] *Ibid, p75.*

limited, the court decided that the main elements of passing off tort included goodwill, damage, misrepresentation, and cybersquatting cases based on passing off rules[159]. The Indian courts have also adopted cybersquatting cases based on passing off regulations. [160]

Chapter 2: Search Engines and Domain Names

Domain names and trademarks have similar characteristics in that both can act as distinctive signs to identify a business in the marketplace. One of the main advantages of the Internet is that it can put the sole trader and the small business person on the same footing as large multinational corporations[161]. However, the rights are registered separately through different organisations. Conflicts can therefore arise when a company registers a domain name that is identical to an existing trademark. One of the areas where conflicts can arise is in the area of searches and trademarks. On this point, it is necessary to examine the main argument that the phenomenon lost its importance in the mid-2000s, mainly due to the major search engines, which significantly reduced the importance of the domain name. It is no coincidence that the last articles on the subject were published sometime in the mid-2000s. There is also the question of whether search engines are infringing trademark rights and domain names.

1. Background

Searching within web pages was introduced with the 1994 WebCrawler. The giant search engine Yahoo was founded in 1993, while Lycos was the first search engine to introduce proximity search. Netscape Navigator appeared as the default search engine in 1993-94[162], followed by Inktomi in 1996 and AltaVista around the same time. Importantly, the emergence of search engines did not and has not diminished the importance of domain names to trademark owners, who have been able to increase their brand presence in cyberspace.
At the same time, it is true that most internet users find their web destinations through search engines. Usually, it is not necessary to remember all the domain names, but only the most important keywords. The search engine performs searches through the hole of registered domain names in its database, requiring registered domain names to complete this process. Meanwhile, the interaction between trademark owners and domain name owners continued, with the conflict actually increasing dramatically in the years following the emergence of search engines. Therefore, the relationship between search engines, domain names and trademarks can, at least this time, be framed within the so-called ‘keyword trademark’.

---

[159] *Ibid, p75.*

[160] *K. Jaishankar and Natti Ronel, First International Conference of the South Asian Society of Criminology and Victimology (SASCV), 15-17 January 2011, Jaipur, Rajasthan, India: SASCV 2011 Conference Proceedings, Publisher K. Jaishankar, 2011, p75.*

[161] *G. Peter Albert, Jr., Right on the Mark: Defining the Nexus Between Trademarks and Internet Domain Names, 15 J. Marshall J. Computer & Info. L. 277 (1997),p279*

[162] *Murray, Andrew D. "Internet Domain Names: The Trade Mark Challenge." International Journal of Law and Information Technology, vol. 6, no. 3, 1998, pp. 285-312.*

1.1 Search engines definition

An internet search engine is software that systematically performs specific searches for a text query. Search engine results are typically displayed in a list of results, commonly called search engine results on web pages (SERPs). When an individual types a query directly into a search engine, the engine checks its index of web pages to find those that are relevant to the individual's query. The results are then ranked according to their importance and displayed to the user. The details can be a combination of web links to websites, images, video clips, charts, short articles, study papers and other documents.[163]

1.2 Search engines submerged

In the digital age, websites have become indispensable for starting and growing a business: they provide an insight into companies, their business models and their product range, and they enable customers to specify, select and compare the best products or services. Customers use search engines such as Google to find information and access websites. [164] The search engine contains a complicated algorithm to gather relevant information for search terms. In addition, keywords entered into search engines allow sites to be ranked and found quickly. A large percentage of users only check the first search results from search engines, and companies consequently invest in trying to ensure their websites appear in the top rankings of these first searches. Search Engine Optimisation (SEO) improves a website for better search results. Various techniques such as link building can be used to achieve these changes, organising content on the website to include frequently searched terms and words, and adding specific keywords to the website's '[165]metadata'. The question arises as to whether search engines are involved in trademark and domain name disputes.

2. Area of the conflict between search engines and trademark

The commercialisation of the Internet has raised issues that have not been well [166]studied. The interaction between trademarks and domain name holders has increased dramatically. Thus, following the emergence of search engines, the relationship between search engines, domain names and trademarks, at least until the present time, can be framed within the so-called 'keyword trademark'.

For many companies, trademarks now represent the bulk of their valuable assets. Trademark owners expect trademark protection to protect their financial investment[167] in marketing. The ad will appear whenever an individual searches for related words. Although it may not be as relevant, the purchase of a keyword phrase confirms that the other owners' listings will

[163] *https://en.wikipedia.org/wiki/Search_engine*

[164] *Chadha & Chadha Intellectual Property Law Firm, Search Engine Optimization and Trademarks, India May 27 2020, https://www.lexology.com/library/detail.aspx?g=8c09f235-df7c-4187-8d02-07346f286ca4.*

[165] *Chadha & Chadha Intellectual Property Law Firm, Search Engine Optimization and Trademarks, India May 27 2020, https://www.lexology.com/library/detail.aspx?g=8c09f235-df7c-4187-8d02-07346f286ca4.*

[166] *Murray, Andrew D. "Internet Domain Names: The Trade Mark Challenge." International Journal of Law and Information Technology, vol. 6, no. 3, 1998, pp. 285-312.*

[167] *Dawson, N. M. "Trade Mark Law and the Creation and Preservation of Well-Known Brands." Northern Ireland Legal Quarterly, vol. 49, no. 4, Winter 1998, pp. 343-362.*

appear prominently in search engine results. What happens when a company buys a competitor's brand keyword? Many people find their website via an online search engine with two listings: relevant (results identified by the internet search engine) and sponsored (listings provided by marketers). Sponsored listings usually appear with relevant listings on the page and at the top of the page. A company can buy a sponsored listing by buying (or bidding for) keyword phrases. On Google.com, the client can click on the "Marketing" web link at the bottom of the web page, and also register to buy keywords (Google calls them "Adwords") for a small setup fee (about $5).

In today's competitive markets, it is an accepted fact that trademarks and popular brand names can achieve a much higher conversion rate (that is, converting a visitor to a purchasing customer) than generic keywords. The direct-response television (DRTV) marketing market estimates that nearly 21% of consumers enjoy seeing ads for a product type and brand in the search box of online search engines such as Yahoo, Google and others.[168] Search engines include the list of results determined by the search engine and lists provided by advertisers. Sponsored listings appear alongside relevant search results. The search engine may link to sponsored listings and advertise by buying or bidding on keywords. For example, Google.com allows a user to purchase keywords for as little as $5 by clicking on the ad link. Keywords are terms that people type into a search engine. Although they may not be relevant, buying a keyword ensures that listings appear prominently in search results.

The question here is whether buying a keyword that is a competitor's trademark should be considered trademark infringement. For example, some companies have purchased the keyword of their competitor "Nolo", allowing a sponsored link to a different website to appear at the top of the page when the keyword is clicked. Courts have allowed companies to purchase competitors' trademarks as keywords if the competitor's trademark does not appear in advertisements. For example, in 2011, the 9th Circuit allowed Network Automation to purchase a competitor's trademark as a keyword. When users searched for "ActiveBatch", the network's ad appeared as a sponsored ad at the top of the page. The court held that this was not trade mark infringement as it was unlikely to confuse customers. The court concluded that internet users have sufficient experience to distinguish between search results and advertisements. In the case of Network Automation, Inc. v. Advanced Systems Concepts, Inc., 638 F. A, the court also found that similarity of tags and marketing channels used were inappropriate factors to consider in keyword advertising cases because the user does not consider the similarity to be confusing[169].

3. Metatags

The interaction between search engines and trademarks is based in the use of keywords and metatags links advertisement. To this point, the question here is whether metatags and keywords violate the rights of the trademark in cyberspace or not. Redress must be given

[168] *Loren Baker, Search Engine Marketing and Trademarks,searxh engines journal, September 25, 2004 4 min readhttps://www.searchenginejournal.com/search-engine-marketing-and-trademarks/903/*

[169] *(in Issue 1-800 Contacts, Inc., No. 9372 (2017)*

where other merchants use a well-known mark to dilute the advertising value of the mark in question[170].

3.1 Metatags concept

A 'meta tag' or 'metadata' is a keyword or term embedded in a site's HTML, an abbreviation for hypertext markup language,[171] This code is used as a method for online search engines to determine and classify the website's contents. It gives internet browsers specific information about a Web site, often increasing its frequency in search engine results[172]. Many firms strategies involve registering both the keywords and metatags associated with rivals or any third party's hallmarks in order to significantly enhance web traffic.[173]. Furthermore, in some cases, such expenses are even asymmetrically allocated among the parties. In this context, the keyword advertising plan that does not authorise third-party use of trademarked keywords is not necessarily much better for the trademark holders[174] .

The for-profit website with hundreds of paid links is not in commerce when it operates third-party trademarks as referencing. Intangible Uses Publishers on the Web can refer to trademarks in a way that consumers cannot perceive. For instance, web publishers can contain trademarks in their ‘keyword meta tags,’ indexing terms that are readable by search engine bots but generally invisible to website visitors. Judicial scrutiny of these "intangible uses" has usually been unfavourable. For instance, tribunals have often treated the inclusion of third-party trademarks in keyword meta tags as a violation and, in many cases, have entirely ignored the use-in-commercial requirement. However, suppose consumers are not "aware" of the trademark inclusion in keyword meta tags. In this case, the meta tags do not indicate the source, and the use of the meta tag should be unrelated to the trademark analysis[175].-The policies of Google's trademark restrict the use of the trademark in ad copy, even though Google does allow bidding on branded keywords. There are ongoing court cases that may lead to policy changes. For example, policies at Google vary by country in terms of Campaign setup[176]. Meta tags can raise the possibility that a website will be returned in search engine results, even if the website has no relationship with the search phrases. Essentially, one website can appropriate the search phrases of other websites and thus gain more hits, ensuring that it appears similar to and of similar status to, the preferred sites.. Using an additional trademark in a meta tag without the owner's consent usually comprises trademark violation. Some uses of another party’s trademark as a meta tag might be

---

[170] Dawson, N. M. "Trade Mark Law and the Creation and Preservation of Well-Known Brands." Northern Ireland Legal Quarterly, vol. 49, no. 4, Winter 1998, pp. 343-362.

171G. Peter Albert, Jr., Right on the Mark: Defining the Nexus Between Trademarks and Internet Domain Names, 15 J. Marshall J. Computer & Info. L. 277 (1997)

[172] Roger LeRoy Miller, William E. Hollowell, Cengage Advantage Books: Business Law: Text and Exercises, Publisher Cengage Learning,,8th edetion, 2016,p 95.

173 Adam Jolly, The Handbook of European Intellectual Property Management: Developing, Managing and Protecting Your Company's Intellectual Property, Publisher Kogan Page Publishers,3rd edition, 2012,p122.

[174] Martin Husovec, Injunctions Against Intermediaries in the European Union, Publisher Cambridge University Press, 2017, 9781108415064 , p22.

[175] Graeme B. Dinwoodie, Mark D. Janis, Trademark Law and Theory: A Handbook of Contemporary Research, Publisher Edward Elgar Publishing, 2008,p421. 9781848441316

[176] Kevin Lee, Catherine Seda, Search Engine Advertising: Buying Your Way to the Top to Increase Sales, Publisher New Riders, 2nd edition,2009,p133.

permissible, provided the service is needed, and does not state that the owner authorizses or sponsors the use[177].

As an example, we can mention the case of Nespresso USA, Inc. which is a well-known espresso and coffee maker manufacturer and owner of the registered trademark "Nespresso." Nespresso offers for sale and makes coffee pills for use with its equipment. “Africa America Coffee Trading” company, operating as Libretto, manufactures coffee pills suitable for use with Nespresso devices. Libretto's capsules coincide in form and size with Nespresso's, but they are constructed from plastic (not aluminium like Nespresso's). Libretto utilised the Nespresso trademark on its boxes. It used the word "Nespresso" as a meta tag in the source code for its website. Nespresso attempted to contact Libretto and demanded that it quit offering and producing espresso capsules that infringed on its trademark, but Libretto did not respond. Nespresso filed a case in a government court in New York City. The US Southern District Court of New York concluded that Libretto had infringed on Nespresso's trademark and permanently prohibited (restricted) Libretto from using the Nespresso mark, including its meta tags.[178]

3.2 Usage of trademarks as meta tags

Meta tags are not visible to routine users of the site (although they can be made visible along with the page's source code). Nevertheless, an online search engine looking for specific keywords will find the site and index it. The more frequently a keyword appears in the hidden code, the more highly an online search engine will rank the site in its search engine results. However, a trademark used as a meta tag is not primarily used to distinguish particular goods or services because it is used in a way that is not visible to the typical viewer.

In some jurisdictions, courts have found that the use of competitors' names as meta tags constitutes unfair competition. (See for example the judgment of the Federal Court of Canada in the case Red label vacations inc. (redtag.ca) v. Travel Buys Ltd. (411travelbuys.ca), 2015 fc 18.) More specifically, in several international disputes, the question was whether the use of a trademark in a meta tag can constitute passing off or trademark infringement (see for example the case Reed Executive plc & Another v Reed Business Information Ltd & Others.)[179] The British Columbia Supreme Court, in the case British Columbia Automobile Assn v. Office and Professional Employees' International Union, found that the use of a trademark and trade name in a meta tag would not support a finding of confusion or likelihood of deception. Therefore, trademark infringement or passing off could not be established by such use alone. As Judge Grauer pointed out, the habits of search engines are not evidence of anything other than the process of an algorithm and online search engine marketing. It is certainly not evidence of confusion. Trademark infringement can occur online, most notably through meta tags. Meta tags online search engines compile their results by looking through a website's keyword coding. Meta tags, or keywords, can be inserted into

[177] *L.T.C. Harms, World Intellectual Property Organization, A Casebook on the Enforcement of Intellectual Property Rights: 4th Edition ,Volume 791 of WIPO publication, 9789280529821, p 167.*

[178] *Roger LeRoy Miller, Frank B. Cross, The Legal Environment Today, Publisher Cengage Learning, 2021, 10th edetion, p236. 9780.357635636*

[179] *L.T.C. Harms, World Intellectual Property Organization, A Casebook on the Enforcement of Intellectual Property Rights: 4th Edition ,Volume 791 of WIPO publication, 9789280529821, p 168.*

this coding to increase the frequency with which a site appears in search engine results, even if the site has nothing to do with the words inserted. A section may correctly contain the keywords of more popular websites. Using this method so that the site in question appears in the same search engine results as the other sites. The use of someone else's trademark in a meta tag without the owner's consent constitutes trademark infringement.[180]

Conflicts have even been raised when website owners have embedded, without authorisation, third-party trademarks in their website's coding. The repeat of the same phrase in meta tags to "entice the attention of online search engines" has frankly been described as "cyber-stuffing." Courts have judged that a defendant who utilises somebody else's trademark in meta tags may infringe the trademark. However, the specific circumstances of each case will always determine whether such an infringement has actually occurred. In one claim, for instance, a short-lived restraining order was approved by the District Court of the Southern District of California against a website owner who embedded recommendations to "Playboy" in the website's coding. However, the appellate court (US court of Appeals for the Ninth District) overturned the district court's ruling and found that the defendant (a former Playboy model) had not infringed on Playboy's trademark. The court held that the use of registered trademarks of Playboy Enterprises in meta tags and otherwise on the Web site of a former "Playboy Playmate of the Year" is a "permissible, nominative use" of the trademarked terms because "no descriptive substitute" exists for the term "Playboy Playmate of the Year 1981." The court found that the defendant's use of the trademarked terms on her website also satisfied the other requirements of the nominative use test, i.e., that she had used only so much of the trademarks as was "reasonably necessary to identify" herself, and she "did nothing in conjunction with her use of the marks to suggest sponsorship or endorsement" by the trademark holder. The court emphasised that its ruling was specific to the facts of the case, and may have been different if the metatags recited the trademarks "so repeatedly that Welles' site would regularly appear above [Playboy's] in searches for one of the trademarked terms."[181] [Playboy Enterprises. Inc. v. Welles. 279 F3d 796 (9th Cir. 2002)]. In other cases, this Court also confirmed that the nominative reasonable usage test was not satisfied when a competitor of the trademark holder made an "unreasonably prevalent" usage of a trademark on its website.[182]

4. Keywords

Keywords are the terms that individuals type directly into the search engine. If the client acquires the words "crochet' and "child," the advertisement will be expected to appear prominently whenever an individual searches for crocheted child hats. Even when the keywords are not as appropriate to the product or service, buying a search phrase nevertheless guarantees that listings will appear prominently in search outcomes. What happens when a company acquires a search phrase that is a rival's trademark? Numerous firms have bought the keyword "Nolo" (the hallmark for the publisher of this publication). Consequently, when a person types "Nolo" into an online search engine, the sponsored web links of these firms

[180] *L.T.C. Harms, World Intellectual Property Organization, A Casebook on the Enforcement of Intellectual Property Rights: 4th Edition ,Volume 791 of WIPO publication, 9789280529821, p 168.*
[181] *Richard Raysman, Emerging Technologies and the Law: Forms and Analysis, Volume 1, Publisher Law Journal Press, 2002,p6-54.*
[182] *Richard Raysman, Emerging Technologies and the Law: Forms and Analysis, Volume 1, Publisher Law Journal Press, 2002,p6-55.*

appear at the top of the web page. This presents questions for the trademark holders wishing to defend their trademarks: does the user (the competitor) commit trademark violation? Or is it the merchant of keywords or AdWords at fault? Or both parties?

4.1 Keywords, trademarks and consumer protection

In the case *Google Inc v. Australian competitors and customer commission,* the High Court of Australia held that Google had not engaged in misleading or deceptive conduct contrary to the relevant provisions of the Australian Consumer Law in publishing 'sponsored links' in response to web page searches. As is well-known, Google operates a search engine. When an internet user requests a search based on one or more words, the search engine will show the websites that appear to correspond to those words, in order of significance . These are described as the 'natural' outcomes of the search[183]. The Australian Competition and Consumer Commission (ACCC) argued that Google engaged in misleading and deceptive conduct because its program allowed advertisers to enter the names of competitors as keywords so that a 'sponsored link' to the advertiser's company would arise when the competitor's name was entered into the search engine. Although the 'sponsored links' by the advertisers *were* held to be misleading or deceptive, Google was held not to be responsible for the misleading or deceptive conduct because it did not author the 'sponsored links', nor did it endorse the misleading representations of the advertisers.[184]

Internet users are significantly trending towards the use of online search engines to find details online, as an alternative to depending on domains to browse the Web. Users request a search using defined terms[185]. The online search engine then utilises manual and automated approaches to locate those keywords in meta tags, URLs, or keywords. Alternatively, they are based on a history of user activity. Some of these online search engines 'sell' keywords to marketers who wish to target their marketing, such that whenever the keyword is entered into the online search engine, an ad appears in addition to any search engine result. Retailers, for instance, have purchased keywords to show their banner advertisements whenever specific trademarked items are search items. It means that a company, such as Google, that sells keywords does not utilise the trademark as a badge of origin or use it in the trademark sense. It rather offers marketing space.

In the case *Google France Sarl and Google inc. v. Louis Vuitton Malletier SA* (C-236/ 08) the Court of Justice of the European Union (CJEU) examined the service of Google's subsidiary Google France. Google offers a paid referencing service called 'AdWords'. That service enables any economic operator, by means of the reservation of one or more keywords, to obtain the placing – in the event of a correspondence between one or more of those words and that/those entered as a request in the search engine by an internet user – of an advertising link to its site, accompanied by a commercial message. That advertising link appears under

[183] *L.T.C. Harms, World Intellectual Property Organization, A Casebook on the Enforcement of Intellectual Property Rights: 4th Edition ,Volume 791 of WIPO publication, 9789280529821, p 168.*

[184] *Sarah Mulcahy and Jeannie Marie Paterson, Google Searches and Misleading Conduct: Google Inc v Australian Competition and Consumer Commission, 29 October 2013, https://blogs.unimelb.edu.au/opinionsonhigh/2013/10/29/mulcahy-paterson-google/#:~:text=In%20Google%20Inc%20v%20Australian,in%20response%20to%20web%20page*

[185] *L.T.C. Harms, World Intellectual Property Organization, A Casebook on the Enforcement of Intellectual Property Rights: 4th Edition ,Volume 791 of WIPO publication, 9789280529821, p 168.*

the heading ‘sponsored links’, which is displayed either on the right-hand side of the screen, to the right of the natural results, or on the upper part of the screen, above those results.[186]. In this case, the CJEU had to decide on the question whether it is lawful to use under the European Union’s trade mark legislation,[187] as keywords in the context of an internet referencing service, signs which correspond to trade marks, where consent has not been given by the proprietors of those trade marks.

In this case, the CJEU highlighted two main issues relating to the relationship between metatags and trademarks, that is, (1) the function of the trademark to indicate the origin of goods or services and (2) that only the likelihood constituting (at least potential) risk of consumer confusion may lead to trademark infringement. The CJEU established that the use, by a third party, of a sign which is identical with, or similar to, the proprietor’s trade mark implies, at the very least, that that third party uses the sign in its own commercial communication. A referencing service provider, however, allows its clients (i.e. the advertisers) to use signs which are identical with, or similar to, trade marks, but does not itself use those signs. If a trade mark has been used as a keyword, the proprietor of that trade mark cannot, therefore, rely, as against Google, on the exclusive right which it derives from its mark. By contrast, it can invoke that right against the advertisers which, by means of the keyword, arrange for Google to display ads which make it impossible, or possible only with difficulty, for average internet users to establish from what undertaking the goods or services covered by the ad originate. In such a situation, the function of the trade mark, which is to guarantee to consumers the origin of goods or services (the trade mark’s ‘function of indicating origin’), is thus adversely affected. In any case, the use of another person’s trademark for advertising purposes is liable to have certain repercussions on the advertising use of that mark by its proprietor and on the latter’s commercial strategy. Such repercussions do not of themselves, however, constitute an adverse effect on the ‘advertising function’ of the trade mark.

The cost of referencing services is determined by the 'maximum cost per click' that the marketer agreed to pay when signing up for the referencing service with Google, based on the number of times that internet users click on the link. Several advertisers can bid for the same keyword. The prominence given to the display of their marketing links is determined in particular according to the maximum rate per click, the number of previous clicks on these links and the advertising quality taken into account by Google. The marketer can therefore improve their position on the screen by setting a higher maximum cost per click or by trying to improve their ad quality. Google has established an automated process for selecting keywords and creating ads. Marketers choose the keywords, write the business message and enter the link to their website. A referencing service provider allows its clients to use signs which are identical or similar to trade marks without itself using those signs. That deduction is not called into question by the fact that the service provider is paid by its clients for the use of those signs. The creation of the technical conditions necessary for the existence and use of

[186] *Ibid, p 168.*

[187] *Currently Directive (EU) 2015/2436 of the European Parliament and of the Council of 16 December 2015 to approximate the laws of the Member States relating to trade marks, OJ 2015 L 336, 1. (Trade Mark Directive, TMD) and Regulation (EU) 2017/1001 of the European Parliament and of the Council of 14 June 2017 on the European Union trade mark (codification), OJ 2017 L 154, 1. (European union Trade mark Regulation, EUTMR).*

a sign for which a fee is paid does not mean that the service provider is using the sign. It follows from the foregoing that a referencing undertaking (in this case Google) is not associated with use in trade.

The rationale for using AdWords is that if a competitor uses a proprietor's trade mark as an AdWord, a user who searches for that trade mark will receive a link to the competitor's website or an advertisement from the competitor will appear on the screen. Put simply, Adword activates a competitor's ad and draws the user's attention to the competitor's site or ad. The underlying approach of the CJEU seems to be that unless the ad or sponsored link uses the plaintiff's trademark in the trademark sense and causes confusion, there can be no trademark infringement.[188].

The keyword advertising discussion deals with the triangular relationship between trademark owners, customers and advertisers, also present in online behavioural advertising linked to search results and browsing history. Brand-related purchases are used as parameters to target brand advertising to consumers. In this context, keyword advertising experiments show that the involvement of trademark owners adds critical policy considerations. Transparency of sources to consumers is necessary to move in the right direction; moreover, a focus on consumer empowerment in this regard will also increase consumer understanding of online behavioural advertising. For trademark owners, however, the overarching policy goal of trademark law and protection comes into play.[189].

According to standard trademark theory, trademarks primarily identify the commercial source of services and goods in a market. As we have seen, the CJEU in the Google France case represented the approach that the primary function of a trade mark is to guarantee the identity of the origin of the trade-marked product to the consumer or end user by allowing him to distinguish, without any risk of confusion, that product from products of another origin. As a result, a protected trademark can act as a source identifier in trade. It ensures fair competition, protects consumers from confusion and contributes to the proper functioning of market economies by allowing customers to clearly express their preferences for particular products or services.[190] From an economic point of view, it can be added that a specific indication of the commercial origin of services and goods reduces consumers' search costs. The inclusion of brand owners in the debate about the clarity of online behavioural advertising means, in addition to the defence of consumers, the requirement for marketplace clarity, i.e. that trademark regulation must contribute significantly to "reasonable play" in the battle between trademark owners and competitors for market share, including one-on-one battles in online advertising.[191] In its BergSpechte decision, which is almost identical to that concerning Google France, the CJEU confirmed the previous likelihood of confusion analysis under Article 9(2)(b) EUTMR and Article 10(2)(b) TMD,[192] as well as its approach regarding the original function of the trademark. These two approaches togetheramount to a test of whether the advertising is too vague to exclude a potential risk of consumer confusion. According to Senftleben, this calibration of legal obligations is nothing less than a shift from proof of likely confusion by the trademark owner, to an obligation on all advertisers to secure market

[188] *Ibid , p 168.*
[189] *Ryan Abbott, Research Handbook on Intellectual Property and Artificial Intelligence, Edward Elgar Publishing, 2022, p316*
[190] *Ibid , p317*
[191] *Ibid , p319*
[192] *See case C-278/08 BergSpechte v Trekking.at, paras 36 and 38-40.*

transparency when using keyword advertising services. Instead of conceiving of trademark rights as instruments that shield trademarks from confusing use by third parties at the initiative of the trademark owner, the CJEU redefined protection against confusion as a positive obligation of third parties to keep a sufficient distance from the origin information conveyed via the trademark.[193].

The CJEU also laid down, in its L'oréal v Bellure judgment that a third party attempts, through the use of a sign similar to a mark with a reputation, to ride on the coat-tails of that mark in order to benefit from its power of attraction, its reputation and its prestige, and to exploit, without paying any financial compensation and without being required to make efforts of his own in that regard, the marketing effort expended by the proprietor of that mark in order to create and maintain the image of that mark.[194]

The Digital Services Act (DSA), applicable from May 2023, is a milestone in the process of completing the Digital Single Market of the European Union. The DSA primarily aims to create a safer digital space in which the fundamental rights of users are protected, and to establish a level playing field for businesses. In line with this goal, the DSA focuses on customer transparency measures. According to its relevant rules, platforms, such as online markets, must guarantee that system individuals receive information that enables them to comprehend when and on whose behalf, as well as metatags and also keywords advertising is displayed along with what criteria are used to direct advertising to the customer, including descriptions of the logic underlying systems for targeted advertising. The case-law of the CJEU provides important signposts that might help create a well-functioning clarity procedure under the relevant DSA provisions.[195]

4.2 The concept of the average consumer related to keyword ads

The concept of the average consumer used by the CJEU in its keyword advertising rules may still be relevant. In this context, the Court defined the average consumer as a web customer who is generally knowledgeable and reasonably observant. When shopping portals generate product recommendations based on previous purchases or purchases made by similar users, the concern is whether a reasonably prudent customer can check the various sources of these product suggestions. If an individual is familiar with item recommendation systems, it could be assumed that the branded product is an imitation rather than a model. The customer is still significantly involved in the purchase decision and is therefore more likely to focus on the commercial source of the suggested choices.

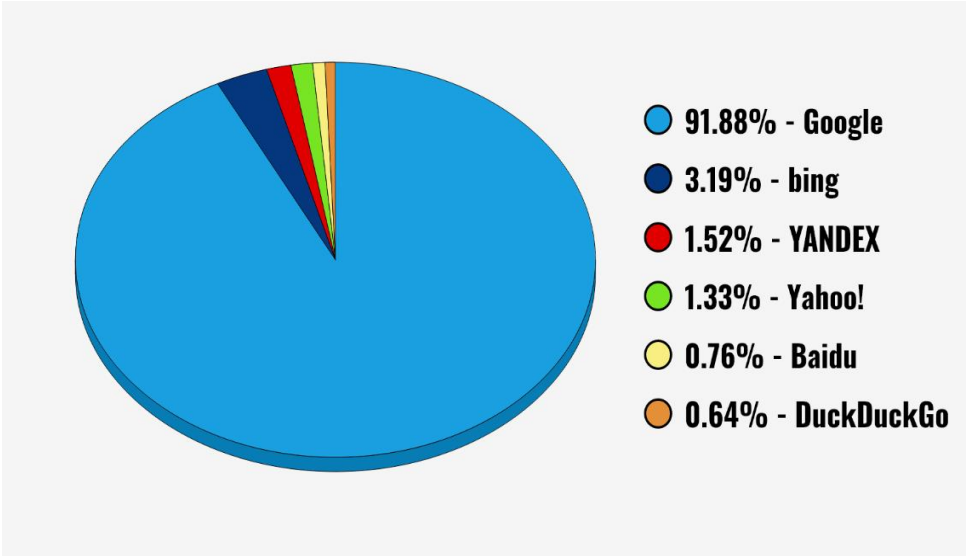
In determining which customers are interested in using certain kinds of goods or services, the CJEU distinguishes between the general public (i. e. average consumers) and a professional or customised public. The latter include a niche group of customers or a specialised sub-group of experts in the given field. The distinction between the public and a specialised public is crucial, as it shows a different type of customer from the point of view of trademark law purposes. It allows for the application of trademark law according to the scenario in a particular situation, thus protecting the underlying interests of allowing trademark protection.

[193] *Ibid , p319*
[194] *Case C-487/07, L'Oréal v Bellure, para. 49.*
[195] *ibid, p321*

The CJEU uses these different types of the relevant public (general or specialised) of the goods and services in question to determine the degree of consideration with which this public acquires. The degree of consideration with which consumers acquire a product is likely to vary according to the nature of the goods or services, the type of public that purchases them and the situations.[196]

Because of the stated discussion of customer vulnerability, the establishment of the new rules regarding responsibilities can give the impression that the European Commission has explicitly focused on consumer empowerment in preparing the new market transparency rules (see the explanatory memorandum of the DSA proposal). In the context of this transparency, the terms used in the new provisions leave room for a broad knowledge of the proposed openness commitments. In particular, it seems likely that there will be an interpretation that includes customers and brand owners. While the DSA consists of detailed descriptions of the terms 'customer' and 'trader', the relevant DSA provisions refrain from restricting the scope of the new openness obligations to the particular classification of 'customers'. More neutrally, both regulations describe the "recipient of the service", a term that Article 2(b) DSA describes as "any natural or legal person who operates the relevant intermediary service". Traders and customers use online platforms, such as online search engines that host third party advertisements and online markets that host third party offers. If the neutral term "recipients of the service" is understood to include both customers and traders, the new obligations can be analysed in a way that ensures access to openness details not only for customers but also for brand owners (= "traders" in the sense of 2(e) DSA). As described, the DSA seeks to confirm that the recipients of the service can recognise "for each particular ad shown to each recipient, undoubtedly and unambiguously and in real time" the origin of the ad (source openness) and the criteria used to target the recipient (parameter clarity).

Figure 1. Search Engine Market Share, 2022[197]



Source: https://cdn.internetadvisor.com/2022/7/1658769866267-1._Search_Engine_Market_Share%2C_2022.png

[196] *Ryan Abbott, Research Handbook on Intellectual Property and Artificial Intelligence, ibid, p304*
[197] *https://cdn.internetadvisor.com/2022/7/16587698662671._Search_Engine_Market_Share%2C_2022.png*

4. Metatags and trademark infringements in other jurisdictions

Search Engine Optimization (SEO) is a marketing instrument operated by many firms to improve traffic on their websites. In this regard, registered trademarks can be inserted into the website using concealed HTML codes in the title tags. Businesses routinely use competitors' trademarks as part of their SEO strategies, in order to achieve the highest ranking and thus visibility to customers. In this context, even a tiny change in SEO can allow a company to gain a higher ranking in search engine results. Section 29 of India's Trade Marks Act deals with the breach of registered trademarks, and Sub-section (8) of Section 29 states "that any advertising of that trademark violates a registered trademark if such advertisement unjustly take advantage of and is delinquent to moral practices in commercial matters." In the case Cosimo Info Pvt. Ltd v. Google India Pvt. Ltd.6, the High Court of Madras said Google would make contributory infringement if the questioned trademarks were bid through Google AdWords services.

Furthermore, the High Court of Bombay, in the case People Interactive Pvt. Ltd. v. Gaurav Jerry & Ors. confirmed the relationship between metatags and the violation of the marks. The court held that the defendant shaadihishaadi.com "spent upon the reputation of Plaintiff's shaadi.com to hijack the Internet traffic from Plaintiff's site, amounting to online pirating." The Court granted an *ex-parte* injunction and demanded that trademark infringement be established following section 29 of the Trade Marks Act whenever trademarks are misapplied and included in meta-tags. Correspondingly, the burden of proof must fall on the trademark owner to authenticate the possibility of confusion. The Delhi High Court issued its decision in favour of the Plaintiff Company "Policy Bazaar" against the Defendant "ACKO Company" for using its trademark "Policy Bazaar" as keyword advertisements through the Google search engine. In addition, the Court fined the plaintiffs for concealing their activity by using the defendant's trademark, "ACKO," as a keyword[198].

SEO uses third-party trademarks as keywords to improve the positioning of the advertisers' ads in relation to the natural results through keywords in their Google AdWords campaigns. SEO is related to a company's marketing on the Internet; thus, the company's website traffic increases the website's popularity among potential visitors. However, the illegal use of registered trademarks as meta tags and keywords is considered an infringement of the trademark in addition to the irreparable loss of its owner. There is a legal and economic necessity to address the steadily increasing issues around keywords associated with well-known trademarks. Therefore, strict laws must be enacted to reduce the infringement of the use of trademarks as meta tags or keywords. Indeed, courts, to date, have even regularly permitted companies to buy a competitor's trademarks as a keyword provided their trademark did not appear in the ad.

In 2011, for instance, the US Court of Appeals for the Ninth Circuit allowed Network Automation to purchase a rival's trademark, ActiveBatch, as a keyword. When users searcheded for "ActiveBatch," Network's ad appeared as a sponsored ad on the search results. Because it was not considered likely to cause customer confusion, the court maintained that this was not a trademark infringement. The Court reasoned that internet users

[198] *Adgully Bureau,PolicyBazaar reprimanded by Delhi High Court in a case against Acko, JUN 07, 2019https://www.adgully.com/policybazaar-reprimanded-by-delhi-high-court-in-a-case-against-acko-86188.html*

knew enough to distinguish between search engine results and sponsored advertisements. The Court also maintained that the similarity of the marks, advertising, and marketing channels used were not suitable variables to consider in keyword marketing instances since the user is not seeing and likening the two marks. (Network Automation, Inc. v. Advanced Equipments Concepts, Inc., *638 F. 3d 1137 (9th Cir. 2011*). The Federal Trade Commission likewise says that using a competitor trademark as a keyword is not a trademark violation.

.

5. Conclusion

Search engines can be liable in trademark infringement in several ways, including dilution. In addition to search engines increasingly displaying trademark infringing domain names on search results pages, this study argues that the nature of domain names is unique in cyberspace and cannot be duplicated. Consequently, new forms of intellectual property infringement have been created, alongside a growing number of infringement cases.[199] There is a steady stream of case law on trademark infringement in online search engine marketing worldwide. However, the question is whether online search engines can infringe trademarks through the release and selection of search results pages and advertisements. In particular, the legal issues arising from trademark infringement in search engine results and underlying sites will be examined to the extent that search engines avoid liability for third party material and communications. Much of the case law offered on the legal liability of online search engine providers relates to whether online search engines have an impact on domain names and trademark infringement.[200.]

Furthermore, the author believes that search engines have no direct relationship to the reduction or elimination of domain name and trademark infringement in cyberspace because search engines deal with a colossal database of registered domain names. The customer does not have to type in specific domain names. If there are no registered domain names, then search engines cannot work perfectly to show accurate results because the customer wants to use search engines to find very specific results. In many cases, the desired domain names to be registered contain someone else's trademark, which can lead to conflicts between the main stakeholders in cyberspace. The author argues that search engines may have introduced new forms of trademark infringement into cyberspace, such as keywords, meta tags and advertising. In other words, search engines have complicated the traditional framework of infringement in cyberspace, as recent cases suggest. In this regard, in the recent case of Bart et al. v. Slocumb May 2022,[201] a plaintiff survived a defendant's motion to dismiss where the plaintiff alleged that the defendant had purchased advertising space from a search engine under trademarked keywords to market goods that did not consist of any of the plaintiff's trademarks. The court found that the plaintiff had adequately pleaded infringement by alleging initial confusion, even though the resulting ad was not infringing. The court noted

[199] *Terence P. Ross, Intellectual Property Law: Damages and Remedies Publisher: Law Journal Press, 2000, P6-4*

[200] *Joris van Hoboken, Search Engine Freedom on the Implications of the Right to Freedom of Expression for the Legal Governance of Web Search Engines, Publisher: Wolters Kluwer 2012,*

[201] *Bart et al. v Slocumb (2-21-cv-01771, Eastern District Louisiana, 26 May 2022),*

that the infringement was not the mere purchase of the keywords, but the marketing resulting from the use of the marks.[202]

Chapter 3: Domain names immune against international crises: COVID-19 as a case study

The COVID-19 pandemic, and the resulting public curfews, undoubtedly accelerated the shift from traditional to digital services, thus fuelling an increase in cyberspace. This chapter examines the relationship between the domain name industry and COVID-19. In this context, many reports indicated an increase in the number of domain names registered during the pandemic. In terms of the legal framework, this chapter will examine where COVID-19 has been a factor in the infringement of the rights of the domain name holder. The area of possible infringement that the chapter will analyse is COVID-19 related domain names spreading misinformation: fraud and malicious purpose or other illegal activities, and the conflict between the main stakeholders in cyberspace. This chapter tries to understand if there is a relationship between the COVID-19 pandemic and the domain name industry. Is there an attempt to profit from the registration of domain names? In particular, this chapter analyses the relationship between (1) exploitation of the pandemic through the use of terms related to the pandemic and their registration as domain names for the purpose of obtaining financial benefits from cyberspace; (2) the possible violation of the rights of the domain name holder; and (3) cases of fraud related to the pandemic in cyberspace. The author supports the assumption of this relationship with concrete facts and data and the study of a large sample of domain names across a group of 12 ccTLDs. ccTLD.[203]

1. The interaction between COVID-19 and the domain names industry

Besides the global prominence and urgency brought by the COVID-10 virus, the following factors played a role in catapulting it to a top online search term: uncertainty over its origins, public fear, lack of trust in governments and media, conspiracy theories and other disinformation, media conflict and censorship, erratic procedures taken by governments and other entities, the rapid spread and increase in infected cases, the death toll worldwide, and the online availability of live dashboards. Furthermore, there were the related economic shutdowns and other restrictions and curfews. All these factors contributed to increasing domain name registration related to COVID-19.

---

[202] *LaTessa Gray, Purchase of search engine ads for word marks is sufficient to constitute infringement, 16 June 2022, https://www.worldtrademarkreview.com/article/purchase-of-search-engine-ads-word-marks-sufficient-constitute-infringement*

[203] *Abbreviation for The country code Top Level Domains; in this regard, ccTLD is a two-letter code for a specific geographic territory, such as .za for South Africa and .uk for the United Kingdom. Every country is allocated a ccTLD. A ccTLD is further divided into second-level domains such as .co (commercial) and .org (organization). The complete ccTLD is then represented as .co.za and .org.zæ Numerous second-level domains may exist within each ccTLD domain name registrations may be restricted in certain countries in that registration iS reserved for applicants who satisfy certain criteria. J. P. Roelofse, From Innovation to Profit: An Entrepreneur's Guide, Publisher Juta and Company Ltd, 2006,p87.*

1.1 COVID-19 in the online space

Furthermore, the pandemic interactions such as Stay-at-Home, e-commerce, and marketing might affect how the domain name industry operated during this period[204]. "As the fact that the overwhelming majority of the world has been working from home, businesses and consumers rely heavily on the Internet and related IT resources– whether to engage in their 'day jobs,' to inform themselves, to shop online, or to stay safe in the current pandemic."[205] Meanwhile, any reduction or absence of normal activity needs to be balanced against consideration of the numerous volunteer activities carried out by companies and various other legal rights owners throughout COVID-19. Online news and other topics related to COVID-19, such as infection and preventive measures, also quickly became available[206].

According to at least one expert, the emergence of the pandemic led spontaneously to a high increase in using the Internet to search for information related to COVID-19, whether regarding the root of the virus, health care information, health advice, or to generally keep up to date about the COVID-19 situation[207]. From then on, the relationship between the domain name industry and COVID-19 seems clearer. In this section, the author will illustrate this relationship by investigating the registration of domain names related to coverage during the pandemic activity.

1.2 Increase in domain name registration related to COVID-19

In this regard, engine searches have driven fearful citizens to find information. Because of the nationwide lockdowns enforced in numerous states to combat the COVID-19 pandemic, online domain name enrolments related to COVID-19 and other terms connected to the pandemic have increased unprecedentedly. In this context, many more individuals have used the World Wide Web for various reasons: acquiring knowledge, interacting socially, working from home, or purchasing goods and services online. As a result, these actions and extraordinary circumstances associated with the pandemic significantly boosted domain enrolment related to COVID-19. This has led potential threats to customer privacy and safety controls. For example, and also as an inevitable outcome of such this scenario, cyber-criminals exploited the panic, changed circumstances, and the unpredictability prompted by the pandemic to trick vulnerable or distracted individuals people into clicking a harmful web link or allowing hackers access to their computer system or personal information[208].

COVID-19 domain names increased as a reaction to the COVID-19 pandemic. In this regard, one expert in the domain names industry, Sean McNee, indicated that the number of bad domains has grew exponentially, similarly to the number of cases of the disease worldwide."[209] Legitimate stakeholders have various reasons for registering COVID-19

---

[204] *Megan GrahamHow a stay-at-home year accelerated three trends in the advertising inid.*

[205] *https://www.wipo.int/amc/en/news/2020/cybersquatting_covid19.html*

[206] *Francis Gurry Intellectual property,innovation, access and COVID-19 ibid,p10.*

[207] *Liqaa F. Nawaf, Chaminda Hewage, and Fiona Carroll Minimization of Cyber Security Threats Caused by COVID-19 Pandemic ibid,p425.*

[208] *ibid,p425.*

[209] *Brandy Zadroznys,Who own coronavirus.com? Behind the lucrative profiteering on website ibid.*

domain names and other terms related to Coronavirus. One of the main reasons is to keep individuals updated on COVID-19 and to provide the right advice.

However, other, more dubiously motivated actors tried to take advantage of the pandemic situation in cyberspace both legally and illegally. In this regard, the previous study on 303 websites by Tombs indicates that around 80% of 300 domain names using coronavirus-related domain names, including Coronavirus, covid19, covid-19, sars-cov-2, and sarscov2, subjected to the mentioned study are governmental entities.[210] Moreover, nearly half were squatting domains or 'under construction.'[211.] the McNee study's importance was to find trustworthy entities by citizens or society to give correct information in light of the conflicting statements from different parties[212].

In this case, government websites were more trusted than the other sources of information, providing their societies with life-critical, coronavirus-related information. Moreover, the study indicated that due to matters of trust, top-level domain names must be limited to governmental entities, and not extended to single individuals or entities not involved in official pandemic response services. This conclusion was aimed at maintaining trusted channels between authorities and citizens throughout the crisis. [213] · In this context, three frames can indicate this relationship. These frames can be seen in the following criteria: **s**everal domain names registered to contain COVID-19 terms or related terms such as Coronavirus. The other criteria are presented in the fact that conflict over domain names related to the COVID-19 term have been brought before courts or arbitration committees due to infringement against other stakeholders in cyberspace. One of the most important criteria is that COVID-19 domain names were used maliciously.

The requests over domain names related to pandemic terms have dramatically increased during the pandemic[214]. For instance, during the two months from February 19 to March 19, 2021, customers made 562,144 queries to 8,080 unique domains, including the words 'COVID-19' or 'corona'. In this regard, there was an increase of 11,287,190 requests across 47,059 domains popular keywords, used together with corona, virus, and COVID-19, for new domain registrations: Wuhan, clinics, lab, tests, self-test kit, self-test kit purchase, kits, helpline. This also shows how a possible COVID-19-themed phishing domain could be purchased and used[215]. According to the huge number of new registrations and the growing efforts to make illegal uses, organisations operating different TLDs are attaching automated control Methodologies. In this context, it is worth mentioning that over 408,236,416 domains have been registered so far, including over 35,976 under the *.bg* area, 3,752,043 under *.eu* fields, and 167,465,081 within the *.com* field[216].

Furthermore, a new study by the leading security company, Check Point, indicated that coronavirus-related domain registrations rose by 6,000 per week. According to a statement launched by a software application firm, more than 2,200 dubious new domain names were

---

[210] *ibid*

[211] *ibid*

[212] *ibid*

[213] *ibid*

[214] *Giri Govindarajulu, Shyam Sundar Ramaswami, Shriram K. Vasudevan It's Your Digital Life ibid,p5-17*

[215] *Ibid p5-17.*

[216] *Yana Todorova, Mario Arabistanov, Can any word be my domain name? How about "COVID-19"ibid*

discovered in the previous three weeks alone. More than 93 were validated as harmful and hazardous to site visitors.

2. The COVID-19 pandemic's illegality in the domain names industry

COVID-19 caused a global health crisis and represented an existential threat to humanity[217]. It also emphasised the global importance of the Internet in the digital age, in managing the crisis. Undoubtedly, the COVID-19 pandemic shed light on the domain name industry. It was assumed immediately that the wWorld Wide Web would play a central role in spreading awareness about the pandemic and keeping people up to date, in the provision of news, important health databases, advice, and other services related to COVID-19.[218] Based on a study prepared in April 2020, the number of registered domain names connected to the COVID-19 pandemic increased significantly, showing that 70% of these websites contained useful material[219]. However, this did not prevent others from illegally using COVID-19 domain names and other terms related to the pandemic. In this context, it is more challenging to differentiate between the legitimate and illegitimate use of COVID-19. For instance, as mentioned earlier, the study indicated that it is important to give more attention to how domain names related to the pandemic will be used[220]. In this regard, taking advantage of the pandemic to register several domain names under COVID-19 and other related terms such corona, virus, and COVID-19, and using it illegally took different shapes such as malware, phishing, scams, ransom, spreading misleading information about the pandemic, and promoting fake products related to the pandemic such as vaccines, masks, and medicines. In this context, as shown by the study, 4% of the domain names related to COVID-19 have been used maliciously, such as malware, phishing or ransom, as mentioned above[221].

On top of that, the study by Tombs, N., & Fournier-Tombs found that 29.7% (90 out of 303 websites surveyed) contained misleading information, and possibly impersonated government authorities to sell unrelated products[222]. According to Domain Tools, a cyber-intelligence company that tracks the legality of domain usage, cybercriminals and spammers were motivated by the opportunity of a captive audience forced to stay at home, who inevitably turned to the Internet to find the latest information related to the Coronavirus; accordingly, an overwhelming majority of people chose to browse websites related to COVID-19 domain names in one way or another[223]. The study located several websites of dubious credibility, demonstrating the contrast between the unofficial and verified government websites. Almost 20% of the websites marketed industrial items or promotions, nearly 10% had domain names for sale, and 3 were verifiably harmful internet sites. The study team ascertained that 40% of

[217] *milica d. đekić, covid-19 as a Scam Challenge ibid.*

[218] *Oliver Hohlfeld, Andra Lutu, Dave Levin, Passive and Active Measurement: ibid,p40.*

[219] *Ibid,,p40.*

[220] *Ibid,p40*

[221] *Ibid,p40*

[222] *Tombs, N., & Fournier-Tombs, E. Ambiguity in authenticity of top-level Coronavirus-related domainsibid.*

[223] *Brandy Zadrozny , Who owns coronavirus.com? Behind the lucrative profiteering on website domains,Ibid.*

sites were under construction, with the implication that these would swell the ranks of the aforementioned categories once completed and launched.[224.]

Figure 2. Percentage of surveyed websites per category[225.]

Category	Count	Percentage
Purports to be a government website	32	10.56%
Government website confirmed	6	1.98%
Domain for sale	30	9.9%
Website overtly malicious	3	0.99%
Domain a commercial initiative (advertisements)	41	13.53%
Domain a commercial initiative (products)	20	6.6%
Website in construction	117	38.62%

2.1 COVID-19 Scam websites

Since the first wave of the pandemic, there has been a substantial wave of internet website fraud using COVID-19 as its primary device. In this context, scams involve fraudulence connecting to clinical tools, fee fraudulence, phony charities, and COVID-19-themed internet sites with concealed malware[226]. One specific fraud behaviour of using the COVID-19 pandemic in cyberspace is to deceive users in order to achieve an unfair financial advantage; it was also noticed that fraudsters chose COVID-19 pandemic domain names as a trending theme, to take advantage of a crowded online space in which their illegal activities were harder to detect[227.] In this context, "Fraud Watch International Society" indicated over 18 million phishing attempts using malware related to COVID-19 in April 2020[228]. It appears that websites, e-mails, and social media platforms related to COVID-19 were the favourite areas where scammers delpoyed their schemes for deceiving vulnerable or distracted people, using the COVID-19 pandemic as a trending theme and connecting it with domain names linked with these areas.[229] For example, spammers sent out emails with the objective of taking control of customers' "Microsoft Office 365" accounts. In this context, Virginia State Court released an order in a civil case brought by Microsoft. The business took handicapped domain names utilised in this attack. Microsoft won a court order against the site that used the COVID-19 domain[**230**.] To this point, Microsoft revealed that the criminal organisation using phishing strikes had utilised a site with the COVID-19 domain to pirate Microsoft

---

[224] *Tombs, N., & Fournier-Tombs, E.. Ambiguity in authenticity of top-level Coronavirus-related domains. Ibid.*

[225] *.. Ibid.*

[226] *Yung Au, Philip N. Howard, Project Ainita, Profiting from the Pandemic Moderating COVID-19 Lockdown Protest, Scam, and Health Disinformation Websites,ibid , p 2*

[227] *Milica d. Đekić, COVID-19 as a Scam Challenge ibid.*

[228] *Gregory C. Rasner,Cybersecurity and Third-Party Risk: Third Party Threat Hunting,,publishe John Wiley & SonsNew Jersey., 1st edetion2021 ,p79.*
-Yung Au, Philip N. Howard, Project Ainita, Profiting from the Pandemic Moderating COVID-19 Lockdown Protest, Scam, and Health Disinformation Websites, Ibid , p 2

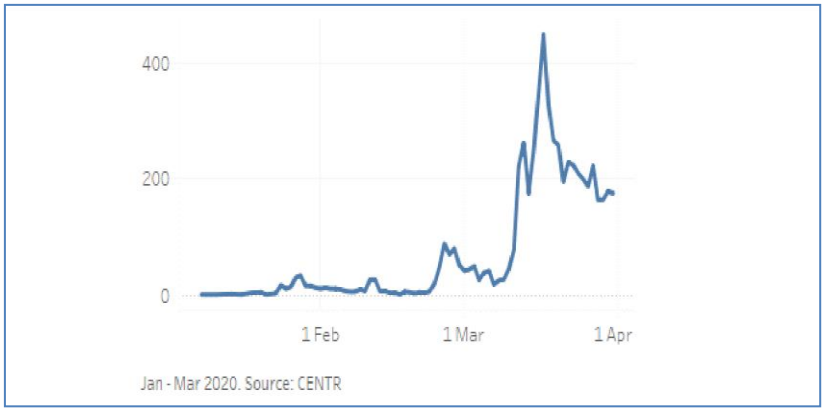
[229] *ibid, p 2.*

[230] *Steven Melendez Microsoft is seizing control of domain names associated with COVID-19 phishing scams. Ibid.*

consumer accounts and steal information. According to the article, the attacks were launched with phishing emails, with some referencing a "COVID-19 bonus offer," the targeted individuals clicked on web links that the messages contained, and those domains triggered web browsers to open an internet application that provided the criminals with access to the targeted individuals' "Office 365" accounts, including contact data, emails and all files in cloud storage[231].

Because COVID-19 affected over 210 countries, citizens worldwide are suffered similar negative impacts of COVID-19 and were thus similarly vulnerable to malicious online schemese seeking to take advantage of Covid-19. While it has been noted that the behaviours related to cybercrime did not notably change compared to the situation before COVID-19, a notable change was observed in the increased use of the World Wide Web[232]Furthermore, it was concluded that domain names connected to COVID-19 comprised the main sources of cybercrime in this regard, particularly the increased number of reports related to emails that have materials related to COVID-19[233]. Based on 114,219 new COVID-themed domain names approved since the beginning of 2020, half of these websites related to the COVID-19 domain names were malicious[234]. Moreover, the FTC unit indicated that scam websites related to COVID-19 domain names led to losses of $114 million, stolen from those browsing these websites[235]. According to another study by the Council of European National top-level domain registries**,** the COVID-19 pandemic has had no significant impact on the domain name industry, either in registrations or levels of abuse detected[236]. This study analysed 6164 domain name registrations within 12 groups of ccTLDs, including covid, corona, or virus expressions, from January to March 2020. The study concluded that the COVID-19 pandemic did not impact the domain name industry, as *Figure 3* suggests.

Figure 3 COVID-19 related to domain names registered during January & March 2020[237]



[231] *ibid*

[232] *Liqaa F. Nawaf, Chaminda Hewage, and Fiona Carroll Minimization of Cyber Security Threats Caused https://www.fastcompany.com/90525306/microsoft-is-seizing-control-of-domain-names-associated-with-covid-19-phishing-scams by COVID-19 Pandemic ibid 1,p425.*

[233] *ibid,p425.*

[234] *Tonya Riley,The Cybersecurity 202: Internet domain names are ripe for scam during coronavirus crisis washington post, September 8, 2020,https://www.washingtonpost.com/politics/2020/09/08/cybersecurity-202-internet-domain-names-are-ripe-scam-during-coronavirus-crisis/,*

[235] *Ibid.*

[236] *Council of European National Top-Level domain Registries(CENTR,), The true effect of corona on the DNS, ibid*

[237] *,Ibid.*

The study justified the result that there was no significant impact on the domain name industry by comparing registration numbers with the same period before the pandemic when 751.000 domain names were registered; this means that domains with a covid-related term (using one of the three terms) represent 0.8% of all new registrations in this period. However, it is the contention of the author that this study did not reflect the true impact of the corona pandemic on the domain name industry because it did not measure the impact of the identified 0.8% in terms of illegal use and financial damage.[238]

2.2 COVID-19 domain names virus: Worm and Ransom

Viruses can trigger huge damage to all sources of information related to the Internet and jeopardise the e-commerce environment, causing colossal revenue losses[239.] During the pandemic, viruses related to COVID-19 domain names took several shapes, such as worms and ransom.

2.2.1 Worms and Malware

Worms are a malicious code devices that automatically spread through all systems in cyberspace. This section is concerned with such worms exploiting the vulnerabilities of website browsers linked to the COVID-19 pandemic, and in general, the systemic risk posed to the public Internet, and most private networks, in terms of disruption or even total dysfunction.[240] In this regard, the healthcare and public health sectors are among other sectors that were particularly at risk during the COVID-19 pandemic, as the American government indicated[241]. The Global Threat Index report revealed that cybercriminals manipulated the profit rate from the pandemic to prolong their malicious activities, with numerous spam projects connecting to the virus. According to a recordby the web server and cloud safety programmer Trend Micro, there have been 41,500 spam e-mails regarding Coronavirus or COVID-19, with harmful web connections targeted at e-mail addresses signed up in the UK. This accounted for nearly a third of all malware assaults in Europe, Africa, and the Middle East combined. The so-called 'dark web' simultaneously hosted a plethora of coronavirus-related activities: special deals by various 'cyberpunks' or anonymous hackers, advertising their items, generally destructive malware or manipulation devices, were marketed over the dark web under propositions with COVID-19 or Coronavirus, complete with discount codes, to an audience of would-be cyber-attackers. Furthermore, the record showed that there was a 738% rise in terms of COVID-19 related terms on dark web resources in the one month alone.[242] In April 2020, Google reported more than 18 million daily scams related to COVID-

---

[238] *,Ibid.*

[239] *C B Gupta S. Chand's ISC Commerce For Class XI Publisheribid, p 300.*

[240] *Tim Rains ,Cybersecurity Threats, Malware Trends, and Strategies: Learn to mitigate exploits, malware, phishing, and other social engineering attacks, ibid ,p108.*

[241] *ibid ,p109.*

[242] *claudia glover 20 Mar 2020, Coronavirus-Related domain Registrations Rise 6,000 in a Week, Coronavirus Related domain Registrations Rise 6,000 in a Week ibid.*

19 domain names or content and phishing malware material and information links related to the COVID-19 pandemic[243] .

2.2.2 Ransom

Ransomware is another kind of malware that can have catastrophic results. . Once ransomware gets into a system, it will encrypt data and lock it until the victim pays money to the criminals to decrypt it. Attackers endeavour to extort all kinds of organisations, including clinics and hospitals; indeed, COVID-19 lock ransomware hit news headlines due to its impact on healthcare infrastructure.[244]

Upon evaluation, the search study was found to consist of 3 internet sites. Based on the study sample, the initial domain name (covid19.Mx) appeared to be a formal Ministry of Health domain name purporting to offer an internet coronavirus examination; however it rerouted customers to paid studies and advertising marketing. The website was removed soon after the information collection. The second domain name, called Coronavirus.Ws, redirected browsers to a scam pharma site offering fake medications, and also redirected browsers to a network of websites associated with the WordPress Pharma hacks. Another suspicious domain name (Coronavirus.Ma) rerouted individuals to a lotto game fraud that urged them to supply their private information in order to retrieve a reward. In order to determine if a detected Covid-19 domain is malicious and understand the impact on e-commerce related to the domain name industry, one needs to take a comprehensive vision of potential damage in cyberspace; In this regard, the 2020 status of the cyberspace field related to cybersecurity cost predictions indicated that Worldwide cybercrime expenses would reach $6 trillion by 2021 (Cybersecurity Ventures).

Moreover, Ransomware damage expenses alone were forecast to climb to $20 billion by 2021, with one organisation succumbing to ransomware attacks every eleven seconds. (Cybersecurity Ventures). According to specialists, damage from cybercrime is predicted to hit $10.5 trillion yearly by 2025.. The worldwide pandemic has led methods for cybercriminals to target numerous brand-new targets: the healthcare sector, unemployment benefits, remote employees, and many more. Here are a few of the most impactful cybersecurity statistics associated with the pandemic: Following the emergence of the pandemic, the FBI reported a 300% rise in reported cybercrimes. (IMC Grupo);,27% of COVID-19 cyberattacks target financial institutions or healthcare companies; COVID-19 was attributed to a 238% increase in cyberattacks on financial institutions in 2020; 81% of cybersecurity specialists reported that their work features have been altered throughout the pandemic (ISC, Fintech News); in May 2020, 33,000 unemployed candidates were subjected to a "Pandemic Unemployment Assistance Program Information Safety Violation" (NBC); 52% of legal and conformity leaders are worried about third-party cyber dangers resulting from remote jobs because of COVID-19 (Gartner); Americans lost more than $97.39 million

[243] *Dr Juan Lopez Jr, Dr Kalyan Perumalla, Dr Ambareen Siraj, ICCWS 2021 16th International Conference on Cyber Warfare and Security, ibid, p393.*

[244] *Tim Rains ,Cybersecurity Threats, Malware Trends, and Strategies: Learn to mitigate exploits, malware, phishing, and other social engineering attacks, ibid ,p111.*

on COVID-19 and stimulation check frauds (Atlasvpn); confirmed information violations in the healthcare sector swelled by 58% in 2020 (Verizon); remote working has increased the typical cost of an information violation by $137,000 (IBM); in April 2020, Google obstructed 18 million day-to-day malware and phishing emails associated with Coronavirus (Google); 47% of staff members mentioned distraction as the main factor for succumbing to a phishing rip-off while working from home (Tessian); half a million Zoom individual accounts were jeopardised and offered on a dark web discussion forum in April 2020 (CPO Magazine); In one year from January 1 2020, when the initial pandemic breakouts were announced, over 16,000 new coronavirus-related domain names were signed up. In this latter regard, at least two domain names were classified as very harmful: "buycoronavirusfacemasks.io" and "betacoronavirusvaccine.io." The experts recommended against any dealing with them.
On top of that, numerous actors are providing ransomware to endpoint gadgets, and Covid-Lock is a case in point. Covid-Lock takes control of a gadget, e.g. a smartphone, by encouraging the victim to access 'the latest' updated COVID-19 stats. A locked display will certainly result, with a message that threatens the deletion of all files and software on the device, unless the victim transfers $300 in anonymous Bitcoin. When it comes to COVID-19 domain names and other related terms such as virus, corona, or pandemic, it was noticed that the criminals do not use common TLDMs such as .org, .gov, or .com; rather, they use other types of domain names such as .io, due to the fact it was easier to obtained these in comparison to top-level domain names that are more often than not restricted to governmental and other organizational bodies [245].Many of these harmful domain names posed as the World Health Organization or medical care companies. Offenders utilised Covid-19 themed domain names to spread false information, host phishing web pages, imitate genuine brand names and organisations, and offer illegal or phony products and services.

2.3 COVID-19 pandemic impact on trademark counterfeiting

While the COVID-19 pandemic had a colossal impact on products and online promotions related to these products, it was observed that not all areas of the domain name industry were impacted equally. In this regard, authorities of law are most likely to be funnelled in the direction of public health for an extended period. This prioritisation implies that other vulnerable areas such as custom checks, market examinations, and other physical controls will certainly be far less policed during this time. Brand names and industries with substantial concerns in physical markets, e.g., pharmaceutical items, need therefore to anticipate a sudden and sustained drop in direct assistance from law authorities in the case of a major crisis. The only efficient method to fight cyber counterfeiting and misleading campaign related to these products online is to redouble online surveillance and eliminations[246]. The international demand for face masks, medicines, and various kinds of individual safety devices was accompanied by a doubling in the level of counterfeiting In this regard, law enforcement authorities in the United Kingdom discovered 31 million face masks with fake certification marks. Likewise, authorities confiscated phony hand sanitizers containing

[245] *Alex Guirakhoo*

[246] *Daniel Bennett Covid-19 and Counterfeiting: How the Pandemic is Reshaping Brand Protection – Part 2 What to Expect in the Short, Medium, and Long Term, ,ibid.*

outlawed chemicals that posed a possible health risk to customers. Such issues likewise encompass the authorities as well. For example, the US Customs and Border Protection reported fake coronavirus test devices. Furthermore, with decreased physical market checks, boosted online enforcement will influence offline examinations[247].

To this point, The US Attorney at Law's Office of the Maryland District confiscated *genobioscience.com, healthbridgescience.com, global-pandemic-vaccines.com,* as well as *genobioscience.com,* and *healthbridgescience.com,* every one of which purported to be "the websites of real biotechnology businesses establishing therapies for the COVID-19 infection" yet they made use of and gathered the information of people viewing the websites, using the data for malicious activities consisting of scams, phishing assaults, as well as the release of malware[248]. The question arises: How did the pandemic affect the domain name industry regarding online product trade? The prolonged duration of the pandemic certainly shaped the online shopping space, and kept volumes at a high level compared to the situation before the COVID-19 wave. This was notably evidenced in the rise and fall of demand for online streaming services and home exercise equipment, witnessed at the beginning and end of the pandemic and its lockdowns (curfews). In this context, it is highly expected that such these large markets will turn to eCommerce to cover the needs of millions of people under curfew, which as a result, would increase the flow of counterfeited products in one way or another, while at the same time, physical control and inspection processes will be decreased because of the restrictions imposed during the COVID-19 pandemic[249] and the diverted attention of law authorities towards policing healthcare and human restrictions. where the trademarks industries adaptmore quickly and flexibly to this new model, success and emulation by forgers will follow[250]. To this point, the Federal Trade Commission collected more than 170,000 customer complaints concerning coronavirus-related scams, from wonder remedies to phony masks, to falsified coronavirus alleviation checks.[251.]

2.4 COVID-19 domain names and misleading information

As people need information to feed their curiosity, misleading information is widespread across social platforms, intentionally and unintentionally. Social media sites have been criticised throughout the Coronavirus pandemic as an environment for the quick spread of false information. Investing an unhealthy amount of time looking for COVID-19 details on coronavirus-related domain names' and social networks has likewise been connected to anxiety prompted via online social media networks. In this regard, social networks might cause information overload and trigger psychological health issues. Scholars have recently asked for further studies to recognise the underlying motivators of concerns, anxiety, and

[247] *Ibid.*

[248] *U.S. Immigration and Customs Enforcement, HSI investigation results in seizure of 3 domain names purporting to be biotechnology company websites with COVID-19 treatments: At least 1 fraudulent website claimed to sell counterfeit vaccinationsUpdated, ibid*

[249] *Daniel Bennett Covid-19 and Counterfeiting: How the Pandemic is Reshaping Brand Protection ibid.*

[250] *ibid*

[251] *Tonya Riley,The Cybersecurity 202: Internet domain names are ripe for scam during coronavirus crisis ,ibid.*

tension[252]. In this regard, the extraordinary COVID-19 situation has radically changed the equation.

On top of that, the domain names related to COVID-19 have ignited concern and increased the debate about the amount of misinformation and misleading data flowing from websites related to COVID-19 domain names and to which extent would affect the pandemic situation and societal/citizens' health[253]. The study mentioned earlier suggests that the flood of misinformation is regulated by the communication standard enforced by the particular social media sites or/and by the certain communication patterns of customers involved with the subject. Social media sites can assist by fact-checking and flagging or removing misinformation, improved tailoring to social habits and communication styles, and customising interaction techniques in a crisis.[254] Because misinformation spreads quickly and reaches a more widespread public than the right information[255,] it was noticed that covid websites ignited the debate about misinformation about COVID-19, even despite the positive outcome of covid domain names and other social platforms allocated for discussing the pandemic, such as facilitating society awareness and encouraging increasing preventive measures against COVID-19. Unfortunately, these legitimate channels also paved the way for the spread of misinformation and negative emotions connected to COVID-19.[256] Some of the top domain names related to social media afford direct access to a huge amount of content that may magnify falsehoods and questionable rumours. The same researchers have observed that, for instance, platforms related to YouTube and Facebook domain names are directly linked to propagating conspiracy theories and misinformation on COVID-19 and other controversial medical issues.[257] Some surveys indicate that older internet users are more likely to share misinformation on social platforms,[258]as well as internet users with more conservative political leanings.[259] In this context, according to the study based on a random sample of American domain names, which were chosen from a checklist of sites monitored by the Arithmetic Propaganda Project the flow of incorrect rumours concerning COVID-19 at the beginning of March 2020 consisted of websites distributing misleading information regarding traditional medicine, anti-vaccination information, COVID-19 pandemic rejection claims.

Additionally, many more common sites were recognised as distributing scams. It was noticed that less than a third of these websites were generated in 2020[260]. The study by Tombs, N., & Fournier-Tombs found that 29.7% (90 out of 303) of internet sites contained false

---

[252] H. Dan O'Hair, Mary John O'Hair, Communicating Science in Times of Crisis: COVID-19 Pandemic Communicating Science in Times of Crisis, ibid,,p132.

[253] Yung Au, Philip N. Howard, Project Ainita, Profiting from the Pandemic Moderating COVID-19 Lockdown Protest, Scam, and Health Disinformation Websites, ibid , p 3

[254]Matteo Cinelli, Walter Quattrociocchi,AlessandroGaleazzi , Carlo MicheleValensise , Emanuele BrugVolume 10 noli , Ana Lucia Schmidt , Paola Zola , Fabiana Zollo & Antonio Scala ,The COVID-19 social media infodemic,Scientific Reports, Issue 16598, Publisher Nature Publishing Group p6.

[255] Patrícia Arriaga, Francisco Esteves, Marina A. Pavlova, Nuno Guerreiro Piçarra Coronavirus Disease (COVID-19): The Impact and Role of Mass Media During the Pandemic, Publisher Frontiers Media SA,1st edetion 2021,p38

[256]H. Dan O'Hair, Mary John O'Hair, Communicating Science in Times of Crisis: COVID-19 Ibid,p132.

[257]Ibid,p132.

[258] Yung Au, Philip N. Howard, Project Ainita, Profiting from the Pandemic Moderating COVID-19 Lockdown Protest, Scam, and Health Disinformation Websitesibid , p3.

[259] ibid , p 3.

[260] ibid , p 3

information due to accumulation. This false information reveals a remarkable degree of opportunism linked to the pandemic. The 'infodemic' of false coronavirus information appeared to be discovering new opportunities to develop and proliferate. Domain name registration experienced a rise and was significantly used to spread false information and participate in prohibited and tricky tasks[261].

Experts and specialists consider that the rise in incorporating pandemic-related terms with widely known trademarks was driven by a substantial boost in modern electronic technologies and an enhanced demand for the domains[262]. Oddly, the surge in COVID-19 seems to have sustained the pattern with a spike in cybersquatting situations. COVID- 19 related domain names indicated that the situation of most individuals functioning from home improved the business of e-commerce internet sites, with home-delivery services and one-click orders now commonplace[263] The pandemic's effects make social networks and pharma markets the most vulnerable. Extensive reports, incorrect details, misguided projects, and fake medicines being guided via domain names similar to preferred internet sites, such as Google (coronavirusgoogle.com) and Facebook (facebookcovid19.com), have triggered a substantial effect. While these firms have dealt with these problems by selecting a uniform domain-name dispute-resolution policy, comparable subjects will likely proceed. Businesses must constantly be active in shielding their brand and relevant domain names[264].

On the other hand, another question arose: can people express their opinions under the principle of free speech even if these opinions contain some misleading information? The author believes the COVID-19 pandemic must be treated as an exception to the free speech principle because incorrect information would affect society and individuals' health. This case will be more concerned with the parallel founding of the vaccine[265]. At this time, it was noticed that many websites related to the covid domain names promote misleading information related to the COVID-19 vaccines and are based on scientific myths. In this regard, it was observed that COVID-19 infection situations are increasing among the individuals who reject immunization against COVID-19 on the basis of covid disinformation disseminated on social networks in tandem with the covid domain names.

Furthermore, anti-vaccine organizations have triggered what a Harvard Medical School doctor, Aditi Nerurkar, calls "vigilante medication," where individuals are delaying or refusing possible lifesaving treatment in favour of unverified treatments recommended by social media groups[266]. These websites and social platforms related to COVID-19 domain names urge people not to get the vaccine and push them to even leave the hospital's ICU. According to medical facts, people who do not get the COVID-19 vaccine are in danger of getting infected or even dying. In this regard, 'anti-vaccine' Facebook groups have put colossal pressure on their community members to reject vaccines and other medical

---

[261] *Tombs, N., & Fournier-Tombs, E. (2020). Ibid.*

[262] *Rupali domain of cheats: Cybersquatters using Covid to spread infodemic - Times of India https://timesofindia.indiatimes.com/india/domain-of-cheats-cybersquatters-using-covid-to-spread-infodemic/articleshowprint/81264726.cms 1/5 domain of cheats: Cybersquatters using Covid to spread infodemic TNN | March 1, 2021, 04.21 AM IST Printed from MUMBAI:*

[263] *Mukherjee, Rupali. domain of cheats: Cybersquatters using Covid to spread ibid.*

[264] *Ibid.*

[265] *Ben Collins , 'Vigilante treatments': Anti-vaccine groups push people to leave ICUs,NBC news, https://www.nbcnews.com/tech/tech-news/vigilante-treatments-anti-vaccine-groups-push-people-leave-icus-rcna2233 Sept. 24, 2021,*

[266] *Ibid*

treatment, even pushing them to leave the emergency room and get their other family members out of the ICU[267]. Their justifications were based on conspiracy claims, for instance, that doctors intentionally kill their patients[268]. Another justification that the author believes is even more dangerous is the claim that casts doubts about vaccine safety, referring to injuries and the profit-driven pharmaceutical industry. Since the pandemic, these claims have become more sophisticated. They now refer to elaborate statistics, apparently supported by test results, to increase credibility among the targeted audience[269]. It was noticed that the misinformation related to COVID-19 has been growing as a cause of anxiety.

Early studies indicated that individuals who tend to drift toward conspiracy anecdotes on social platforms are more expected to automatically promote misinformation claims than individuals who scientifically approach social and other societal cases[270]. Active user participation supports the anecdotes, with users forwarding them and positively commenting[271]. On this point, misinformation is to be disintinguished from disinformation, in terms of intent: disinformation is the deliberate development or sharing of details known to be deceptive or incorrect, whereas misinformation is considered to be unwitting. As assumed by COVID-19, misleading data goes beyond spreading rumours and includes etiology, transmission, treatment monitoring, and healing. If extensively adopted, misleading COVID-19 information risks dissuading people from healthy and balanced preventive actions and harm reduction. It can compromise effective treatment and funding allocation. It can erode trust in health systems, even to the extent of jeopardising the safety of health employees in addition to philanthropic benefactors and volunteers devoted to stopping COVID-19's spread[272].

Furthermore, misinformation increases infection and causes death. In this context, social media sites related to COVID-19 domain names, including social platforms, particularly Twitter, comprise a significant component of COVID-19 misinformation. Furthermore, an evaluation of 1500 ‘misinfodemic’ tweets regarding COVID-19 was assessed by 92 fact-checking companies. It was confirmed that Twitter’s managers systematically circulated and developed COVID-19 misinformation[273]. Another study indicated that peers' opinions about vaccination in influenced individuals due to their relying highly on their peers' advice.

Moreover, this impact was very clear on social media platforms. Further studies examining the opinions on vaccination across different websites associated with the covid domain name terms (including highly actively influencing social platforms) may help determine what makes individuals reject vaccines and then jeopardise their own communities, in particular,

---

[267] *Ibid*

[268] *Ibid*

[269] *Kim ward, Ask the Expert: Social media’s impact on vaccine hesitancy, https://msutoday.msu.edu/news/2021/ask-the-expert-social-medias-impact-on-vaccine-hesitancy?collection=79022467-cc5d-4b0d-9d69-8f773df52178, June 15, 2021,*

[270] *Patrícia Arriaga, Francisco Esteves, Marina A. Pavlova, Nuno Guerreiro Piçarra ,Coronavirus Disease (COVID-19): The Impact and Role of Mass Media During the Pandemic, ibid,,p39.*

[271] *Yung Au, Philip N. Howard, Project Ainita, Profiting from the Pandemic Moderating COVID-19 Lockdown Protest, Scam, and Health Disinformation Websites,ibid ,p 3*

[272] *Ing. Carsten Busc,, Prof. Dr. Tilo Wendler, Martin Steinicke ,ECEL 2020 19th European Conference on e-Learning, Publisher Academic Conferences International Limited ,UK,1ST edetion, 2020,p43.*

[273] *Ibid,,p43.*

old and ill people[274]. Certainly, the author understands this behaviour presented in rejecting vaccines is driven by misleading information, which may spread among people on the Internet, and when a person dies as a direct result, the situation might arguably be presented as a homicide. The authorities would then be expected to initiate criminal responsibility against those found to be using these websites to promote misleading information. In particular, the campaign to reject the vaccine based on misleading information flowed from websites related to the COVID-19 pandemic.

3. COVID-19's financial effect on the domain name industry

To understand the effect of COVID-19 on the domain name industry fully, the final side related to this industry needs to be analysed, such as the cost of COVID-19 related domain names registration, covid domain name related terms' trade, COVID-19 domain name related advertisements, and the damage costs of using covid domain names illegally to obtain ransom.

3.1 COVID-19 domain names' registration cost

According to data on domain names registered since the pandemic began, 100,000 domain names related directly to COVID-19 or other related terms such as a virus (Vprpons.) or COVID-19 vaccines have been registered. These numbers show how the COVID-19 pandemic impacted the domain name industry by the increasing number of domain names, reflecting the economic effect. In this context, the registration cost per year ranges from $5 to $500, depending on the service package provided by a *registrar*, such as storage space, bandwidth, privacy options, search engine submission services[275], domain registration fees, site design, and, in some cases, professional copy, photography, and artwork used to populate the site.[276] In this connection, the register agencies would be expected to greatly benefit from the high demands over domain names related to covid-related terms. The minimum cost of registration is 5x100000 =500000$ while the maximum is 500 x100000 =50000000 $.

3.2 COVID-19 domain names' trade cost

Covid-19 increased the domain name trade, in particular via the domain names related to Coronavirus. These domain registrants profited from an arbitrage possibility by quickly enrolling emerging keywords[277]. On the other hand, the coronavirus domain names and other terms related to the COVID-19 virus became attractive as a chance to gain profit. For instance, coronavirus-related domains increased to more than 68,000 in 2020. According to *Domain Tools*, a cyber-intelligence company that tracks such domains, COVID-19 quickly became a "hot item" in the domain marketplace[278]. The domain names related to COVID-19

---

[274] *Derina Holtzhausen, Jami Fullerton, Bobbi Kay Lewis, Danny Shipka ,Principles of Strategic Communication Publisher Routledge, new York, 1st edition,2021,p13.*

[275] *Lisa Sabin-Wilson, WordPress For Dummies Publisher John Wiley & Sons, USA. 9th Edition 2021,p33.*

[276] *Barbara Weltman J.K. Lasser's Small Business Taxes 2021: Your Complete Guide to a Better Bottom Line, Publisher John Wiley & Sons, usa,10th edetion,2021,p372.*

[277] *Tombs, N., & Fournier-Tombs, E. (2020). Ambiguity in authenticity of top-level Coronavirus-related domains. ibid,p5.*

[278] *Brandy Zadroznys,Who own coronavirus.com? Behind the lucrative profiteering on website ,ibid.*

pandemic registration were registered for different reasons, for example, to run a business online or to be connected to health care sectors. Besides that, the other reason to register such domain names was to resell them to individuals or companies interested in these kinds of domain names. They considered the real value of domain names related to the pandemic or the high expected value in the near or far future. In this context, as was mentioned earlier, the study indicated that the average resale value was 10,889$[279]. As needed, governmental agencies had to compete against domain squatters to access their ccTLDs. For instance, the website containing covid19.pl was offered for 100,000 Zloty (roughly USD 23,900). According to the GoDaddy company, the first-year cost of registering a .pl domain is $0.5, meaning that this registrant is reselling at a 4,780,000% markup[280].

3.3 COVID-19, investments and ethical questions

Despite the tragedy and suffering caused by the COVID-19 pandemic, some investors looked to benefit from the health crisis. It is crystal clear that some people decided to gain some profit in the domain name industry by quickly booking and registering domain names related to the coronavirus terms, hoping they would resell them at high prices. In this regard, the domain name coronavirus.com can be expected to be highly attractive and would quickly attract investors experienced in the industry. For instance, a domain name dealer, Schultz, was the previous domain name owner related to the Ebola virus. After he succeeded in booking the domain name Ebola.com, he sold it later for $200,000 in 2014. This experience motivated him to retry the same adventure with the coronavirus pandemic. In this regard, Schultz bought the (coronavirus.org) domain name for a registration fee of $9.[281] · He was not able to obtain the other domain name, covid19.com, whose owner is unknown because he is covered under a pseudonynmous identity. In this context, the market researcher, IBISWorld, confirmed that the domain name trade industry in 2019 was estimated to have produced more than $6.4 billion in profits[282]. In another context, the domain names industry increases the debate about ethical standards for trading COVID-19 themed domain names.

Nevertheless, the Coronavirus has likely appeared to be a good possibility for many individuals interested in gaining profits, specifically in the domain market. Many respectable investors in the domain name industry avoid investment in pandemic-related domains. In this context, Elliot Silver, a domain name investor, said: "They constantly appear to be individuals acquiring domains connected to catastrophes." COVID-19 has indeed incarnated the concept of transforming a disaster into an opportunity[283]. In this regard, the author believes that the industry's decision-making must consider ethical standards to restrict these domain names and limit them to scientific, educational, and health institutions and organisations besides governmental agencies.

---

[279] *Tombs, N., & Fournier-Tombs, E. (2020). Ambiguity in authenticity of top-level Coronavirus-related domains. ibid,p5.*
[280] *ibid,p5.*
[281] *Brandy Zadroznys,Who own coronavirus.com? Behind the lucrative profiteering on website domains ibid.,*
[282] *Ibid.*
[283] *Ibid.*

3.4 COVID-19 domain names advertisement cost

The stakeholder interaction during the pandemic shows strong evidence that domain names related to COVID-19 have played a big role in the domain names industry based on advertisement factors. The study showed that COVID-19 related domain names dramatically affect the industry. The advertisement-related COVID-19 domain names took a different shape. For instance, many health professionals used social media to promote preventative health behaviours during the Coronavirus disease epidemic. In this regard, over 90% of the almost 100,000 pandemic-related domain name enrolments were approved by domain name dealers aiming to generate income using pay-per-click profits or re-sale. The specific suite of domain names starting with the 'coronavirus,' 'covid19', and 'covid-19' tags have likely been signed up throughout more than 400 expansions worldwide[284].

Furthermore, As the experts agree, during the COVID-19 pandemic, digital advertising on the Internet dropped, with surveys indicating a 9% drop generally throughout Europe, and Germany and France dropping by 7%-12%. The first three quarters of 2020 had a comparable effect to the economic crisis in 2008. The advertising market had previously expanded to approximately $646 billion in 2019. On top of that, the pre-coronavirus advertising market had been anticipated to increase to $865 billion by 2024. The coronavirus pandemic compelled a rethink. In this context, trackers, which have come to be an essential aspect of websites, deserve closer attention. Trackers are items of software applications that gather details regarding individuals and their online behaviours and preferences. Generally, tracking occurs with web browser cookies, internet browser fingerprinting, and IP monitoring. In this context, the trackers' classifications include advertising services, information collection, and behaviour evaluation.

Furthermore, the tracker's function is extended to include targeting and analytics such as data analytics, website use, and efficiency trackers. Essential trackers like tag supervisors and personal privacy notifications are important to a website's performance. Widgets are embedded on several websites and bring information through websites (usually back to social media sites).[285] On the other hand, nearly 70% of the trackers on COVID-19-pandemic disinformation sites are marketing trackers. This shows how much these disinformation sites depend upon marketing as a financial resource. Google, as well as Facebook, have especially common visibility throughout all four-tracker classifications as well as in all site examples. As stated, Google and Facebook agreed to eliminate advertisements that are intended to misinform their users about the COVID-19 pandemic.

Nonetheless, to what degree advertisements have been eliminated and what role networks play, is not completely clear. For example, if an advertisement is eliminated from Twitter or YouTube, it is not clear whether it is also then eliminated from Google. Also, Facebook is even more basic in terms of advertising and marketing and analytics related to its communities. Meanwhile, the tracker's economic impact has become a big component of the information sector. According to an evaluation launched by GumGum, most online web

---

[284] *Chris Melka, COVID-19 domains: what's going on?, APRIL 9, 2020, https://clarivate.com/markmonitor/blog/covid-19-domains-whats-going-on/*

[285] *Jonathan Walfisz, Verizon recovers infringing covid-19 domain names; Michael Jordan ends long-running dispute; Syria fee changes – news digest, 14 Apr 2020, world reademark reviwer, https://www.worldtrademarkreview.com/anti-counterfeiting/verizon-recovers-infringing-covid-19-domain-names-michael-jordan-ends-long*

content consisting of key phrases connected to the coronavirus pandemic is not risk-free for brand name marketing. With COVID-19 dominant in news coverage, many marketers were hesitating or even pulling internet marketing investment to avoid the reputational risk of showing up alongside COVID-19 conspiracies and rumours, with COVID-19 included in keyword obstructing devices.

Nonetheless, the evaluation launched by Verity agency determined 2.85 million web pages, including covid-related keywords. GumGum's research found that 62% of material containing covid-related keyword phrases is "brand name risk-free." All the worries elevated recently concerning coronavirus search phrases are subject to blocklist mechanisms[286]. Furthermore, those domains are names involved in commercial campaigns whose websites deal with advertising and marketing, straight item sales, or associate web links to market areas such as Amazon. These commercial sites typically rely on information and infographics from trusted organizations. For example, the research highlighted Moldova's covid-19.md, selling emergency supplies. Product web links to supposed hand sanitizer or masks N95r were intermixed with "John Hopkins University" information charts, video clips of the head of the WHO, and main CDC infographics[287].

As a result of COVID-19, there was a boosted demand for information. This field saw a 52% rise in advertisement investing betweenMarch 1 and March 18, 2020. Various other areas saw surges in promotion investing including interests and hobbies (31%), innovation and computers (14%), and also education and learning (13%). Significantly, these are all tasks that can be done in the house. Before the COVID-19 pandemic, eMarketer anticipated that search advertisement investing would climb by 14.4% in 2020. Without a doubt, they recommended there would certainly be a constant surge in search advertisement, continuing to at least 2024. In the early days of the COVID-19 pandemic, however, with lockdowns throughout the globe and disruption on the Internet, online purchasing was not yet typical. There was actually a decrease in internet purchasing questions, especially in the travel market[288].

Nevertheless, despite (and in some ways, because of) the long period of the pandemic, online search recouped its losses, as online purchasing became the standard. eMarketer estimated a 5.9% development in search advertising costs during 2020.They currently anticipate marketers will invest $99.22 billion on exams in 2024, up from their earlier estimate of $91.32 billion. Bazaarvoice evaluated over 5,000 customers in several nations for more information concerning their vacation purchasing strategies in the post-COVID world. Customers in all these nations recognised that they went shopping much more on the Internet than before the pandemic: Canada (59%), the United States (62%), the United Kingdom (58%), Germany (32%), Mexico (70%), France (41%), and Australia (47%). Overall, 49% of buyers claim they shop online more than pre-COVID[289].

---

[286] *Jonathan Walfisz, Verizon recovers infringing covid-19 domain names; Michael Jordan ends long-running dispute; Syria fee ibid.*

[287] *Tombs, N., & Fournier-Tombs, E. (2020). Ambiguity in authenticity of top-level Coronavirus-related domains. Ibid p5.*

[288] *Jonathan Walfisz, Verizon recovers infringing covid-19 domain names; Michael Jordan ends long-running dispute; Syria fee changes ,ibid.*

[289] *Ibid.*

3.5 Covid-19 related domain names conflict cost

Any analysis of the impact of the COVID-19 pandemic on the domain name industry must consider the cost of the conflict between the main. As related in the studies mentioned earlier, the number of domain name registrations related to the COVID-19 pandemic increased; a similar increase can be expected in the number and scale of conflicts between interested parties in the domain name industry. Besides the time and effort spent by the fighting parties to prove the rights related to domain names and rights related to their trademarks, the most tangible cost will be in the form of compensation paid upon violating the contested rights of trademark holders. In this regard, each conflict's cost will depend on the method by which it is solved. To this end, there are two main ways: judiciary and arbitration. In this regard, the American courts have ordered the closure of more than 300 fraudulent websites selling health and safety device brands related to the Coronavirus in the USA.[290] In this regard, the American Lanham Act or the domain name act of 1999[291] that makes cybersquatting illegal[292] indicates the cost of the conflict in the court. The judge can grant rightful damages up to $100,000 per single domain name violation. For instance, the Court applied the Lanham Act in *Crossfit, Inc. v. Davalos*. The Court granted Crossfit $100,000 as statutory damages besides the attorneys' cost[293]. As for resolving the conflict by arbitration, the World Intellectual Property Organization (WIPO) provides a unique treatment that allows trademark holders and proprietors to solve malicious domain enrolment.

Furthermore, the World Intellectual Property Organization is an international supplier under the Uniform Domain-name Dispute Resolution Policy (UDRP rules) [294]. This forms and alternative solution to the conflict over contested domain name rights. It appears in the shape of fees according to the domain name's number attached to the complaint and the number of panelists[295] based on the following schedule.[296] The cost mentioned in the schedule contains a total to be preserved by the center of WIPO as a management cost and a specific amount to be paid to the designated panelist[297]. For instance, as *Figure 4* suggests a single panelist costs between $1500[298] to $5000[299]

---

[290] *Tonya Riley,The Cybersecurity 202: Internet domain names are ripe for scam during coronavirus crisis washington post, ibid.*

[291] *Michael Wallace ,Larry Webber, IT Governance: Policies and Procedures, Publisher Wolters Kluwer ,New York. 2021 , P 22-34.*

[292] *Roger LeRoy Miller Business Law Today Essentials: Text and Summarized Cases, Publisher Cengage Learning, 2021,p164*

[293] *Frank B. Cross, Roger LeRoy Miller ,The Legal Environment of Business: Text and Cases Publisher Cengage Learning, new York, 11th edition,2020, P 172 ibid*

[294] *World Intellectual Property Organization, Guide to WIPO Arbitration Publisher WIPO, 2020 Volume 919 of WIPO Publication,P34.*

[295] *Maud Piers, Christian Aschauer, Arbitration in the Digital Age: The Brave New World of of Arbitration , Publishe Cambridge University Press, UK,1st edetion,2018, p236*

[296] *Wipo, Schedule of Fees under the UDRP (valid as of December 1, 2002), https://www.wipo.int/amc/en/domains/fees/*

[297] *Ibid*

[298] *Ian Johnstone, Steven Ratner Talking International Law: Legal Argumentation Outside the Courtroom PublisherOxford University Press,UK & USA, 1st edetion,2021,p291.*

[299] *Ibid ,p291.*

- Wipo, Schedule of Fees under the UDRP ,ibid.

Figure 4 Single Panelist

Source https://www.wipo.int/amc/en/domains/fees/

Number of Domain Names Included in the Complaint	Fee (United States Dollars)
1 -5	1500 :1000; WIPO Center: ,Panelist: 500]
6 -10	2000: WIPO Center: 700]Panelist: 1300;
More than 10	To be decided in consultation with the WIPO Center

"Number of Domain Names Included in the Complaint	Fee (United States Dollars)
1 to 5	4000 [Presiding Panelist: 1500; Co-Panelist: 750; WIPO Center: 1000]
6 to 10	5000 [Presiding Panelist: 1750; Co-Panelist: 1000; WIPO Center: 1250]
More than 10	To be decided in consultation with the WIPO Center."

4. COVID-19 pandemic effect on government domain names

One of the key areas of the domain name industry during the COVID-19 pandemic was governmental domain names. The effect of the pandemic has reflected on the domain names at the governmental level. It became difficult to validate the identity of these domains, bearing in mind that such domain names before the pandemic were fully trusted and secure. The study mentioned above suggested that the pandemic prompted the registration of false government websites connected to COVID-19 terms that were actually overtly harmful websites with a commercial nature. The author considers this study to be very important because governmental domain names must keep credibility as they are considered the main communication channel between the state and society.

Furthermore, any threat to this stability jeopardises the state's own credibility and trust in relation to its citizens. The illegal stakeholders took advantage of the obscurity of what makes up false information emphasised by the high-level domain name technicality.

The challenge in developing domain possession is that the research study cannot completely establish the right for 81.25% (or 24 of 32) of domain names that appear to be governmental. The study found that developing domain possession, and simply dealing with government

domain names, is challenging unless governments utilise a restricted second-level domain name. The study looked at the websites' security certificate register to establish ownership[300].

Certification by a third-party authority involves securing traffic between a customer and a website using the HTTPS procedure. This third party can be a governmental entity but is frequently non-government, making it less reliable for validating domain name possessions. Moreover, website traffic from specific domain names that seem governmental, for instance, Mauritius' *covid19.mu*, is unencrypted across HTTP, indicating that no certifications will be readily available for verification. Mozilla Browser or Firefox Browser designer recognizes five federal governments as certificate authorities, specifically Spain, Hong Kong, Taiwan, Turkey, and The Netherlands[301.]

5. COVID-19 pandemic impact on the conflict in the domain names industry: The legal issue related to Covid trademark

Since the COVID-19 pandemic emerged publicly, increasing the registration of domain names related to COVID-19 has impacted the industry negatively. One clear impact was increased domain name conflicts related to covid-themed and other trademark rights[302]. There are two situations to differentiate between the conflicts regarding the illegal usage of the domain name. The first type of conflict is where the domain is the essence of the conflict, and the second type is where the domain name *per se* is not included as a contested right (even if the domain name results in contested rights later[303], e. g. for scams, counterfeiting, and misleading news, besides various ransom viruses that use the covid domain name as a cover.

The first type of conflict happens when the domain name owner embeds someone's trademark in his domain name, whether to benefit from the fame of this mark or to intend to resell this domain to the trademark holder, known as cybersquatting[304]. Logically, the domain name is supposed to contain the same items as the other trademark holder or is confusingly similar[305]. Drug firms, particularly, need to watch out for cybersquatting risks because scammers were seen to capitalise on the buzz regarding new medications reported to treat COVID-19.

Furthermore, imitations of these medications can be easily offered online, utilising trademarked names for the medicines in the domain to induce website traffic and suggest recommendations. In this context, the first 'coronavirus' UDRP rules instance was submitted on March 19, 2020, relating to *coronavirusgoogle.com*. After the proprietor granted the domain transfer, Google recouped *googlecoronavirus.com* via the UDRP rules. Along with these two Google instances, fellow tech giant Facebook is associated with a conflict over *facebookcovid19.com.*[306] In this regard, in November 2020, the World Intellectual Property

---

[300] *Nathanael Tombs, Eleonore Fournier-Tombs, Ambiguity in authenticity of top-level Coronavirus-related domains, The Harvard Kennedy School Misinformation Review1 August 2020, Volume 1, Special Issue on COVID-19 and Misinformation,Attribution 4.0 International (CC BY 4.0) ,Reprints and permissions: Website: misinforeview.hks.harvard.eduAUGUST 31, 2020,p4*

[301] *ibid,p4*

[302] *WIPO's Anti-"Cybersquatting" Service Surpasses 50,000 Cases amid COVID-19 Surge Geneva, November 30, 2020 PR/2020/869 https://www.wipo.int/pressroom/en/articles/2020/article_0026.html*

[303] *Council of European National Top-Level domain Registries(CENTER), Measures taken by registries to help tackle COVID-19 related online abuse, Ibid.*

[304] *Roger LeRoy Miller Business Law Today Essentials: Text and Summarized Cases, Publisher Cengage Learning, 2021,p164.*

[305] *Frank B. Cross, Roger LeRoy Miller ,The Legal Environment of Business: Text and Cases Publisher Cengage Learning, , ibid P 172.*

[306] *Safenames organization, Cybersquatting and Opportunism: The Heightened Threat During ibid.*

Organization confirmed a considerable increase in cybersquatting[307], occurring from a rise in Internet use in parallel with the start of the COVID-19 pandemic. According to the report released by WIPO's arbitration and mediation center, the relationship between the COVID-19 pandemic and increasing cybersquatting cases was confirmed. From January to October 2020, the WIPO center managed 3,405 cases, presenting an 11% rise over the same duration throughout 2019[308].

There are three recurring UDRP rules situations, including the KALETRA medication. In one instance, the questioned domain settled on an internet site marketing the medicine to buy within dealing with Coronavirus. KALETRA underwent clinical research studies concerning its ability to deal with the infection. It is clear that dealing with pharmaceutical trademark abuse in the domain name in the context of a pandemic is not simply defending against brand name tarnishing or dilution; it goes beyond that to include the defence of public safety and national and international security[309].

Moreover, cybersquatters utilise terms like COVID-19, corona, medications, and vaccinations within the questioned and disputed domain names to churn out fake reports, incorrect information, and misleading campaigns. According to Erik Wilbers, WIPO supervisor at the mediation center: "among the many indications of cybersquatting is the malicious enrolment of web domain names created to take advantage of public health situations. In contrast, other stakeholders, including companies, struggle to keep their brands' reputations and keep them safe from cybersquatters.[310] A deep investigation revealed some weak points related to best practices in dealing with domain name violation issues during the pandemic. For instance, UDRP rules represent an approach to fight cybersquatting. Based on this mechanism, the trademark Clearinghouse (TMCH), the registries, and the registrars can be provided with an updated global list of trademarks during domain name enrolment to prevent third-party infringements on trademark rights[311]. This mechanism was fairly effective in a normal situation where a trademark holder could protect his right versus illegal domain names. However, during the COVID pandemic, this mechanism fell short of protecting the trademark holders against cybersquatting because COVID-19 and other terms related to the pandemic were not considered trademarks *per se*. There was no real owner for these terms registered as domain names[312]. The UDRP committee decision regarding *Gilead Sciences, Inc. v. Main Contact* supports this point of view. In this context, the committee indicated that the different corona theme used in the domain name does not distinguish the complainant's GILEAD mark from the domain name. Rather, this term increases the probability of confusion[313]. Several trademarks have suffered from cybersquatters who seek brand domains using coronavirus terms to cover their illegal behaviours. For instance, Verizon was surprised that its name was engaged with several covid domain names such as *verizoncovid19.com,*

---

[307] *WIPO's Anti-"Cybersquatting" Service Surpasses 50,000 Cases amid COVID-19 ,ibid.*

[308] *Ibid.*

[309] *Safenames organization, Cybersquatting and Opportunism: The Heightened Threat During Coronavirus ibid.*

[310] *Tombs, N., & Fournier-Tombs, E. (2020). Ambiguity in authenticity of top-level Coronavirus-related domains. Ibid.*

[311] *Oliver Hohlfeld, Andra Lutu, Dave Levin · Passive and Active Measurement: 22nd International Conference, PAM 2021, Virtual Event, March 29 - April 1, 2021, Pro ceedings2021, Publisher Springer Nature, 2021,p49.*

[312] *Oliver Hohlfeld, Andra Lutu, Dave Levin · Passive and Active Measurement,ibid,p49.*

[313] *Gilead Sciences, Inc. v. Main Contact Case No. D2020-0776*

verizoncovid-19.com, and verizoncovid19.info[314.] Besides that, WIPO witnessed increasing cases of conflict of domain names related to corona themes violation of famous trademark holders. In this context, considerable numbers of conflict cases were presented for WIPO to deal with, significantly in the section of banking and finance, biotech and pharma, and Internet and IT, as well as events-related classifications as coronagileadsciences.com[315] tokyo2021.org, wwwlillycovid19testing.com, *facebookcovid19.com, tokyo2021.cn, gileadcopay.co, HMRC-refund-covid-19.com, sanofivaccine.com, and dettolhandsanitizer.com.*[316]

[314] *Jonathan Walfisz, Verizon recovers infringing covid-19 domain names; Michael Jordan ends long-running dispute; Syria fee changes ibid.*

[315] *(WIPO Case No. D2020-0776),*

[316] *WIPO, Covid-19 Update on WIPO's UDRP and ccTLD Case Operations March 20, 2020),https://www.wipo.int/amc/en/center/wipocenterupdate.html*

SECOND PART: DOMAIN NAMES VS. TRADEMARK CONFLICT MECHANISM

Cyberspace, a manifestation of globalisation and the digital revolution, poses many legal challenges. One of the most obvious motivating factors is the desire to benefit from the profits of the e-commerce business. In particular, business owners and service providers have engaged in efforts to expand their businesses, increase their profits, and find more markets and customers for their products and services. They are expected to set up websites as a gateway to their virtual shops in cyberspace. In order to do so, they must have an appropriate domain name, often derived from a trademark, trade name, or service mark. However, when they try to register their domain names, they fail because someone has already registered them. As a result, the conflict between domain name owners and trademark holders becomes inevitable. This situation begs the question of when this conflict happened. And why? Answering these questions depends on determining the mechanism of this conflict on the one hand and the reasons that led to the conflict on the other. This chapter clarifies the causes of this conflict between trademark holders and domain name owners.

Chapter one focuses on the role of registry agencies, while chapter two focuseson cybersquatting and reverse domain hijacking phenomena. The domain name registration system is discussed in the third chapter. Finally, the domain name economy is investigated in the fourth chapter.

Chapter 1: The role of registry agencies in generating conflicts between domain name owners and trademark holders

Domain name registration agencies are considered highly controversial. One of the main questions is to what extent these agencies have ignited the conflict between trademark holders and domain name owners. To answer this question, we need to search for the roots of this conflict.

The causes of the conflict can be divided into two main types: those of a material nature and those of a legal nature. The latter type is explained in detail in the second chapter.

Material reasons highly contributed to this conflict. They are presented by the competition of companies and the failure of registration institutions to effectively control the domain name registration process for such companies and benefit from their value and the emergence of cybersquatting (Subchapter 1.). Besides that, the author examines another leading group of material reasons for the poor management of domain names in Subchapter 2.

1. Competition over domain names

The conflict between domain name owners and trademark holders is primarily driven by the competition between big companies and major institutions to gain a foothold in cyberspace

hoping to in order to capture the profit generated by e-commerce which has begun to compete with or even outperform traditional trade. These companies and institutions spurred other parties and individuals to acquire domains because obtaining domain names is the key to e-commerce in cyberspace[317].

As the experts contend, these companies opposed the expansion of the domain names' scope to protect the value of their trademarks and to avoid having to register hundreds of these domains proactively, which may cost them more to protect the domains[318]. Those companies present the rational justification that they are being forced to pay fees to buy domain names they do not want, and similarly, they have rejected the expected massive expansion of gTLDs.[319]

For example, ICANN[320] has been involved in a costly and bitter dispute over its charter allowing new companies to sell domain names with the extensions *.org*, *.net*, and *.com*. It was a profit-generating process, and Network Solutions performed the registry and registrar functions under that contract[321]. Although such competition must theoretically lead to positive development, it has led to some serious and negative consequences. The registration institutions have lost control over their essential functions, where competition led to the neglect of responsibility by some institutions toward domain name ownership and the inability to register some domain names by other competitors, such as NSI. It is possible that such negligence was the main reason for several conflicts, such as *Sex.com vs. Network Solution*.[322] For this situation, the fundamental explanation behind this contention was the carelessness of Network Solution, which changed the registration of *Sex.com*'s domain from one genuine proprietor to a malicious actor after receiving a bogus message requesting they exchange that name to its new proprietor. Network solution granted the bogus request without performing any reasonable checking. The carelessness of that registration organisation resulted in substantial misfortunes for the legal proprietor of the domain name.

Interestingly enough, in the case of *Pitman Training LTD vs. PTC Oxford HD against Nominet UK Inc.*, 1997, the respondent had received an application for registration of the domain name *pitman.co.uk* from the plaintiffs who own the mark. The respondent deactivated and cancelled the domain and was reregistered by another party. The action was done in trying to restore the first registration[323]. This discrepancy was due to the Nominet institution's negligence. Instead of registering the domain name and allocating it to Pitman Training Ltd.,

---

317 Savas Cetinkaya the importance of domain name in ecommerce business, on 26 October 2014, http://www.shopio.com/ blog/ the-importance-of-domain-name-in-ecommerce-business/

318 Deborah E. Bouchoux, Intellectual Property: The Law of Trademarks, Copyrights, Patents, and Trade Secrets, Publisher Cengage Learning, 2012, edition 4, p147.

319 ibid, p147.

320 Internet Corporation for Assigned Names and Numbers.

321 Roger L. Freeman, Reference manual for telecommunications engineering, Volume 2, Edition3, Publisher Wiley, 2002,p 2701
- Publish magazine. - Volume 14, Issues 7-12 - Page 20.

322 network Solutions - the Internet's biggest domain name registrar and the owner of the .com domain - has heralded the end of the Internet in court filings to the Californian Supreme Court.
It warns that if a forthcoming decision by the court goes the wrong way it "would cripple the Internet and jeopardize the national economic benefit for e-commerce". It would also "threaten all Internet registrars' survival".
The astonishing revelations feature in a 14-page submission sent to the Supreme Court on 23 January and regard the on-going legal dispute with Gary Kremen, owner of the domain Sex.com.

323 Pitman Training Ltd and Another v Nominet UK and Another: ChD 22 May 1997, https://swarb.co.uk/pitman-training-ltd-and-another-v-nominet-uk-and-another-chd-22-may-1997.

Pear Son Professional retained it instead of the natural and legal owner.[324] The Royal Courts of Justice justified returning the name to the Pitman company. The Nominet agency allocates domain names based on the first-come, first-served principle. [325] Nominet repeated the same mistake in the case *Spirit Vs. MCI*; Nominet registered the domain name *mci.com* for Spirit rather than MCI. [326] Similarly in *Al Jazeera Vs. John William*, Network Solutions was tricked quickly into allowing John William (Racine, Wisconsin, USA) to manage the *Aljazeera.net* domain, where Al Jazeera kept a makeup domain and email service[327]. William confessed to FBI representatives that he had called Network Solutions by telephone and sent an email to acquire control of the *Aljazeera.net* domain. He ultimately produced a falsified photo ID card to pose as an Al Jazeera systems manager.[328]

Suffice it to say, the registration establishments have fallen short when it comes to remedying their errors,typically due to their poor management or lack of technological ability. Since no authorised party can compel these establishments to raise their standards, some suggest the primary factor exists in these establishments' privacy, and they still enjoy immunity against lawful procedures.[329] This immunity was affirmed in 2012 in the conflict between a Malaysian national oil company and *gooddady.com*, the official domain registrar. It has been found immune from liability for the responsibility of trademark rights violation[330.]

Garry Kremen filed a claim for damages against Michael Cohen and Network Solutions Inc. for $65 million[331], besides requesting the return of the domain name.[332] The created letter deceived the registrar by designating Kremen's domain rights, sex.com,[333] to Cohen.[334] The Court raised the issue as to whether domain-name registrants have property rights in their intangible domain names. When Network Solutions took control over the *sex.com* domain, Kerman claimed ownership in 1994, intending to resell it to Cohen at a profit. According to the Court, "registering a domain name is equivalent to staking a claim on a piece of land."[335]

---

[324] *Lillian Edwards and Charlotte Waelde, Law and the Internet Regulating Cyber Space, ,ibid, p 84.*

[325] *Charlotte Waelde, Is the Dam about to Burst? An Analysis of domain Name Disputes in the UK, Journal of Information Law & Technology.1997. p3.*

[326] *Kumor, D. Kelly, Trademark: Intellectual Property Protection on The Information Super High Way, European Intellectual property Review, p 482.*

[327] *Richard Gisele, Digital Underworld, Publisher Lulu.com, 2005,p 180.*
- Robert W. Taylor, Digital Crime and Digital Terrorism, the University of Michigan, Publisher Pearson/Prentice Hall, 2006,p40.
- Athina Karatzogianni, The Politics of Cyberconflict, Publisher Routledge, 2006, p208 & 209

[328] *Richard Gissel, Digital Underworld, ipid, p180.*

[329] *Jane K. Winn, Benjamin Wright, The Law of Electronic Commerce,4th edition, walters cluwers, new York, 2019 , p 11-35*

[330] *Ibid p 11-35*

[331] *The CPA Journal - Volume 78 , Publisher New York State Society of Certified Public Accountants, 2008 Page 63.*
- Roger Bernhardt , Joyce D. Palomar, Patrick A. Randolph, Property: Cases and Statutes, Publisher Carolina Academic Press, 2005, p35.
- cyberspace Lawyer - Volume 11, Publisher Glasser Legal works, 2006, Page 61.
- Jonathan D. Hart, Web Law: A Field Guide to Internet Publishing, Publisher Bradford Publishing Company, 2004, iPage62
- Richard Allen Epstein, Cases and Materials on Torts, Publisher Aspen Publishers, 2004, p 580

[332] *Jonathan D. Hart, Internet Law, a Field Guide, Publisher BNA Books, 2008 ,p 839*

[333] *Brandweek - Volume 41, Issues 23-26 - Page 41.*
- Jonathan D. Hart, Web Law: A Field Guide to Internet , ibid, P62

[334] *Michael L. Rustad, Punitive Damages in cyberspace: Where in the World is the Consumer? Chapman Law Review , the University of California , Volumes 7-9 ,Publisher Chapman University School of Law, 2004, P 61.*

[335] *D. Benjamin Barros, Anna P. Hemingway, Property Law ,Publisher Wolters Kluwer Law & Business, , 2015 p981*
Roger Bernhardt, Joyce D. Palomar, Patrick A. Randolph, Property: Cases and Statutes, ibid ,p36.
- Jentz, Toby Miller Case Printouts; Bus Law Today Publisher ,Cengage South-Western, 2005 p235..

To name a few cases, on May 4, 2002: The domain registrar *VeriSign* exposed the weak fabric of Internet society by wrongly moving a New York author's domain name to another person who lived in Germany.[336] The issue lay with the firm's insistence on the traditional way of checking, based on published and faxed records, instead of web-based password-protected entries to registrant details that many other registrars use.

Hoever, many clients' criticisms and extensive rumours of workers' dismissal at the world's largest registrar on April 26, 2002, suggested an even bigger problem for the executives. On May 13, 2002 the web domain's seller VeriSign Inc was subjected to a complaint submitted by a competitor that charged VeriSign with utilizing incorrect marketing to take clients. On May 13, 2002, *Bulk Register*, the fourth biggest domain name registrar, submitted a legal claim versus *VeriSign* at the Court of the Area of Maryland. In March 2002, 'Verisign' apparently sent out a misleading domain name registration statement.This was described as part of advertising and marketing project that allegedly constitutedparticipation in unfair competition by 'domain name expiry notifications.' Participants of the ISP-DNS checklist stated on May 9, 2002, that seemingly benign VeriSign 'billings' might be efforts to take service from a rival and amount to email fraudulence, a crime. On July 20, 2001, VeriSign was implicated in taking consumers from micro-companies, apparently revealing its strategies to enrol telephone numbers.

2. Bad management of domain names by formal registrar's institutions

The stalemate and overall lack of development in the operation of these registrar institutions not only endanger their credibility, butalso form a concern for trademark holders and domain name owners alike. Furthermore, mismanagement is evident in many different issues.. A good example is the policies implemented by Nominet and other institutions regarding the allocation of domain names. They reflect the previous lax conventions that revolve around this area, showing that they do not consider the previous difficulties encountered by other institutions, such as NSI, which engaged in the confrontation over domain name ownership with trademark holders.[337] It also led to comprehensive conflicts over domain name ownership[338].

The second issue which endangered the credibility of registrar institutions is non-impartiality. The primary objection towards these establishments is theirlack of impartiality and integrity, which catalysed the conflict between the domain name owners and trademark holders.[339] However, non-impartiality is manifested in several aspects, such as distributing domain names' property outside the scope of applicable laws.[340] Another aspect is to allow third parties to register domain names. For example, the Internic Foundation allowed third parties to register specific domain names.[341] In this regard, dual-function performance can be

---

[336] *Scott Granneman, Why You Should Never Use Network Solutions, on https://www.granneman.com/ webdev /domains/neveruseverisignnetworksol*

[337] *Malr Gould, an Island on the Net: domain Naming and English Law, John Marshal Journal Comp & Info, V 15, Issue 3, 1997, P 493.*

[338] *Ibid, P 493.*

[339] *Christopher Lee, The Development of Arbitron, Richmond Journal Law & The technology, V7, Issue 1, 2000*

[340] *Victor Arcri, domain Name vs. Trade Mark Disputes, Archive Search Service.*

[341] *Lillian Edwards And Charlotte Waelde, Law and The Internet Regulating Cyber Space, ibid , P 50.*

considered a clue for non-impartiality. For example, NSI was performing two functions at one level, managing the registry office on the one hand and competing with other companies as a registrar.[342] In the related frame of reference of international domination of VeriSign, it was reported that the mentioned agency had been accused of 'infringing on China's sovereignty' by establishing its technical standards for Chinese domain names.[343] The predilection to one party at the expense of the other is a clear sign of non-impartiality, whether by negative or positive activity. Its sluggish feedback presented such activities to demands for assistance or suggestions offered, where the response was constantly sluggish, adverse, and inefficient. Nonetheless, this is clear regarding the Harrods case, where the firm battled a one-year battle to restore the domain. Harrods' company demand was met with a chilly response by a domain name service company about the application sent to it connecting to the support of that firm in recovering its domain name. Ultimaately, there was a consent judgment in favour of Harrods [344] .

[342] *Christopher Lee, the Development of Arbitron, Richmond Journal Law & Technology, Op: Cit, V7, Iss 1, 2000*

[343] *Birgit Zinzius, Doing Business in the New China: A Handbook and Guide, Publisher Greenwood Publishing Group, USA, 1st edition, 2004, p10.*
- Monika Ermert and Christopher R. Hughes What's in a name? China and the domain name system, originally published in Hughes C R and Wacker G, China and the internet: politics of the digital leap forward. London, UK: Routledge, 2003, pp. 127-138.: http://eprints.lse.ac.uk/9641.

[344] *Rupert Kendrick ,Cyber Risks for Business Professionals: A Management Guide, Publisher IT Governance Ltd,UK, 1st edetion,2010, p217.*

Chapter 2: Cybersquatting and reverse domain hijacking phenomena

The relationship between the leading digital community's stakeholders (domain name owners and trademark holders) has often been described as unstable and conflicting over brands' potential interests, profits, and commercial reputations. In the early digital revolution, the Internet was a double edge sword on both sides of commercial and legal technical aspects. In this regard, the author tries to illustrate the essence of these phenomena and clarify how they would impact the domain names conflict in cyberspace.

1. Domain names Cybersquatting institutions

Because domain names and domain name cyber equations play an important role in the online world and trademark, it is essential to shedding light on the same institution that governs these issues. For this purpose, WIPO's Advisory Committee on Enforcement (ACE) offers technical support and coordinates with other companies and the economic sector to fight counterfeiting and piracy activities; offers public education; supports the execution of national and local training programs; and promotes the exchange of details on enforcement concerns. A WIPO Judicial Institute was developed in 2018 to support the administration of IP in alignment with member states' national legal traditions.[345] The WIPO Judicial Institute cooperates with all appropriate WIPO sectors to coordinate a cohesive and structured technique. This work is assisted by a Board of Advisors of Judges, which contains broad geographical and subject-matter representation[346]. Besides these institutions, ADR between private parties is supported by the WIPO Arbitration and Mediation Center (hereinafter the Center).

As of 2021, the Center follows the instant resolution of conflicts between conflicting parties. Domain Name Dispute Resolution Service is another institution focused on fixing disputes over cybersquatting, i.e., the aggressive registration of another trademark in a web domain. In 2020, WIPO notified a significant current boost in cybersquatting, emerging from an augmentation of online activity given the beginning of the COVID-19 pandemic. The service is supplied following the Uniform Domain Name Dispute Resolution Policy (UDRP) that was, on WIPO's suggestion, adopted by "the Web Corporation for Assigned Names and Numbers" ICANN in October 1999. Cumulatively, throughout 2000-20, more than 50,000 UDRP cases relating to some 90,000 separate domains were issued by WIPO under UDRP treatments. WIPO releases an online Legal Index of WIPO UDRP Panel Choices and keeps an online database of cybersquatting claims. The Center also arranges workshops and helps create WIPO design agreement stipulations and industry-specific resolution schemes[347].

---

[345] *WIPO, Report of the Director General to the 2020 WIPO Assemblies: Retrospective 2008-2020 Volume 1050 of WIPO Publication, WIPO, 2020,P96.*

[346] *World Intellectual Property Organization, Report of the Director General to the 2019 WIPO Assemblies, WIPO, 2019,p22. Volume 1050 of WIPO Publication, 9789280530650.*

[347] *Zorzeta Bakaki, Sarah P. Lockhart. , Jeannette Money ,Kate O' Neill ,Preslava Stoeva, Joanne Yao The Europa Directory of International Organizations 2021, Routledge, Jul 28, 2021 ., Europa Publications, Routledge, 2021, 9781000427912*

2. The emergence of cybersquatting

The nature of domain name cybersquatting is a crucial issue in cyberspace. Knowing the legal nature of domain names' cybersquatting would help us to deal with these phenomena in the best way as long as we can present a long-term guarantee to the cyberspace community and stakeholders' rights and provide dynamic legal stability to the investment in the digital era. There is currently no consensus on the legal nature of domain name cybersquatting. This chapter offers insights into the legal nature of domain name cybersquatting to protect and recognise contested rights over domain names.

This chapter considers the illegitimacy of domain cybersquatting based upon the principle of 'first-come, first-served,' as well as based upon ACPA. With the beginning of domain name registration earlier, the stakeholders were unaware of any legal challenges, either registration agenesis or domain trademark holders. Bearing in mind that the registrations are based on the first-come, first-served principle, it was an excellent motivation to open the door to everyone equally to have the right to register any domain name. This principle paved the way for cybersquatting to register domain names that contain someone else's trademark. Furthermore, according to this principle, domain name cybersquatting became a legitimate process and reduced the protection given to trademark holders.

3. The legal nature of domain name cybersquatting

One of the most common and frequent causes of domain name conflict is the emergence of cybersquatting, and most claims of disputes are prosecuted based on it.[348] The expanding significance of the web has turned it into an effective device for companies to advertise, promote, and market services and products. Regrettably, cybersquatting, the result of unethical and illegal conduct, has also proliferated.[349] Accordingly, essential aspects related to domain name cybersquatting might help understand its legal nature. The colossal technical and legal contrasts have created a profound gap between the conflicted parties over disputed rights.[350] This gap has been incarnated in unique legal challenges, providing a headachefor legislators and legal entities. With the absence of legal organizing rules, the main obstacles relate to a lack of clarity in the legal nature of domain name cybersquatting.

3.1 First-come, first-served: Legitimizing of cybersquatting

The first-come, first-served principle is the only tool to exclusively use the domain name and related trademark rights in digital space.[351] The legal literature's perspective has adopted a

---

[348] *Diana Cabell, Berkman Fellow, Trademark, domain Names and Related up Issues on the Internet, Massachusetts Bar Association, 22 June 1999.*
- J. Fasthoff, Are you the master of your domain? Enforcing Trademark Rights Online through the Icann domain Name Dispute Resolution Policy & The Anti Cybersquatting Consumer Protection Actlhenry, IV, 2 May 2000, p7, note 21.
- David J. Loundy, a Primer on Trademark Law and Internet Addresses John Marshall, Journal of Computer & Info Law, 1997, p 46.
- Simon Stokes, Art and Copyright, rBloomsbury Publishing,UK, 1st edetion,2021p241.

[349] *Charan Piyush, A Survey of the Prominent Effects of Cybersquatting in India, International Journal of Information Security and Cybercrime, 2015/06/29, p48.*

[350] *This paper was published in sea journal under title*

[351] *Constance E. Bagley, Managers and the Legal Environment: Strategies for Business, Publisher Cengage Learning,9th edetion,UK&USA 2019 ,p311.*

different attitude to understanding the legal nature of cybersquatting. Two main aspects defy the legal nature of cybersquatting: one is the legal norm (first-come, first-served principle) used to register the domain name.[352] However, the domain name is obtained by applying for registration with NSI (Network Solutions Inc.)[353] which is an American-based technology company and a subsidiary of Web.com, the fourth largest .com domain name registrar with over 6.7 million registrations as of August 2018. It first operated the domain name system (DNS), the leading registrar, at an early stage of conflict over domain name-related rights.[354]
Moreover, when it approved the enrolment of the domain signed up, the registrant and NSI were bound by the enrolment contract[355] where the domain names are given out based on the sole principle for this aim: 'first-come, first-served.'[356] Due to this managerial process, the debate began between companies having long-standing trademark rights and other illegitimate parties preferring specific domain names.[357] Allowing registration of the domain on a first-come-first-served principle increases the domain's violation margin.[358] There have been examples where cybersquatters attempted to use the trademark to route website traffic to another site.[359] That trouble originates from the first-come, first-served principle.[360] However, according to this same principle, some argued that cybersquatting was not illegal, at least at the early stage of the conflicts between domain name owners and trademark holders. In this regard, WIPO concluded that the brand names and the customers who rely on the brands would encounter many dangers associated with cybersquatting.[361] Besides that, the behaviours of trademark holders have brought legitimacy to cybersquatting action by rebuying the domain names related to their trademark. It would be arguable that the registry agencies involved effectively turned this practice into a legal norm with statutory power.
Furthermore, the equation between main stakeholders (domain name owners and trademark holders) has changed with the increase in the pace of domain names registry by a third party. This has changed the behaviour of the trademark owners, who have attempted to claim special status. However, the third parties have legitimated the right in their trademarks registered as domain names, making them subject to the trade rules of supply and demand. There has been a considerable rise in "cybersquatting" entailing the brand-new TLDs.[362]
On top of that, this process helped turn domain names into valuable commodities and raised prices dramatically. For example, the domain name *Las Vegas.com* was sold in a transaction valued at about $90 million. The domain name *CarInsurance.com* was sold for $49.7 million

---

-,Poul F. Kjaer,The Law of Political Economy: Transformation in the Function of Law,ibid,P352.

[352] *Julia Hörnle, Internet Jurisdiction Law and Practice, Oxford University Press,Uk,1st Edetion, 2021, P305.*

[353] *Representing the Corporation: Strategies for Legal Counsel, Aspen Online, 1996, p151.*

[354] *Jacqueline D. Lipton, Internet domain Names, Trademarks and Free Speech, Edward Elgar Publishing, 2010, p 298.*

[355] *Computer Law Reporter, Computer Law Reporter Incorporated, 2003, Volume 38 - Page 815*

[356] *David V. Radack Understanding Some Ground Rules in Internet domain Name Disputes, in the journal JOM, 50 (1) (1998), p. 60.*

[357] *ibid, p. 60.*

[358] *Dara B. Gilwit, The Latest Cybersquatting Trend: Typosquatters, Their Changing Tactics, and How to Prevent Public Deception and Trademark Infringement, Washington University journal of law & policy vol 11, January 2003, p276*

[359] *William H. Manz, Anticybersquatting Consumer Protection Act: a legislative history of Public Law no. 106-113: appendix I, 113 Stat. 1501A-545, William S. Hein, 2002. Volume 1,*

[360] *Asper review of international business and trade law, the University of California Published 2007, Volume 7, P264*

[361] *World Intellectual Property Organization,: Guide to WIPO's services for country code top-level domain registries Item. World Intellectual Property Organization, Geneva, Switzerland ,2019 .p17.,*

[362] *Gerald M. Levine, Esq., Understanding the legal options used to fight cybersquatting Cybersquatters jeopardize your exclusive trademark rights, and there are multiple ways to fight back. January 14, 2015, ibid.*

in 2010. The enrolment system urges dishonest parties such as cybersquatters to prevent the rightful trademark from securing their own trademark by registering it as a domain name and demanding ransom to release it.[363]

3.2. First-come, first-served principle in light of trademark registration rules

While the trademark registration systems have had tremendous accumulative legal experiences for about 100 years,[364] the shallow accumulative legal experiences of domain names registration systems have participated in this massive contrast between the protection given to trademarks and the protection given to domain names incarnated in principle of first-come, first-served. One question arises whether registering a domain name does not automatically give any rights over the matching trademark. Can a person only gain this right by registering his domain? To answer this question, one needs to understand the trademark registration system.

This chapter is based on three essential axes: the principle of registration priority; the system in which registration is carried out; and the principle of non-liability, which results in unprioritized legality of domain names or whether that domain name registration has violated the trademarks holders.[365] So, how did these issues contribute to the occurrence of this conflict? The principle of registration priority is an urgent point that has great importance in this conflict. Hence, it is possible to see the correlation between the technical and legal aspects of the registration system's subject. The registration process is purely technical and cannot be dispensed with domain names because operating a website without domain names is impossible. This technical rule has become legal, reflected in the principle of registration priority, which states: 'first come, first served.' Priority of registration will still exist, and hence the problems associated with domain snatching will remain[366]. Contrary to today, the registration of domain names was formerly processed over time by the NIC agency and managed by NSI.[367] That customary rule dominated the internet community for over a decade, and the advantage was in favour of the party who first registered the domain name. This standard did not give any importance to potential stakeholders. Here, one must address the system of trademarks' registration to understand to what extent such a system would provide a margin of rights to potential stakeholders. In this regard, the trademark registration mechanism provides a fair margin to every potential stakeholder. However, different registration systems achieve the ideal goal beyond registration. Two sorts of enrolment techniques are embraced by those states that enable the enrolment of trademarks (most countries around the globe). For instance, those who have adopted the exam method and those who do not, such as France.[368] As the overwhelming majority of states use trademark

---

[363] *Dara B. Gilwit, The Latest Cybersquatting Trend: Typosquatters, Their Changing Tactics, and How to Prevent Public Deception and Trademark Infringement, ibid 276.*

[364] *Amanda Michaels, Andrew Norris, A Practical Guide to Trade Mark Law, Publisher Sweet & Maxwell, 2002, p v.*

[365] *John R. Hewitt, James B. Carlson, Securities Practice and Electronic Technology, Law Journal Press, 2019 P4-7*

[366] *aaron upcroft*trade marks as domain names: an australian perspective, 3 mac lr,p54.*

[367] *John R. Hewitt, James B. Carlson, Securities Practice and Electronic Technology, ,ibid P4-7*

[368] *Tom Blackett Trademarks, Palgrave Macmillan UK, first edition, 1998, p45*

inspection or exam systems, as mentioned above,[369] it continues to the substantive assessment, which evaluates the application of absolute and relative rules[370] if a trademark is not opposed.[371] However, the trademark is only registered if an application efficiently passes the substantive assessment.[372] Ultimately, trademark inspection systems come in one or both of the two kinds called 'absolute' or 'relative.'[373]

The absolute system decides over a questionable trademark regarding whether it is acceptable to be provided[374] [375] or refused.[376] [377] The inspection system indicates the acceptance or rejection of the trademark registration.[378] Moreover, this system will shrink the efforts, conflicts, and damages if the contested trademark is accepted to be registered. With such an examination system, conflicted domain names registered before based on the first-come, first-served principle could be easily prevented, at least at an early stage of the conflicts that emerge in cyberspace. On the other hand, absolute systems somewhat give the candidate a monopoly right in the trademark based on some criteria, e.g. descriptive, , the simple shape of the product, or a geographical area.[379] The absolute standard relates to diversity as well as specific public interest purposes.[380] Common law countries often use this system, for example, the UK, the USA, Japan, and Germany.[381]

The second type (the 'relative grounds' system) implies the reasons put down in the trademark substitute declining to register the mark by considering it in connection with other earlier trademarks.[382] It entails the trademark registries searching for their trademark signs to determine if any previous enrolments or applications already on data conflict with the mark requested.[383] The policies of trademarks distinction will differ from country to country. However, as a rule, it will entail visual, phonetical, and conceptual aspects.[384] This outcome is taken for granted because each country has different trademark laws and intellectual property regulations.[385] It also means that the treatments for getting a global protection vary

[369] *Stef van Gompel, Formalities in Copyright Law: An Analysis of Their History, Rationales and Possible Future, Volume 23 of Information law series, Kluwer Law International B.V, Netherlands ,2011, p39*

[370] *Ibid, p39*

[371] *Tom Blackett Trademarks ibid p46.*

[372] *Carsten Fink, Christian Helmers, Carlos Ponce, Trademarks Squatters: Evidence from Chile, Volume 22 of WIPO Economic Research Working Paper, World Intellectual Property Organization,2014, p20.*

[373] *Tom Blackett, Trademarks, ibid, p46*

[374] *Ibid, p46*

[375] *Tobias Cohen Jehoram, Constantinus Johan Jozef Clemens van Nispen, Tony Huydecoper, J. L. R. A Huydecoper, European Trademark Law: Community Trademark Law and Harmonized National Trademark Law, Kluwer Law International B.V., 2010 p169*

[376] *Tobias Cohen Jehoram, Constantinus Johan Jozef Clemens van Nispen, Tony Huydecoper, J. L. R. A Huydecoper, European Trademark Law: Community Trademark Law and Harmonized National Trademark Law, Kluwer Law International B.V., 2010 p16*

[377] *9 Stef van Gompel, Formalities in Copyright Law: An Analysis of Their History, Rationales and Possible Future, ibid, p39*

[378] *Ibid p39*

[379] *Tom Blackett Trademarks, ibid, p46.*

[380] *BPP Learning Media, Business Essentials: Company and Commercial Law, BPP Learning Media, Uk, 2nd edition 2010, p220.*

[381] *Tom Blackett Trademarks, ibid, p46.*

[382] *, Intellectual Property Office of Singapore relative grounds for refusal of registration, Singapore, Version 4 (November 2015), p3*

[383] *Tom Blackett Trademarks, ibid, p46. 46*

[384] *ibid, p46.*

[385] *Jeff Fulton, Steve Fulton, The Essential Guide to Flash Games: Building Interactive Entertainment with ActionScript, Publisher A press, usa, 2010 p368.*

from country to country, which is to be expected. It is to be anticipated that the process is expensive and complicated.[386]

Regions that take on a relative assessment procedure include the Scandinavian countries and most common law states besides Spain.[387] *Per contra*, some states did not check out an application for relative grounds for rejection.[388] On 28 March 2006, the Singapore treaty on the regulation of trademarks was embraced at a diplomatic meeting held in Singapore. The treaty has streamlined the relevant processes for trademark application and made the process more practical.[389] In this regard, one of the main results has been agreed on by emphasising that changing the trademark at the start of the process is much less expensive and will have a less negative effect on the product's competitiveness than if changed later.[390] Denmark changed the relative exam system to an absolute one in 1999. Remarkably,[391] Germany adopts a definitive examination treatment and leaves it to the registered trademarks to oppose applications if they think they conflict with their existing registration(s).[392]

If the state did not make the trademarks subject to any examination, in that case, it would be known as a deposit state. Merely because the applications to register the trademarks are deposited on the trademark registers without any exam (on relative or absolute grounds) being conducted. The principle beyond this is that the registry is merely there to register trademarks, and any dispute should be solved by courts.[393] According to this system, the owner of the earliest legitimate registered trademark would typically have the privilege to avoid dealing with later filed enrolments. Some countries have adopted this system including Austria, Italy, France, and the Benelux,[394] which contains the economic union of Holland, Belgium, and Luxembourg.[395] The main question arising from this approach is whether the same method can be applied to domain names and what benefit can be gained. To answer this question, we need to evaluate the principle of domain names registered early on (first come, first served), then look at the rules legislated later on in the shape of regulations or laws.

3.3. Level of protection, granted by the first comes, first served principle

As aforementioned, the principle of first come, first served for domain name registration did not give enough protection to the potential stakeholders (especially trademark holders) from the author's point of view. By contrast the trademark registration system was structured to

---

[386] *Richard Stim, Trademark law, Publisher West Legal Studies/Thomson Learning, 2000, P193.*

[387] *Tom Blackett Trademarks, ibid, p46.*

[388] *Records of the Diplomatic Conference for the Adoption of a Revised Trademark Law Treaty - Singapore, 2006, Volume 329 of WIPO publication Singapore Publisher WIPO, Geneva ,2010 p422*

[389] *, Xianggang Zhongguo zhuan li yu shang biao za zhi she, China patents & trademarks - P 85, publusher Xianggang Zhongguo zhuan li yu shang biao za zhi she, china 2007, P 85*

[390] *Nuno Garoupa, Carlos Gómez Ligüerre, Lela Mélon, Legal Origins and the Efficiency Dilemma, Volume 24 of The Economics of Legal Relationships, Taylor & Francis, 2016, p119.*

[391] *ibid p119.*

[392] *ibid p119.*

[393] *Tom Blackett Trademarks, ibid, p46.*

[394] *Ibid p46*

[395] *Frank R. Abate, The Oxford Desk Dictionary of People and Places, Publisher Oxford University Press, 1999 p 483*
- Angus Stevenson, Oxford Dictionary of English, Publisher OUP Oxford,3rd edition, 2010, p 154.
- Els Witte, Jan Craeybeckx, Alain Meynen, Political History of Belgium: From 1830 Onwards, ASP nv (Academic and Scientific Publishers nv Brussels) ,1st edition,2009,p405.

prevent potential conflict or expected infringement as early as possible because time is essential. Besides the adverse effects on the company, trademark, and plans, it is clear that every second would cost money and effort. Even though domain name registrations are inexpensive, quick, and convenient compared to trademark registrations,[396] the domain name registration's principle does not take into consideration the practical nature of domain names which is incarnated in the fact that there cannot be more than one domain name on the web including the same trademark at the same level. The rational fact supports that every trademark holder has the right to be the domain name owner of his trademark.

Accordingly, the structure of the trademark registration system has reduced the frequency of conflicts by preventing them almost at the cradle, and before they escalate and protract. In this regard, it would be more practical if the domain name registration's agencies considered registering domain names by using the trademark database to determine who would have the right to request the domain name registration. The impossibility of domain names' duplication in cyberspace would be an advantage to make a decision less complicated than an examination of trademarks registrations because it is initially expected to register a similar trademark at the local, regional, or international level, besides considering some vital issues such as the products and the ability of trademark to distinctiveness.

Another issue related to registration and which is worthy of being discussed here is fair registrations. If there was reasonable satisfaction by the registration committee that every party has its right to register a similar trademark but with different products, and it appeared to the committee that there would not be any confusion, then both of them would be registered. On the other hand, in the domain names' case, fair registration would be given only to one person to be registered at that specific level. Accordingly, this application of the first-come, first-served principle could be crucial in offering trademark owners the right to have the corresponding domain name in light of the absence of duplication in cyberspace.

Furthermore, fair competition and market stability are vital to the digital economy. Another question arises as to whether the first-come, first-served principle has considered causality when deciding who would have the legal right to register the domain name compared with the trademark ruling system. This principle completely ignored the causation verification before granting the right to a domain name registration. It only verifies that the domain is available for registration according to the non-duplication of the domain name base. In this regard, Richard Stim indicates that when it comes to domain registration, the company or the individual must be particular that no one else is utilising it as a trademark for similar items, products, or services with a comparable name.[397] This evaluation concluded that domain name registration was limited to the availability of domain names rather than any checking out and examination of the reasonableness of the request. It ignored the trademark databases, which was one of the reasons that resulted in the conflict reaching an advanced stage. As a result, some regulations have been set out to organise domain name registration. However, the question is whether or not these regulations succeeded in limiting the severity of the conflict between domain name owners and trademark holders. Another question that could be left for discussion is whether these regulations set out the causality relationship between the

[396] *Jean L. Batman, Advising the Small Business: Forms and Advice for the Legal Practitioner, Publisher American Bar Association, 2007 p19*

[397] *Richard Stim, Patent, Copyright & Trademark: An Intellectual Property Desk Reference, Publisher Nolo, 2017, 15th edition, p397*

registrant and the domain name, bearing in mind that most domain names contain or include trademarks.

3.4. Trademark holders' behaviours

Most trademark holders believe paying the requested ransom to cybersquatters was the cheaper and more expedient because the legal action would cost them much more and take longer.[398] Before 1999, many businesses and companies did not expect domain names to play crucial roles in their businesses. These circumstances contributed to cybersquatting, and the acquiring domain names for ransom, and resale to the legal owner.[399] In this correlation, many elements related to this behaviour need attention. For instance, the effects associated with the first-come, first-served principle, and its flexibility; the absence of any legislation on cybersquatting criminalizing; unclear domain name nature; trademark owners' behaviour, causality checks between the third party; and disputed names were not being observed by registration authorities. According to the fact that the official agency registration gives credentials and legitimate rights to the registered party, the concept of cybersquatting in legal literature contradicts its essence, which should have been identified as the forcible taking of the domain name for variously dubious purposes.

In comparison, the registration given is accepted by the registration authority. In this context, it begs whether the traditional concept of cybersquatting needs to be redefined and whether the cybersquatter should be entitled to the legitimacy of having the right in that trademark as a domain name, at least in registration made before the enactment of the Anticybersquatting Act.

Table 1: Most expensive domains in the world 2022[400]

Domain names	Price	years
CarInsurance.com	: $49.7 million	2022
Insurance.com	$35.6 million	2022
VacationRentals.com	$35 million	2022
PrivateJet.com	$30.18 million	2022
Voice.com:	$30 million	2022
Internet.com	$18 million	2022

4. Reverse domain hijacking (RDNH)

When we talk about reverse domain name hijacking in the context of trademark violation in cyberspace, it is essential to understand the background of RDNH and its theoretical frame

[398] *Little Rock Law Review, University of Arkansas, School of Law, 1999, Volume 22, P64, Look, J. J. (1999). The Virtual Wild, Wild West (www): Intellectual Property Issues in cyberspace—Trademarks, Service Marks, Copyrights, and domain Names. In University of Arkansas at Little Rock Law Review (Vol. 22, Issue 1, p. 64). School of Law.*

[399] *John W. Bagby, F. William McCarty, The Legal and Regulatory Environment of E-business: Law for the Converging Economy, Publisher Thomson/South-Western/West, 2003 P 643,*

- The Michigan Bar Journal, Publisher State Bar of Michigan, 1999 Volume 78, Issues 5-12, P1261.

- University of Illinois Journal of Law, Technology & Policy, Publisher Board of Trustees of the University of Illinois, 2003, Volume 3, p460

[400] *The 10 Most Expensive Domains (2022 Update) Tuesday, August 9, 2022 https://www.get.inc/blog/most-expensive-domains*

because it cannot be separated from domain name cybersquatting. RDNH is defined as using the dispute resolution policy in "bad faith to attempt to deprive a registered domain name holder."[401] Any case of this conflict could be presented as a cybersquatting case and be subsequently identified as a reverse domain name hijacking case.

4.1 Theoretical Framework for Reverse Domain name Hijacking

The protection of domain name rights differs from the protection of trademark holder rights. The ICANN authority is responsible for solving the conflicts between domain name owners and trademark holders and was founded to protect trademark holders against cybersquatters. On the other hand, UDRP's policy was designed predominantly to deal with cybersquatters.
One of the main facts related to this issue is that the trademark holder should always have the right to register any domain names that might look similar to his trademark. On this line, there is another fact that should be taken into consideration. The number of reverse domain names hijacked reflects that UDRP rules have failed to provide legal domain name owners the complete protection they deserve. The small number of approved reverse domain name hijacking cases indicates many more that have rather been approved cybersquatting cases. Vice versa, if there are many approved cybersquatting cases, the indication is that many reverse domain hijacking cases have been disapproved. The crucial issue that can be concluded is that the disapproved reverse domain name hijackings against trademark holders turn the case into an approved cybersquatting case against a legal domain owner.

4.2 Mechanism of Reverse domain name hijacking

Disputes arise over the domain name rights on traditional trademark principles.[402] These rights can be compromised;[403] The mechanism of reverse domain hijacking is presented by enrolment trademark as a domain name or even using it in bad faith.[404] The trademark's owners unequivocally exercise reverse domain name hijacking by taking advantage of their commercial rights to seize domain names from legitimate owners.[405] The Anticybersquatting Consumer Protection Act explains this mechanism by considering registering, trafficking in, or using a website domain name with bad faith intent to profit from the goodwill of a trademark belonging to someone else.[406]

---

[401] *Dowie-Whybrow, Margaret. Core Statutes on Intellectual Property 2022-23. United Kingdom: Bloomsbury Publishing, 2022,p546*

[402] *Journal of Legal Studies in Business - Volume 6, Publisher West Publishing Company, 1999, Page 110*

[403] *Emily Hurtt, What's in a Name? The Rights to domain Names Under Various Principles,ibid, p840.*

[404] *David Lindsay, International domain Name Law: ICANN and the UDRP, ibid p96.*
- BNA's Banking Report - Volume 74 ,2000, Page 896.

[405] *What's in a Name: Reverse domain Name Hijacking and Cybersquatting, https://hutchersonlaw.com/reverse-domain-name-hijacking-cybersquatting/*

[406] *the United States federal law known as Anticybersquatting Consumer Protection Act (ACPA), 15 U.S.C. § 1125(d), is a U.S. law enacted in 1999 that established a cause of action for registering, trafficking in, or using a domain name confusingly similar to, or dilutive of, a trademark or personal name.*

4.2.1 Reverse domain name hijacking under UDRP rules

The UDRP rules specified a reverse domain hijacking name in a bad faith complaint[407] which infringed on UDRP policy. It similarly makes a reason to act for RDNH against the legal owners of trademarks who misappropriate or misuse their lawful rights.[408] It turns out to be hard to identify what constitutes an objective 'bad faith,' often leading to the actual contradictions of the parties as undetermined or intangible at best. Therefore, despite its explicit acknowledgment of the UDRP rules, the discovery of domain name hijacking is rare[409] because RDNH is instituted only in extraordinary situations where the trademark holder can make it.[410]

4.2.2. Bad faith criteria

Bad faith criteria[411] are inherently controversial and difficult to approve. Proving 'bad faith' is complicated because it involves proving something in the decision-maker's mind,[412] and it is impossible to anticipate all the possible fact patterns related to bad faith.[413] It is difficult in all cases but especially difficult in two respects: first, the decision is often set within legal limits. Second, it is always easy for a dishonest decision-maker to provide reasonable justification for his illegal decision.[414] Although the domain name owner is considered acting in bad faith when registering another well-known trademark for commercial purposes,[415] NSI placed the burden on the applicant to act in good faith in requesting the domain name.[416] The UDPR policy stipulated three substantive matters of reverse domain name hijacking. The first is that the contested domain name is similar or confusingly comparable to the mark. [417] The second one is that the domain name registrant has no legal rights or interest in the questionable domain. The last is that the 'domain name' has been enrolled and used in bad

---

[407] *the UDRP Policy Rules Paragraph 15 (e)*

[408] *Adam V. Floyd, O'Connor's Federal Intellectual Property Codes Plus, Jones McClure Pub., 2007, p 60*

[409] *American Bar Association. Section of Public Utility, Communications, and Transportation Law, Annual Report, Publisher American Bar Association Section of Public Utility, Communications and Transportation Law, 2003, p201*

[410] *Ibid*

- United Nations Conference on Trade and Development, E-Commerce and Development Report 2002, p44.

[411] *Raymond S. R. Ku, cyberspace Law: Cases and Materials, Wolters Kluwer Law & Business, 2016, p290-291*

- David Lindsay, International domain Name Law: ICANN and the UDR, ibid, p161.

- Peter Luther & Alan Moran, Technology in America, Macmillan International Higher Education, 2018, p533.

- Vakul Sharma, Information Technology Law and Practice, Universal Law Publishing, 2011, p 531.

- Margaret Jane Radin, John A. Rothchild, Gregory M. Silverman, Intellectual Property and the Internet: Cases and Materials, Foundation Press, 2004, p180.

- J. Thomas McCarthy, Roger E. Schechter, David J. Franklyn, McCarthy's Desk Encyclopedia of Intellectual Property, the University of Michigan, Publisher Bureau of National Affairs, 2004, p523.

- Harold C. Wegner, Edward G. Poplawski, Understanding the new patent law: how the changes affect your patent practice and portfolio, Publisher Practicing Law Institute, 2000, p100.

- Anthony Connerty, A Manual of International Dispute Resolution, Publisher Commonwealth Secretariat, 2006, p320.

- Steve Hedley, Tanya Frances Aplin, Blackstone's Statutes [on] IT & E-commerce, Edition 2, Oxford University Press, 2004, p333.

- Practicing Law Institute. Advanced Seminar on Trademark Law, Publisher Practicing Law Institute, 2002, p 900.

[412] *Christopher Enright, Federal Administrative Law, Federation Press, 2001, p393.*

[413] *David E. PozenConstitutional Bad Faith, 2016, ibid pp. 885-955*

[414] *Christopher Enright, Federal Administrative Lawibid, p393.*

[415] *Graham Earnshaw, China Economic Review's China Business Guide 2005, Publisher SinoMedia (Holdings) Co. Ltd., p577.*

[416] *Michael D. Scott, Scott on Multimedia Law, Aspen Publishers Online, 2008, p 5-48*

[417] *United Nations Conference on Trade and Development, E-Commerce and Development Report 2002, p43.*

- Jenny Ng, The domain Name Registration System: Liberalization, Consumer Protection, and Growth, Publisher Routledge, 2013, p43

faith.[418] Suppose the complainant verifies that the enrolment was in bad faith. The respondent must also confirm that the domain name has been registered in good faith. In the case of *DIGIT minimal obligation business v. Privacy Administrator, Anonymize, Inc/ Michele Dinoia, Macrosten L.T.D.,* the administrative panel of the WIPO arbitration and mediation center declared that the plaintiff is requested to bring the convincing proof related to the contested domain name that it is confusingly similar to the 'service mark' or trademark in which the plaintiff has a legal interest. Besides, he must prove that another party (defendant) has no legal rights or legitimate profit relating to the contested domain name and that it has been signed up and is being used in bad faith.[419]

ICANN has identified the initiatives to extract repayments utilising the domain as examples of bad faith. Moreover, ICANN has gone beyond the enrolment itself, considering whether it aimed to stop the owner from utilising his trademark as a domain name. Furthermore, ICANN considered whether enrolment evidence was an element of an initiative to disrupt the mark proprietor's business, besides the evidence that the domain was operated to divert commercial internet website traffic from the mark owner.[420]

One factor to be considered is whether there is bad faith in the extent to which a trademark is used commercially before registering or using a domain name.[421] As mentioned above, showing evidence of bad faith is rarely straightforward. For instance, Lady Gaga initiated an arbitration procedure against an unauthorised user of the domain name www.ladygaga.org. Her claim was unsuccessful, although the website involved in that case was a fan site promoting Lady Gaga. The national arbitration forum involved in this dispute decided that using the domain was confusing. There was no legitimate right or interest on the domain name user's side; however, this particular use as a fan site promoting Lady Gaga had not been proven to constitute bad faith.[422]

Supposing that, after considering the submission situations and conditions, the WIPO arbitration and mediation center panel discovers that the complaint acted in bad faith, for instance, to bring a criminal RDNH case or was attended mainly to disturb the domain name owner. In a situation like that, the panel will declare in its verdict that the claim was generated in bad faith and also constitutes abuse of the administrative policy and procedures.[423] In the case of *Digit Limited Liability Company v. Privacy Administrator, Anonymize, Inc Michele Dinoia, Macrosten L.T.D.*[424], after attempting to use UDRP rules illegally to seize the *digiti.com* domain name, the panel decided that the company headquarters in Belgium was guilty of RDNH, even though the trademark to which the contested domain name had been entirely similar was established only in 2018, after 16 years of the domain name being enrolled. Furthermore, the Arbitration and Mediation Center of WIPO favoured the complainant's decision to transfer the contested domain name, *parvi.org,*

---

[418] *Ibid p43*

[419] *DIGITI limited liability company v. Privacy Administrator, Anonymize, Inc / Michele Dinoia, Macrosten LTD Case No. D2018-2148, November 15, 2018*

[420] *Delta & Matsuura, Law of the Internet, 4th Edition, Volume 1, Publisher, Wolters Kluwer Law & Business, ibid 2016 Page 12-38*

[421] *ibid, p 12-38*

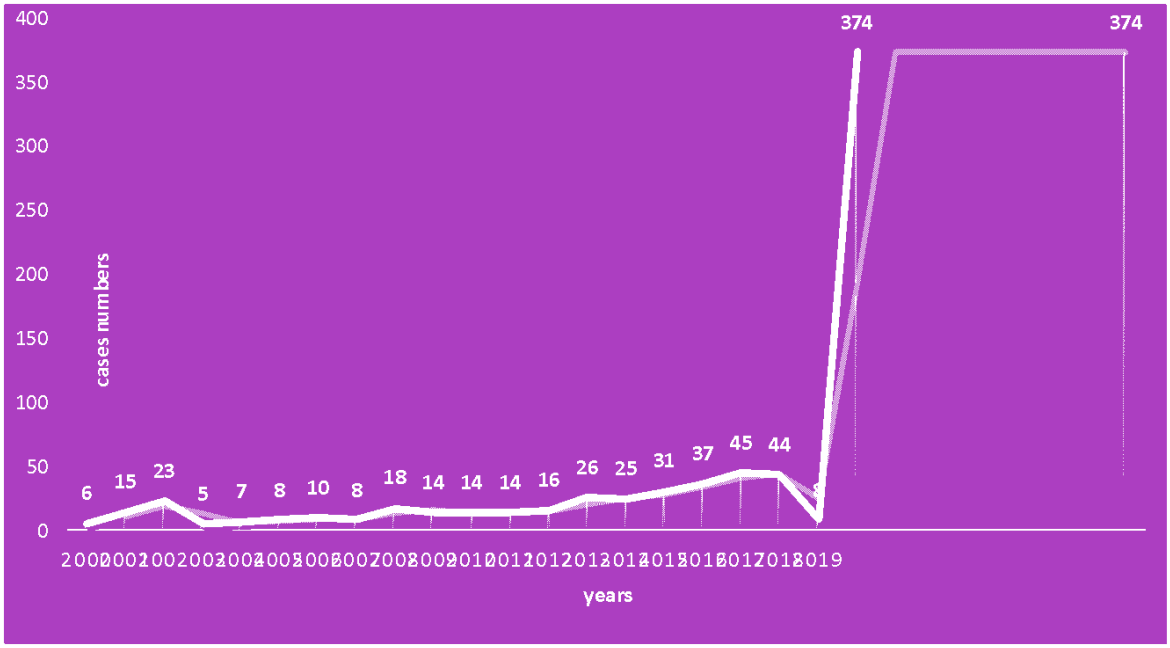
[422] *, ibid, p 12-34*

[423] *section 15(e) of the Rules for Uniform domain Name Dispute Resolution Policy.*

[424] *Case Number: D2018-2148, https://www.wipo.int/amc/es/domains/search/text.jsp?case=D2018-2148*

to him.[425] The WIPO committee noted that the domain had been registered for over sixteen years before initiating the trademark. Additionally, such behaviour consisted of the RDNH ruling. The panel mentioned: 'The complainant seems to have assumed that because it has a registered trademark identical to the disputed domain name, and the disputed domain name was linked to a P.P.C. webpage, it could file the briefest of complaints without any further supporting detail or useful information.'

Figure 5: RDNH cases 2000- 2019 source RDNH website 2019



4.2.3. ACPA rules on Reverse domain name hijacking

Before the ACPA, no law specifically made such behaviour illegal[426] . However, trademark and domain name conflicts are among the oldest legal arguments on the Internet.[427] The ACPA is considered a natural extension to Lanham Law, codified by the current common law of trademarks.[428] The Anticybersquatting Consumer Protection Act does not exclusively identify reverse domain name hijacking. It frequently only restricts defendants' recovery to recognition or transference of the domain name.

Furthermore, it failed to treat attempts to reverse cybersquatting targets.[429] Nonetheless, the law allows monetary relief where a breach of contract, careless neglect, or a subpoena's willful infraction is included. Meanwhile, it makes a reason for reverse domain hijacking versus trademark owners who abuse or violate their legal rights.[430] The ACPA[431] prohibits

---

[425] *Ville de Paris v. Jeff Walter, Case No. D2009-1278, WIPO Arbitration and Mediation Center, administrative panel decision, November 19, 2009, https://www.wipo.int/amc/en/domains/decisions/html/2009/d2009-1278.html*

[426] *Computer Buyer's Guide and Handbook, University of Minnesota, Volume 20 Computer Information Pub., 200 Publisher Computer Information Pub., 2001 1, University of Minnesota, Page 96*

[427] *Ibid, p96.*

[428] *Emily Hurtt, What's in a Name? The Rights to domain Names Under Various Principles, University of Cincinnati Law Review December 1, 2017 p843*

[429] *Computer Law Reporter - Volume 38, Publisher Computer Law Reporter Incorporated, 2003, Page 824*

[430] *Adam V. Floyd, O'Connor's Federal Intellectual Property Codes Plus, ibid, p 60.*

'cybersquatting' or other forms of domain name speculation. Some strongly believe that cybersquatting differs from joint trademark infringement, considering that cybersquatters do not utilise the domain to sell products and services. The reason for cybersquatting is to draw out remittance from the proprietors of trademarks.[432] In bad faith, the cybersquatters seek to enrol domain names to extract benefits from trademark holders.[433] Generally, courts can enforce the rights of trademark owners if they prove that the domain name confuses consumers between the services or items and other peers' registrar or the relationship between the entities.[434] In this regard, the question arises whether the rights of domain names should be considered primarily as part of a property[435] or whether they can be considered a contract,[436] as we already discussed above. This question has opened the floodgates to a controversial and heated debate on the lawful nature of domain names and the best way to solve any related conflicts. Under the ACPA, it is a crime to register a domain name that is confusingly similar to the trademark or personal name or to register a well-known trademark as a domain name based on a desire to sell it to the trademark holder. The ACPA prohibits these kinds of extortionist behaviours, including cybersquatting. However, principles of concepts of intellectual property rule will examine whether the actions constitute cybersquatting rather than considering it as simply a violation of the contract act.

On the other hand, in light of contract law principles, registering a domain name creates a contract right, not a property right. Like for any other contract, it must be entered in good faith. Considering this fundamental contract principle, when an individual renews a domain name registration to keep that particular domain name for himself and, therefore, unavailable to anyone else, the individual's actions fall within the purview of the extortionist behaviour ACPA was drafted to prohibit. The discussion will then[437] dissect each approach to conclude that, in light of the intent to prevent extortion and unfair business practices apparent from the ACPA, the third and eleventh district circles of American Courts correctly interpreted rights to domain names under principles of contract law.[438] Some legal experts still suggest that the most extensive domain registrar has seemed to yield that the domain is not contracting services but intangible property[439] .

---

[431] *the ACPA is an extension of the Lanham Act which was passed by Congress in 1946, and codified the existing common law of trademarks.*

[432] *Lee A. Bygrave, Jon Bing, Internet Governance: Infrastructure and Institutions, ibid, p82*

[433] *Richard A. Spinello, A Defense of Intellectual Property Right Edward Elgar Publishing, 2009, p11,*

[434] *National Center for Preventive Law (US), Preventive Law Reporter, Publisher Butterworth Legal Publishers, 1999Volume 18, Page 62*

[435] *Gerald B. Halt, Jr., John C. Donch, J., Amber R. Stiles, Intellectual Property in Consumer Electronics, Software and Technology Startups, Publisher Springer Science & Business Media, 2013, p61.*
- John G. Sprankling, The International Law of Property, Ibid,p90.
- Konstantinos Komaitis, The Current State of domain Name Regulation: domain Names as Second-Class Citizens in a Mark-Dominated World, ibid, p58.
- Journal of intellectual property law - Volume 11, the University of California,2003, Page 128.

[436] *Kentucky Law Journal - Volume 99, Issues 1-2, Publisher University of Kentucky, College of Law, 2010 Page 192.*
- Konstantinos Komaitis, The Current State of domain Name Regulation: domain Names as Second-Class Citizens in a Mark-Dominated World, , ibid, p92.

[437] *Emily Hurtt, What's in a Name? The Rights to domain Names Under Various Principles, ibid, p840.*

[438] *Ibid p841*

[439] *Right Xuan-Thao N. Nguyen Jeffrey A. Maine, Taxing the New Intellectual Property Right, Hastings Law Journal - Volume 56, Issues 1-3, Hastings College of Law, 2005, Page 41*

4.2.4. Compensation for damages

Procedures were proposed through WIPO to resolve domain name conflicts. The existing judicatory system and the development of an adaptive technicality for settling disputes were considered appropriate remedies that took many years to prevent reverse domain hijacking.[440] However, ICANN's guidelines did not perform an attempt to resolve issues that certainly do not concern a bad-faith domain name owner.[441] The UDRP rules are confined to situations of "bad faith" registration or usage[442] , bearing in mind that UDRP rules still, until now, have no real devices to penalise abuses such as RRDNH. This finding may be used in a regional jurisdiction where such misuses might shape a tort, including tortious interference and unfair competition practices. A domain registrant whose domain has been put on hold, impaired, or moved under a guideline defined under UDRP rules might, upon note to the proprietor, submit a civil claim based on the fact that the enrolment or even use of the domain name through such registrant is certainly not wrongful under this act.

Moreover, it might be considered unfair competition and deserve compensation.[443] Courts may also grant judicial compensation to the domain name's registrar, including reactivating the domain name or transferring the domain name to the domain name registrar.[444] By analysing the Lanham Act 15 U.S.C. § 1117(d), we can find further protection related to statutory damages. *It has mentioned within issues 'involving a violation of section 1125,' an election of damages in the court's discretion of 'not less than $1,000 and not more than $100,000 per domain name'.*[445] This was a quantum leap allowing the plaintiff to claim compensation for statutory damages of up to $100,000 per domain name instead of actual damage[446] in some cases, based on this law. It is a rational step given the difficulty of proving that the violator can trigger sufficient damage to make the federal suit applicable.[447]

---

[440] *Zheng Qin, Introduction to E-commerce, Springer Science & Business Media, 2010, P 186*

[441] *Luke A. Walker, ICANN's uniform domain name dispute Resolution policy Berkeley Technology Law Journal - Volume 15, Publisher University of California Press, 2000, Page 310*

[442] *United Nations Conference on Trade and Development, E-Commerce and Development Report 2002, p43.*

[443] *Zhou lin, China Court Cases on Intellectual Property Rights, ibid,, p 323.*

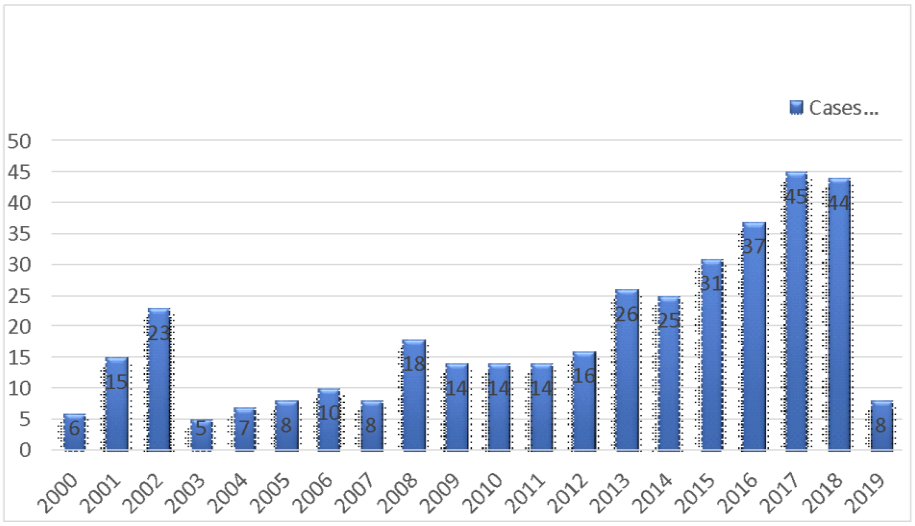
[444] *EC-Council, Computer Forensics: Investigating Network Intrusions and Cyber Crime, Publisher Cengage Learning, 2009, p 9-4.*
- United States Code, 2006, V. 8, Title 15, Commerce and Trade, Sections 80a-1 to End, p596.
- Congressional Record, V. 145, Pt. 21, November 17, 1999 to December 3, 1999, Publisher Government Printing Office, p30501.
- Rachel Gader-Shafran, MA, jd, llm, the trademark law dictionary, Publisher iUniverse, 2013, p218.
- Carol Chadirjian, The Business of Trademarks: A Practical Guide to Trademark Management for Attorneys and Paralegals, Publisher Universal-Publishers, 2018, p134.
- Thomas Hoeren, Jochen Stauder, International Sources of Electronic Commerce Regulation, Publisher Lit, 2001, p281.
- United States Code Service - Volume 15 Publisher LexisNexis, Page 5

[445] *Lanham act at 15 U.S.C. § 1117(d)*

[446] *Roman L. Weil, Peter B. Frank, Michael J. Wagner, Litigation Services Handbook: The Role of the Financial Expert, Publisher John Wiley & Sons, 2002, p21-10.*
- Jeffery Handelman , Guide to TTAB Practice, Publisher Aspen Publishers Online, 2007, p A-44.
- Mark A. Glick, Lara A. Reymann, Richard Hoffman, Intellectual Property Damages: Guidelines and Analysis, Publisher John Wiley & Sons, 2002, p457

[447] *Travis Crabtree, City of Paris ordered to pay for reverse domain name hijacking in groundbreaking decision, on web cite https://www.emedialaw.com/city-of-paris-ordered-to-pay-for-reverse-domain-name-hijacking-in-groundbreaking-decision/*

Figure 6: RDNH cases, the years 2017 & 2018 show the increase of approved reverse domain name hijacking cases compared to previous years. The total number of RDNH cases is about 374 from 2000- to 2019. Source: RDNHwebsite cases, the years 2017 & 2018.



5. Effects of Reverse domain hijacking

Neither the ACPA nor the UDRP rules offer much immunity to prevent trademark holders' misuse of their rights, and to thus reduce RDNH behaviours. Some also dispute that the UDRP rules method will likely not be suitable because it will extend the conflict settlement operations.[448] Therefore, reverse domain hijacking may interrupt or even gravely affect the businesses and procedures of the domain name owners, featuring the rejection and fraud of e-mail services, unwarranted declaration of relevant information employing phishing, and tapping websites.[449]

[448] *ADR Report - Volume 4, Publisher Pike & Fischer, 2001Page 34*

[449] *James Van Roekel, MaryAnn Bell, Bobby Ezell, Cybersins and Digital Good Deeds: A Book About Technology and Ethics, ibid,, p51.*

THIRD PART: RESOLVING DISPUTES UNDER DOMAIN NAME DISPUTE RESOLUTION POLICY (UDRP)

When a party's rights are violated, a dispute arises, which needs to be settled. Where the dispute concerns both trademark holders and domain name owners, the settlement of such disputes shall be either administrative or judicial.
In this section, the author illustrates the mechanism of the UDRP rules, examines to which extent it effectively solves the conflict between main stakeholders in cyberspace, explains the uniform domain name dispute policy in Chapter 1, and the procedures of domain name dispute resolution policy in Chapter 2.

Chapter 1: Uniform domain names dispute resolution policy: the ICANN's role

So far, one essential tool for dealing with the domain name issue is the so-called uniform domain name dispute policy. This policy would not see the light without its founder ICANN. Hence, this chapter must shed light on ICANN and its created tool.
The 'Internet Corporation for Assigned Names and Numbers (ICANN) is a non-commercial American organization. It is responsible for working with, upkeeping, and treating several data sources associated with the infrastructure of cyber names and digital numbers connected to web areas, ensuring the network's protection and security. It was established in Los Angeles, California, USA, on September 18, 1998[450].
The online world certainly varies from other areas; it requires central administration besides monitoring its address system (for instance, the .com, .org, .edu, .nl, and .uk). In line with this, the national telecommunication and information administration agency of the United States Department of Commerce, also known as NTIA,[451] has made the online world safer and more secure. In this context, the safety and security of how the web could ideally attain via privatising the domain name system's (DNS) technological administration and worldwide participation.[452] Presently, the United States federal government performs this function by employing (NTA), which has designated monitoring of the DNS to the charitable company (ICANN). The configuration of ICANN envisaged that the United States federal

---

[450] *Emmanuel Coffy MSEE JD, Albert Decady MSEE MSIS JD, The Value of Your Idea$: Make Intellectual Property Work for You, Publisher Trafford Publishing, USA 7 Canada1St edition 2020, p38.*
- Willem Th. Oosterveld, Sijbren de Jong, Stephan de Spiegeleire, Joshua Polchar and Anne-Fleur van Veenstra The Fission of Power: Flex and Flux in an Age of Fragmentation, the Hague Centre for strategic studies and tno, Netherland, 1st edition, 2015, p59.

[451] *United States. Congress. House. Committee on Appropriations. Subcommittee on Commerce, Justice, Science, and Related Agencies, Commerce, Justice, Science, and Related Agencies Appropriations for 2014: Hearings Before a Subcommittee of the Committee on Appropriations, House of Representatives, One Hundred Thirteenth Congress, First Session, Part 1, Publisher U.S. Government Printing Office, 2014, p 1451.*

[452] *United States. Congress. Senate. Committee on Commerce, Science, and Transportation. Subcommittee on Communications, Internet Corporation for Assigned Names and Numbers (ICANN): Hearing Before the Subcommittee on Communications of the Committee on Commerce, Science, and Transportation, United States Senate, One Hundred Eighth Congress, First Session, July 31, 2003, Publisher U.S. Government Printing Office 2014, Volume 108, Issue 984 of S. hrg, United States Congress, p5.*

government's function in IANA would undoubtedly be short-lived. IANA is an Abbreviation for the Internet Assigned Numbers Authority; in this regard, IANA is a standards organisation that oversees global IP address allocation, autonomous system number allocation, root zone management in the Domain Name System, media types, and other internet Protocol-related symbols and internet numbers. In time, the other would undoubtedly offer this function to the non-public economic sector.[453] Based on the announced plan by the US government, the functions have been moved to the global interested parties,[454] officially transitioning on October 1, 2016.

NTIA kept a duty connected to the domain system through three different legal arrangements: mainly the 2009 Affirmation of Dedications and ICANN; also 'IANA142 Agreement' with ICANN to carry out technological features such as designating IP address, modifying the root zone data, collaborating the task of different protocol numbers; a participating arrangement with VeriSign was made to take care of and also preserve the primary domain data system zone's origin. Via these three legal arrangements, the USA Federal Government, with the NITA, worked out heritage authority and stewardship over ICANN and perhaps had even more impact over ICANN and the domain system than other governments.[455] On March 14, 2014, the NITA revealed that it meant to change its stewardship duty and authority over domain name call system features to the international .net multi-stakeholder society. On June 9, 2016, NIT IA released its IANA Stewardship Shift Proposition Analysis. The record introduced that the change proposition satisfied its requirements and that the change procedure might continue.[456] The main question here is whether the functions of (NTIA) have fully transmitted from governmental control to the non-governmental party.

Moreover, why is such a transition important? The fear of the leading cyber society players and stakeholders was fed by the exposed internet surveillance of by some governmental parties, especially the US federal government, bearing in mind that such unlimited control would jeopardise all cyber communities. In this context of governmental overreach, there was an effort to move web administration towards a non-governmental frame, or at the very least, to respecify a multiagency structure in which states play a leading role.[457] This opinion held that there could be no more state-led prevention without endangering the existence of the 'open Internet' .[458] In line with this, the Snowden revelations have threatened ICANN's authority and prompted for the forfeiture of the USA for its controlling role in the cyber society.[459] Accordingly, numerous states and actors with a massive ICANN component saw a possibility of multi-stakeholder web domination in this situation.[460]

---

[453] *Willem Th. Oosterveld, Sijbren de Jong, Stephan de Spiegeleire, Joshua Polchar and Anne-Fleur van Veenstra The Fission of Power: Flex and Flux in an Age of Fragmentation,ibid, p59*

[454] *Uchenna Jerome Orji, International Telecommunications Law and Policy, Publisher Cambridge Scholars Publishing, UK, 2018, p117.*

[455] *ibid, p117.*

[456] *ibid, p117.*

[457] *Nicola Palladino, Mauro Santaniello, Legitimacy, Power, and Inequalities in the Multistakeholder Internet Governance: Analyzing IANA Transition Publisher Springer Nature, 2020, p6.*

[458] *ibid, p6*

[459] *Ibid, p6*

[460] *Ibid, p6.*

Moreover, revelation that the monitoring activities had been accomplished by the national security Agency (NSA) of the United States with the acceptance of the leading American companies in the industry, such as Skype and VeriSign, has damaged the United States' placement for the future of the Internet, as well as threatening dependency on the prime stakeholders as the real sponsors of this industry.[461]

In Montevideo's statement, ICANN organizations and other active members in the web industry have cautioned against losing confidence in the Internet. Additionally, it asked for activation of 'community-level initiatives towards establishing cross-Internet co-operation between several stakeholders' and 'increasing ICANN's globalisation.[462] On top of that, many presume the driving pressure behind this contract with ICANN to be the objection to adhering to Edward Snowden's discoveries of the degree of federal government involvement in surveillance activities.[463] One of the most influential stakeholders in the web industry, the European Union, has issued comments and explained that the USA had lost the global community's trust as a prime sponsor of cyberspace.[464] In its affirmation that the United States needed to do more to restore the confidence of the web industry, NTIA provided a collection of suggestions to the worldwide net area. These suggestions outlined the problems the United States federal government will consider among the web administration obligations recognised as web authorisation.[465] Such a colossal influence exerted by actors and other agencies had led an unready US administration to give its controlling role in the DNS to 'prevent other governmental parties that have impetuous goals to impose their control like China and Russia over the DNS by using some international governmental instructions under the umbrella of UN.'[466] The IANA functions transition is a turning point for the actors of web society in terms of cyberspace governance.[467] In this context, its effectiveness was thought to "strengthen the actors' strategy to net administration as well as beneficial deal decisions connected with governance selections."[468]

Another question that arises here and is worth discussing is what would happen if this shift in oversight failed to materialise. This question is a justified concern, particularly in the context of the need for fundamental change. In line with this context, Palladino & Santaniello, among other scholars, believed it could open a deadly weak point in the multi-stakeholder activity if the method fell short. In the long run, the IANA changed the procedure determining its work in 2016. It managed to eliminate the oversight role of the US federal government over internet society and changed the composition of the multi-actors in this industry.[469] One of the most significant impacts of the US oversight removal was the shrinking of intergovernmental intervention in internet society.[470]

---

[461] *Ibid, p6*

[462] *Ibid, p6*

[463] *Vidushi Marda, Internet democratization: IANA transition leaves much to be desired, ibid.*

[464] *Derrick L. Cogburn, Transnational Advocacy Networks in the Information Society: Partners or Pawns? Publisher Springer, 1st edition, 2017, p21*

[465] *Ibid p21.*

[466] *Nicola Palladino, Mauro Santaniello, Legitimacy, Power, and Inequalities in the Multistakeholder Internet Governance: Analyzing IANA Transition ibid,, p6*

[467] *ibid, p6.*

[468] *Ibid, p6*

[469] *Ibid, p6-7.*

[470] *Ibid, p7.*

Moreover, the transfer of supervision over the Internet authority reduces government interference in the Internet community. It grants non-state actors freedom in managing the global internet community, far from international polarisations and conflicting interests of states.[471] In turn, it paved the way for ICANN, supported by other non-governmental actors, to work on solving the web society problems and dilemmas. One of these issues was the domain name conflict, which led to finding a unique mechanism to deal with the dispute resolution policy dilemma.

1. Mission

The surge in internet use driven by technical breakthroughs has also put pressure on ICANN and increased its burdens on worldwide web sovereignty.[472] For instance, ICANN has broadened the variety of top-level domain names.[473] In this context, while TLD control is traditionally a portion of the binding obligation of ICANN, the ICANN has recently regulated TLDs both in terms of liberalisation and globalisation.[474] Among other missions, ICANN's essential task is to expressly guarantee the safe, steady, and dependable procedure of the world wide web's special identifier devices.[475] Much of its work involves the Internet's worldwide domain system facilitation DNS.[476] Besides that, ICANN consists of a plan for the globalisation of the DNS.

Moreover, ICANN's core work focuses on setting and creating a new genus of top-level domain names (TLDs)[477] in cyberspace to deal with the increasing demand for domain names. It is also responsible for administrating the name server's root function autonomous system number as well. In this context, ICANN also spends more effort on allotting regional IP addresses and making them available for registration. Furthermore, ICANN works on the facilitation of Internet protocol identifiers. Besides the above, ICANN's job involves generally protecting the web's operational security, guaranteeing that all competitors can obtain a fair distribution of the web benefits, particularly for cyber society stakeholders. It also accomplished the implementation of DNS body surveillance and security broadening.

2. ICANN's functions

One of the most urgent missions that ICANN was tasked with is to find practical solutions to address the issue of the domain name conflict based on generic top-level domains (gTLDs) because top-level domain (TLD) is the most critical part of the domain name system.[478] In line with this, ICANN's solution has incarnated its policy in close collaboration with the

---

[471] *Ibid, p7.*

[472] *Scott J. Shackelford, Cyber War and Peace: Toward Cyber Peace, Publisher Cambridge University Press, UK, 1st edition ,2020, P181.*

[473] *ibid P181.*

[474] *Wolfgang Benedek, Matthias C. Kettemann, Freedom of expression and the internet: Updated and revised Publisher Council of Europe, 2nd edition, 2020, p111.*

[475] *Fredrik Lindeberg, Coordinating the Internet, Publisher Linköping University Electronic Press, Sweden 1st edition, 2019, p176.*

[476] *Matthew Bernhard, Andrea Bracciali, L. Jean Camp, Shin'ichiro Matsuo, Alana Maurushat, Peter B. Rønne, Massimiliano Sala, Financial Cryptography and Data Security, Publisher Springer Nature, Switzerland edition, 2020 p236*

[477] *Ibid, p236*

[478] *Joseph K. Liu, Xinyi Huang, Network and System Security: 13th International Conference, NSS 2019, Sapporo, Japan, December 15–18, 2019, Proceedings, Publisher Springer Nature, 2019,1ist edition, p273.*

World Intellectual Property Organization (WIPO). Later, this mechanism will be known as the unified dispute resolution policy (UDRP).[479] This policy tries to provide efficient, concrete, robust, and dynamic solutions based on a rational, rapid, inexpensive resolution of the domain name conflicts away from a complicated tribunal approach by directly bringing cases to ICANN bodies adjudicating domain name conflicts. However, according to ICANN policy, domain names cannot be accepted to be registered without agreeing to abide by the UDRP rules.[480] Examining the UDRP rules decision patterns has led to the conclusion that compulsory domain name arbitration is less likely to provide a fair hearing to domain name owners asserting defences under the first amendment and other laws, particularly in the federal courts of appeal.

3. ICANN nature and structure

California's legislation has officially considered ICANN a not-for-profit organisation from its inception.[481] However, ICANN is ruled by a 16-member board of supervisors including 8 participants chosen by an appointing board on which all the voters of ICANN have stood for, and 6 representatives of its supporting agencies that deal with specific issues of the policy under ICANN.[482] There are, at this time, three leading assisting associations. GNSO, ccNSO, andASO GNSO is an abbreviation for the Generic Names Supporting the Organization. It is an organization dealing with policymaking on generic top-level domains (gTLDs). ccNSO isan abbreviation for the Country Code Names Supporting Organization. In this regard, ccNSO is an organization that deals with policymaking on country-code top-level domains (ccTLD). ASO (address supporting organization) is a supporting organization affiliated with ICANN. It was founded in 1999, and its members comprise the Address Council. The ASO's website states that the ASO's purpose "is to review and develop recommendations on Internet Protocol address policy and to advise the ICANN Board[483]. ASO deals with policymaking on IP addresses.

ICANN likewise depends on some advising boards and various other advising systems to get guidance on theissues and requirements of stakeholders that are not dealth with by existing organisations. One of them is the Global Advisory Board (GAC). GAC is an executive advisory board; its key role is to advise ICANN on public policy issues, especially where there may be an interaction between ICANN's activities or policies and national laws or international agreements[484] GAC is made up of reps of a lot of nationwide federal governments throughout the globe to provide nonbinding consultations.[485]

---

[479] *Maud Piers, Christian Aschauer, Arbitration in the Digital Age: The Brave New World of Arbitration Publisher Cambridge University Press, UK, 1STedetion, 2018, P31*

[480] *Matthew Bernhard, Andrea Bracciali, L. Jean Camp, Shin'ichiro Matsuo, Alana Maurushat, Peter B. Rønne. Financial Cryptography and Data Security, ibid,p236.*

[481] *Scott J. Shackelford, Anjanette H. Raymond, Eric L. Richards, Legal and Ethical Aspects of International Business Publisher Wolters Kluwer Law & Business New York, 2nd edition, 2021, P 582.*
- Jan Oster, European and International Media Law, Publisher Cambridge University PressUK,1st edition, 2016, P215.

[482] *Jan Oster, European and International Media Law, ibid, P216.*

[483] *https://aso.icann.org/*

[484] *Wolfgang Benedek, Matthias C. Kettemann, Freedom of expression and the internet, ibid,2020, p77.*

[485] *Matthias C. Kettemann, The Normative Order of the Internet: A Theory of Rule and Regulation Online, Publisher Oxford University Press, Uk,1stedetion, 2020,*

ALAC (At-Large Advisory Council) is an advisory committee to ICANN and the primary organisational home within ICANN for individual Internet users with a mandate to "consider and provide advice on the activities of ICANN[486]. The ALAC, which is made up of private web customers from all over the world chosen by each of the high-ranking agencies and other vital organizations in the area of the regional At-large Organizations (RALO)[487] and nominating boards like the *root web server system advisory board*, which provides suggestions on the procedure of the DNS root web server system. SSAC (Security and Stability Advisory Committee) is a committee to advise the ICANN community and Board on the security and integrity of the internet's naming and address allocation systems[488], which incorporates technical experts to examine concerns referring to ICANN and TLG safety requirements. To this point, TLG (Technical Liaison Group) is committees, task forces, and other groups providing advice related to specific matters. It acts as a bridge between the board and appropriate sources of technical advice relevant to ICANN. The TLG comprises four organizations: W3C[489], IAB[490], ETSI[491], and ITU-T[492]. This technical intermediary team comprises reps of various other global technology companies that operate, at least partially, online. [493]

4. ICANN accountability

According to the reviewers of the UDRP rules, the reviewing has concluded that the UDRP rules are the only unanimity frame that has not been involved in policy review since the organisation's starting. In this regard, one main issue with the UDRP rules from stakeholders' viewpoint, including domain registrants, is that the actual application of the policy is not uniform or foreseeable. This issue may increase as ICANN depends on more territorial UDRP rules providers in developing economies. Moreover, it is more complicated because while ICANN provides credit to UDRP rule service providers, it gives them the power to stop or transmit the domain names. ICANN has no contractual rapport with any UDRP rule

---

[486] V. Sridhar, Emerging ICT Policies and Regulations: Roadmap to Digital Economies, Publisher Springer Nature, 2019,p299.

[487] Regional At-Large Organizations (RALOs) The RALO combine At-Large Structures and individual members based on their geographical areas. As the info channel and facilitators, RALOs share details from ICANN, promote the involvement of their members, and transport the local user's point of view to ICANN. Each RALO is managed by its arranging documents, including a Memorandum of Comprehending with ICANN. Playing a crucial role in ICANN's local methods, several RALOs partner with ICANN to facilitate the development of important infrastructure for the Domain Name System. https://atlarge.icann.org/ralos/euralo#:~:text=Regional%20At-Large%20Organizations%20%28RALOs%29%20The%20five%20RALOs%20unite,the%20regional%20user%20point%20of%20view%20to%20ICANN.

[488] Section 12.2 (b) of the ICANN Bylaws.

[489] W3C is an abbreviation for the World Wide Web Consortium . W3C is the main international standards organization for the World Wide Web. Founded in 1994 as an international community where Member organizations, a full-time staff, and the public work together to develop Web

[490] IAB An abbreviation for Interactive Advertising Bureau IAB is The Interactive Advertising Bureau is an American advertising business organization that develops industry standards, conducts research, and provides legal support for the online advertising industry. https://en.wikipedia.org/wiki/Interactive_Advertising_Bureau

[491] ETSI. An abbreviation for the European Telecommunications Standards Institute. ETSI is is an independent, not-for-profit, standardization organization in the field of information and communications. ETSI supports the development and testing of global technical standards for ICT-enabled systems, applications and services. https://www.gartner.com/en/information-technology/glossary/etsi-european-telecommunications-standards-institute

[492] ITU-T .An an abbreviation for the Telecommunications Standardization Sector of the International Telecommunications Union. (ITU-T) is one of the three Sectors of the International Telecommunication Union (ITU). It is responsible for coordinating standards for telecommunications and Information Communication Technolog Lee A. Bygrave, Jon Bing ,Internet Governance: Infrastructure and Institutions, Publisher OUP Oxford, 2009 p110

[493] ICANN - Wikipedia

service undertakers.[494]One of the most logical criticisms directed at ICANN is the fragile relationship with providers of UDRP rules. In this context, ICANN was accused of being reluctant to take action. ICANN deliberately does not engage in any contractual relationship that gives it enforcement toward the other related parties. In response, ICANN defended the option of a lack of a contract with UDRP rules suppliers based on its need for a margin of flexibility to conduct its job effectively. However, this claim has been refuted not only on grounds of logical sense or sound judgment but also due to the simple fact that ICANN has certainly never taken a particular disciplinary action against any of the UDRP rule providers despite the well-documented questionable behaviour cases concerning those providers. Efficient ICANN operations calls for crystal-clear legal boundaries and on-call enforcement devices where ICANN can easily intervene with UDRP rules and URS service providers.[495] Main stakeholders suggested that ICANN implement a regular procedure for developing uniform procedures and adaptable methods for applying and marking mediation supplier accountabilities. ICANN had found that a 'it would be an exhausting use of resources to insist on arriving at a contractual relationship on the same outcome day.' The main stakeholders advise the ICANN board to expeditiously build strengthened requirements for the approval of UDRP rule suppliers and enforceable and uniform specifications controlling the management of UDRP rule situations through service providers.[496] Despite the colossal pressure exerted by international stakeholders to force ICANN to engage in a contractual relationship with UDRP rule providers to have legitimate enforcement power, ICANN has apparently resisted such contractual relationships.[497] Based on expert witnesses, this has been considered a singular failure of ICANN since its inception.[498][499]. It was also suggested that ICANN has an illegal connection with the US Division of Commerce in offense to the US Constitution or government laws. In 2009, confirming the dedications arrangement between ICANN and the US Commerce Division, the intended development of global oversight was especially controversial. Within December 2011, it was reported that ICANN had long fallen short of providing safeguards to customers from cyber impostors. In 2011, seventy-nine firms supported by the organisation of the national advertisers and led by high-ranking companies such as Coca-Cola and Samsung had rejected the ICANN schedule related to the initiation of the TLD extension program, occasionally referred to as a 'business land grab.' As a result of this objection, a further 102 organizations and 79 significant businesses have added their names.

Accordingly, ICANN started an initiative to shield trademarks in domain enrolments, which at some point finished in the facility of the trademark Clearinghouse. Among other propositions voiced during IBSA's summit held in 2011 between India, Brazil, and South Africa, there was a suggestion to move web oversight to (UN-CIRP). UN-CIRP (United Nations Committee for Internet-Related Policies) combines the functions of the Internet Governance Forum and some of the revenues of ICANN in a structure that puts governments

[494] *, ibid, p122*
[495] *, ibid, p122*
[496] *ibid, p122*
[497] *ibid, p123*
[498] *Roxana Radu, Negotiating Internet Governance, Publisher Oxford University Press, UK,1St edition,2019, P96*
[499] *Jan Oster, European and International Media Law, ibid, P216.*

on top[500]. This entity would certainly work as a part of the United Nations to offer suggestions for the urgent issues to be considered by technological companies such as those represented by ICANN and worldwide organizations such as ITU (International Telecommunication Union).

In this regard, ITU is a specialized agency of the United Nations responsible for many information and communication technology matters. It was established on 17 May 1865 as the International Telegraph Union, making it the first international organisation. This suggestion to move web oversight to the *United Nations Committee for Internet-Related Policies* implicitly criticises the lack of confidence in ICANN neutrality. The criticism extended to cyber trust. In this vein, and to name a few points, on October 7, 2013, the Montevideo declaration "revealed an urgent issue over the threatening of confidence of net customers around the world due to current discoveries of prevalent surveillance as well as monitoring."[501.]That has required speeding up the universalisation of ICANN and IANA features in the direction of an atmosphere where all stakeholders, including all federal governments, get involved on the equivalent ground. It is necessary to minimise the USA connection with the web in a considered response to the ongoing US surveillance scandal, precipitated by the NSA. Furthermore, this complicated situation of ICANN prompted some experts to declare that ICANN is still considered an American entity.[502]

Chapter 2 Domain name dispute resolution procedures

The UDRP rules developed the lawful structure that controls the resolution of conflicts between domain name owners and a third party over the violent enrolment and application of the generic top-level domain names. Because of this, any private company can file a generic top-level domain name (gTLD) that utilises the UDRP rule treatments.[503]

1. The aim of UDRP procedures

The Uniform Domain-Name Dispute-Resolution Policy (UDRP), as described above, is a practical mechanism founded by ICANN to deal with the conflict between main stakeholders (domain name owners and trademark holders) based on violating domains registered at the gTLD level or the use of domain names in an illegal way.[504,505] The goal beyond this mechanism is to avoid complicated, long, and expensive procedures before judicial forums.[506]

---

[500] *https://www.internetgovernance.org/2011/10/29/a-united-nations-committee-for-internet-related-policies-a-fair-assessment/*

[501] *Nicola Palladino, Mauro Santaniello, Legitimacy, Power, and Inequalities in the Multistakeholder Internet Governance: Analyzing IANA Transition, ibid, p7*

[502] *Richard A. Clarke, Robert K. Knake, The Fifth domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats, Publisher Penguin, New York, 1st edition, 2019, p210.*

[503] *Matthias C. Kettemann, The Normative Order of the Internet: A Theory of Rule and Regulation Online, Oxford University Press, UK, 1st edition,2020, P219.*

[504] *Roxana Radu, Negotiating Internet Governance, Publisher Oxford University Press, UK,1st edetion, 2019, P92.*

[505] *ibid, P92.*

[506] *European IPR Helpdesk, Fact Sheet domain names and cybersquatting, November 2017, p6*

Contrary to popular opinion, resorting to the UDRP rule mechanism was preferable.[507] Regulation of ICANN is believed to confirm the mandatory use of this mechanism before moving into a courthouse to resolve the conflict. To show how this mechanism works and to what extent it is practical, we need to explain UDRP rules and their procedural steps and conditions.

2 The scope of UDRP procedures

ICANN offered two decision forums to promote legal dispute decisions: UDRP and the rapid uniform suspension (URS) system.[508] Extra disputes are solved with the UDRP rules, enabling common regulation of trademark insurance claims and having fewer procedural needs. The URS system can be utilised by signing trademark holders with clear violation cases.[509] The UDRP rules might fix the following conflicts related to the domain names the registrant registered if it was comparable or similar to a trademark to which the plaintiff has rights. In return, the registrant has no legal right or genuine interest regarding that domain. A typical model of a domain name used or utilised in bad faith is when the primary goal or the reason beyond registering the domain is to trigger difficulties or create an obstacle to a rival's business.[510] UDRP rules became the "'significantly chosen system for domain conflict resolution".[511] On January 14, 2000, the first-ever case was solved via the UDRP rule mechanism[512] based on the ICANN database. The practice contracts with domain name owners by all certified registrars to guarantee during the signed agreement that the domain name owners agree not to violate the rights of the other parties and accept to file any dispute from registered domain names under UDRP rules.[513]

3. The operation of UDRP procedures

When the trademark holder considered the domain name owner as abusive to his rights, he would have the right to decide to bring a UDRP rule case -as complainant- against the supposed defendant. In line with this, the infringer who registers the allegedly abusive domain name will be be subject to the UDRP rules. The question that arises here is how does the UDRP mechanism work? The uniform domain name dispute resolution policy that ICANN has adopted sets forth the contract's registration conditions regarding any possible conflict between the main stakeholders and various other parties.[514] Suppose the trademark holder thinks the domain name owner violates his right to his trademark: in that case, he might start a case under the UDRP rule. In this context, the registrant must provide such

---

[507] *Ibid,, p6*

[508] *Kenneth W. Clarkson, Roger LeRoy Miller, Business Law: Text and Cases, Publisher Cengage Learning, United Kingdom & United States 15th edition, 2020, p172.*

[509] *ibid, p172.*

[510] *domain names regulations, 28 mar 2016 at: https://www.chambers.law/domain-names-regulations/*

[511] *Roxana Radu, Negotiating Internet Governance, ,ibid, P92.*

[512] *Farley, Christine Haight (2019) "Confusing the Similarity of Trademarks Law in domain Name Disputes, "Akron Law Review: Vol. 52: Iss. 3, Article 1. Available at: https://ideaexchange.uakron.edu/akronlawreview/vol52/iss3/1*

[513] *Ibid, p8*

[514] *Andrew Christie, Blackstone's Statutes on Intellectual Property, Publisher Oxford University Press UK, 15th edition, 2020, p 460.*

proceedings according to policy conditions related to a gTLD enrolment.[515] Paragraph 4 of this rule requires accurate and complete statements based on the registration covenant. Besides that, the domain name's registration must comply with all related laws and must not breach the legal rights of other litigants.[516]

The question arises: what is the nature of the complaint, and what does it need to be considered effective? On the justification of the analysis of the objective requirements of improving online negotiation to the end of resolving the e-disputes, it was clear that it is mainly related to the increasing market of e-commerce.[517] It subsequently creates the requirement to settle legal disputes without straight interaction between the defendant and the complaint. Furthermore, it has led to a new period of the online conflict resolution process.[518] In line with this, it assumes that the mechanism would effectively deal with such challenges. Theoretically, this vision has dominated the mainstream for a long time. However, some observers have suggested that the UDRP rule treatment has become more expensive and complicated than initially meant and occasionally unforeseeable in its result. In addition, given that the UDRP rule decisions are not mandatory, both parties can bring the case to court if they are dissatisfied with the result. Based upon previous ICANN settlements, the probabilities appear heavily in favour of the individual claiming or having trademark legal rights. The ICANN conflict resolution system,[519] in accordance with the UDRP rules, is a non-mandatory adjudication treatment typically completed within 60 days, much faster than any Ccourt decision would take.[520] The UDRP rules authorise complainants to submit a case with the resolution provider defining the domain in question, the domain holder, and the registrar of the domain name, and the areas for the objection.[521] Such background reports consist of their central standards of how the domain is similar or different to a mark to which the complainant has legal rights. Why must the participant be considered to hold no rights or actual interest regarding the domain in the debate? Furthermore, why must the domain name be considered signed up and utilised in bad faith?[522]

Moreover, the participant is provided the chance to protect himself from claims.[523] One of these guarantees is that the chosen committee by the arbitration center of WIPO will guide the registrar indefinitely to transfer the questioned domain to the complainant.[524] The

---

[515] *Frequently Asked Questions: Internet domain Names (wipo.int)*

[516] *Andrew Christie, Blackstone's Statutes on Intellectual Property, ibid, p 460.*

[517] *Agnessa O. Inshakova, Aleksei V. Bogoviz, Alternative Methods of Judging Economic Conflicts in the National Positive and Soft Law, Publisher IAP, USA,1st edition 2020, P131*

[518] *Ibid, p131.*

[519] *Richard Stim, Patent, Copyright & Trademark, Publisher Nolo, California, USA 16th edition, 2020, p494.*

[520] *ibid, p494.*

- Agnessa O. Inshakova, Aleksei V. Bogoviz, Alternative Methods of Judging Economic Conflicts in the National Positive and Soft Law,-ibid, P133.

[521] *Charles Wild, Stuart Weinstein, Neil MacEwan, Neal Geach, Electronic and Mobile Commerce Law: An Analysis of Trade, Finance, Media and Cybercrime in the Digital Age, Publisher Univ of Hertfordshire Press, Hertfordshire 1st edition,2011, p 77.*

-John Mathiason, Internet Governance: The New Frontier of Global Institutions, Publish Routledge london and new Yorkist edition,2009 P156.

[522] *Charles Wild, Stuart Weinstein, Neil MacEwan, Neal Geach, Electronic and Mobile Commerce Law: An Analysis of Trade, Finance, Media and Cybercrime in the Digital Age, ibid, p 77.*

John Mathiason, Internet Governance: The New Frontier of Global Institutions, ibid, P156.

[523] *, ibid P156.*

[524] *ibid P156.*

-Frederick M. Abbott, Thomas Cottier, Francis Gurry, International Intellectual Property in an Integrated World Economy, Publisher Wolters Kluwer, New York, 4th edition 2019, p556.

application procedure is relatively easy. The plaintiff needs to attend to the issue to match the UDRP rules, which, among other things, needs the complaint to include: the complainant's option of the panel level, including one member, three-member, or ten, besides the registrar whom the domain is registered; the trademark on which the topic is based and also the products or services with which the trademark is associated; in addition, the domain name which is the topic of the question; and the assumptions on which the debate is made.

4. UDRP rules conditions

Within the scope of UDRP rules, the complainant must prove that the domain is confusingly similar[525] to or the same as a trademark i which the plaintiff has legal rights[526] . The registrant has no legal rights or reputable interests concerning the domain name.[527] Besides, it must be proven that the domain name owner has a reason based on bad faith beyond choosing this domain to be registered.[528]

4.1 Domain is confusingly similar or the same as a trademark

Under section 4(a)(i) of the UDRP rules, a plaintiff must confirm that it has rights to a legitimate trademark and that the questioned domain is confusingly similar[529] to it. Not only do trademark legal rights establish a plaintiff is standing to bring a situation, but a UDRP rules panel will also not consider any other elements if legal rights are not confirmed. However, the resilience or vulnerability of the alleged mark will additionally factor a right into the panel's investigation of the registrant's legal rights and breach of contract, and it might identify the result of the case.[530] WIPO decided that the domain name will typically be considered confusingly comparable to that mark in its revision to these controversial criteria. The domain integrates the totality of a trademark; at the very least, a dominant attribute of the associated brand is recognisable in the domain.[531] One crucial question is whether additional terms could affect the decision in favour or whether the domain name is confusingly similar to the trademark. In this regard the questioned domain name might combine the trademark

---

[525] *Andrew Christie, Blackstone's Statutes on Intellectual Property Oxford University Press,UK, 2nd edetion2004,,p460.*
-Julian S. Millstein, Jeffrey D. Neuburger, Jeffrey P. Weingart, Doing Business on the Internet: Forms and Analysis, Publisher Law Journal Pres., New York 2020, p21.

[526] *Matthias C. Kettemann, The Normative Order of the Internet: A Theory of Rule and Regulation Online, ibid, p219.*
- Douglas A. Rettew; Jonathan Uffelman, Maximising Success in UDRP Complaints, World Trademark Review, July 1, 2016, issue 62, p73-79 www.WorldTrademarkReview.com.

[527] *Matthias C. Kettemann, The Normative Order of the Internet: A Theory of Rule and Regulation Online, ibid, p219.*

[528] *Ibid, p 7.*
- Andrew Christie, Blackstone's Statutes on Intellectual Property ibid, p460.
- Michael D. Scots, Scott on Multimedia Law, Publisher Wolters Kluwer Law & Business, 2019 4th Edition - Volume 1 - P 5-94
-Julian S. Millstein, Jeffrey D. Neuburger, Jeffrey P. Weingart, Doing Business on the Internet: Forms and Analysis, ibid, p22.
- David P. Twomey, Marianne M. Jennings, Stephanie M Greene, Anderson's Business Law & The Legal Environment - Comprehensive Edition, Publisher Cengage Learning, USA& uk 24edetion ,2021, p171.
- Matthias C. Kettemann, The Normative Order of the Internet: A Theory of Rule and Regulation Online, ibid, p219.

[529] *Howard B. Rockman intellectual Property Law for Engineers, Scientists, and Entrepreneurs, Publisher John Wiley & Sons,2nd edition, 2020, p684.*
- Ian Lloyd, Information Technology Law, Publisher Oxford University Press,UK, 9th edetion, 2020 P 388.
- David P. Twomey, Marianne M. Jennings, Stephanie M Greene, Anderson's Business Law & The Legal Environment ,ibid ,p169.
- Mark J. Davison, Ann L. Monotti, Leanne Wiseman, Australian Intellectual Property Law , Publisher Cambridge University Press,UK,4th edetion 2020,P 554.

[530] *Douglas A. Rettew; Jonathan Uffelman, Maximising Success in UDRP Complaints, ,ibid p73-79.*

[531] *section 1.7 of WIPO Overview of WIPO Panel Views on Selected UDRP Questions, Third Edition ("WIPO Overview 3.0")).*

with the added term ‘blockchain.’ The enhancement of the expression ‘blockchain’ does not resolve the confusing resemblance to the trademark, as it is identifiable in this domain.
Consequently, the committee finds that the disputed domain corresponds to the trademark, as the disputed domain name is confusingly comparable to the trademark. In this regard, UDRP rules adhere to a relatively easy three-limb framework. First, it indicates if the domain is confusingly comparable or identical to a trademark in which the complainant has legal rights. Second, it examines if the participant has the rights or authorised concern of interests regarding the domain name. Lastly, it investigates whether the respondent's domain has been signed up and utilised in bad faith.
In this context, the three parts are additionally classified into six factors that answer the following questions. Does the plaintiff have enough position to bring a complaint? Is the domain name identical to the plaintiff's mark? Does the participant have an identified lawful right concerning the domain name? Can the complainant confirm that the participant signed up for the domain name with the complainant's trademark? Or can the complainant prove that the participant uses the domain in a way that unjustly targets the complainant's mark?[532]

Regardless of such separate inquiries, the elements must be read. Simply put, a plaintiff must verify that the domain name was signed up and used with the critical function of taking the unjust benefit of its approved rights.[533] The initial part is within the single control of the plaintiff, which, in its most basic form, can be developed by holding a countrywide or regionally enrolled trademark or solution mark. The second limb is gotten over by giving a *prima facie* view, specified as “proof ample to generate a reality or raise an anticipation of fact unless shot down.”[534] The third component is more explicit than might be expected. In this context, bad faith calls for evidence of the respondent's clear and wilful act,. The condition is additionally conjunctive, suggesting that past and present conduct should be recognised. Here, the question arises if the subsequent bad faith usage occurs in this term.

Despite the subsequent usage with bad faith, registering a domain name in good faith will not be enough under the UDRP rules. [535] Inadequate proof or weak evidence is, among other things, another of many reasons why a complainant may be declined, including a lack of attention paid to these basic components. In such circumstances, the complainant would not accomplish the wanted outcome. However, inexperience is seldom compensated with a verdict of RDNH. Where the complainant falls short of meeting the evidentiary demands of the policy, the following question must be discussed: what connects a woefully inadequate complaint to the realms of abuse?[536]

---

[532] *Micah Ogilvie and Caroline Valle, Avoiding UDRP misuse – from the misinformed to the malicious, https://www.worldtrademarkreview.com/brand-management/avoiding-udrp-misuse-misinformed-malicious, 16 jan ,2020*
[533] *Ibid.*
[534] *ibid*
[535] *Ibid.*
[536] *Ibid.*

4.2 Establishing rights to a domain name identical or confusingly similar to a trademark

This element has two parts. First, the complainant must show that he or she has rights to the trademark. Second, the complainant must show that the domain name is identical or confusingly similar to that trademark. Trademark registration is the easiest way to prove rights in a mark. Panels generally accept that such registrations are proof of ownership. However, it may also have acquired common law rights in an unregistered mark if it is distinctive or has acquired secondary meaning through use.[537] When solving the conflict between domain name owners and trademark holders, it is believed that registering marks without proving the related rights is insufficient, which might dismiss the complaint.[538] In this context, such evidence might consist of money spent on advertising and marketing, unsolicited media insurance coverage, sales, announcements, marketing initiatives in that period, and continuation of the mark's usage, sales terms, and customer questionnaires.[539]

As for the scope of protection, competitiveness, and individuality,[540] the question arises if the mark is specific to a geographical area. What is the fate of the disputed domain name related to this mark? According to the common law mark, if circumstances consider whether that trademark is limited to a specific geographic market, the UDRP rules panel might admit the registrant's right to operate that disputed domain name in that regional market.[541] The complainant's requirements supply a copy of the enrolment certificate from any jurisdiction to determine his legal rights in his trademark.[542] Consequently, this step is logical and suggests that all the rejections and resistance are eliminated from the trademark, giving the claimant the right to release the trademark certificate.[543] It must be proven that the complainant possesses an authorised mark in the jurisdiction where the registrant lives.[544] The panel rejected shifting the domain name *religionnewsservice.com* to the proprietor of the RNS NEWS trade mark because the expression had been abandoned. The UDRP panel justified this decision because even though the complainant had likewise registered the expression on the supplemental register this did not, by itself, show that the expression had distinctiveness.[545]

Plaintiffs must prove that the mark works as a resource sign if the declared mark has any certain geographical significance or integrates a geographic term. If the registrant utilises a domain name that connects entirely to the geographic relevance of the mark, the objection might not stand. A UDRP panel declined to move the domain name *wifi-Paris.com* to the city

---

[537] *Howard B. Rockman, intellectual Property Law for Engineers, Scientists, and Entrepreneurs, ibid, p 684.*

[538] *Douglas A. Rettew; Jonathan Uffelman, Maximising Success in UDRP Complaints, ibid p73-79*

[539] *ibid p73-79 .*

[540] *Henning Hartwig, Research Handbook on Design Law, Publisher Edward Elgar Publishing, UK & USA, 1st edition, 2021, p166.*

[541] *Douglas A. Rettew Jonathan Uffelman, Maximising Success in UDRP Complaints; ibid, p73-79 .*

[542] *Ibid p73-79 .*

[543] *R.K. Singla, Business Studies - Class 11 - CBSE (2020-21), Publisher Global Publications, Delhi, 1st edition, 2021, p 355.*

[544] *Douglas A. Rettew; Jonathan Uffelman, Maximising Success in UDRP Complaints, ibid p73-79*

[545] *ibid p73-79*

of Paris because while the city had enrolled the trademark 'Paris', it did not follow automatically that it had trademark rights to Paris' geographical term itself.[546]

Trademarks of generic or descriptive phrases might have difficulties in all three plan aspects. In the case related to the domain name *tirediscounter.com*, UDRP panels have indicated that only a one-letter-difference is enough to conclude the decision about the similarity to the domain name *tyrediscounter.com*, indicating that it was not confusingly similar to the questionable trademark. Furthermore, a registrant's website content may determine whether the domain name was registered in bad faith. Because of the abovementioned situation, the panel might examine whether the registrant has an actual interest in the domain name under reasonable usage protection or is not practicing it in bad faith.[547] The UDRP board declined to transfer the domain *publicstoragephoenix.com* to the proprietor of the general public storage mark because the respondent had in fact used the domain name descriptively to give details regarding storage available to the citizens of Phoenix.[548]

Furthermore, suppose the mark was included in random letters or consisted of general phrases. In that case, various other individuals might legally use it. In such a situation, as with descriptive trademarks, complainants should conduct brand research in search engines to determine the degree to which other bodies use identical or related terms. In this context, the more the other parties use, the larger the load on the complainant to demonstrate that the domain name was enrolled and is used with the particular trademark in mind.[549] For instance, a UDRP panel declined to transfer the domain *MPS.mobi* to the proprietor of the enrolled M.P.S. mark, keeping in mind that M.P.S. is a three-letter phrase used by any number of other individuals for a variety of legitimate purposes. By comparison, the panel moved the domain *ehf.com* to the EHF mark holder, regardless of the registrant's evidence that EHF is a general acronym; the panel justified the decision based on the complainant's evidence that the registrant had clearly and wilfully targeted the disputed mark.[550]

4.3 The registrant has no legal rights or interests in the registered domain name

One of the main UDRP requirements to initiate the case is the approval that the registrant has no legal rights to or interests in the registered domain name.[551] Based on UDRP rules, the margin of legitimacy interest within a domain name could include the registrant using or executing verifiable preparations to make use of the domain or a name representing it about a

---

[546] *ibid p73-79.*

[547] *ibid p73-79*

[548] *ibid p73-79*

[549] *ibid p73-79*

[550] *Ibid, p73-79*

[551] *Fernand de Visscher, Christopher Dumont, the importance of prior rights in domain name disputes https://simontbraun.eu/wp-content/uploads/2021/02/News-domain-names-Importance-of-prior-rights-bpost-February-2021.pdf,February 2021, p1.*
- Matthias C. Kettemann The Normative Order of the Internet: A Theory of Rule and Regulation Online
ibid, P219.
- Andrew Murray, Information Technology Law: The Law and Society, Publisher OUP Oxford, UK, 2nd edition,2013,p426.
- Howard B. Rockman, intellectual Property Law for Engineers, Scientists, and Entrepreneurs,ibid, p 684.
- Julian S. Millstein, Jeffrey D. Neuburger, Jeffrey P. Weingart, Doing Business on the Internet: Forms and Analysis, ibid, p4-20.
-Simon Stokes, Art and Copyright Publisher Bloomsbury Publishing,UK & USA,1st edition, 2021, P224.
- Michael D. Scott ,Scott on Multimedia Law,PublisherWolters Kluwer, 4th Edition,2021 ,P 5-94

bona fide presence of items or services before any notice to the registrant of the conflict as section 4(c)(i) suggests.[552] The registrant (a particular business or other institution) must generally know if the domain has obtained no mark or rights in the service mark, as seen in section 4(c)(ii).[553] The registrant accepts a legitimate non-commercial or reasonable use of the domain without intent for a commercial gain to divert customers misleadingly or defame the trademark or service mark.[554] In this regard, the other party has a legitimate interest in a domain if the confusion about a similar mark can be ignored.[555] The registered domain name related to personal names as trademarks is considered a solid indicator of good faith, according to the UDRP ruling.[556] Even though this vital factor stands in the complainant's favour, he is still responsible for confirming it. In this regard, the complainant has to support his good faith and hold the burden of approving that the registrant has no legal rights or legitimate affairs in the contested domain name. Afterward, the burden of concern moves to the other party[557.] This component is one of the various doubts for a plaintiff because it seldom recognises what proof exists to verify a registrant's right to use the domain name,[558,559] except for a reasonable usage in the case.[560] In this regard, the UDRP rules provide a non-exhaustive list of three conditions that shows a registrant's legal claims or legal affairs in the disputed domain name.[561] To this point, section 4(c)(ii) of the UDRP rules indicates that the registrant (as a business, individual, or other organization) has been commonly known and recognised by the domain name, even if it has acquired no trademark or service mark rights.[562] Besides that, the second condition (iii) is registering the domain name to disrupt the competitor trades. The third condition is focused on whether the registrant is making a legitimate non-commercial or fair use of the domain name without intent for commercial gain, or if they are using it to divert consumers misleadingly, or to tarnish the trademark or service mark at issue, as mentioned in section 4(c)(iii)[563]. Showing *bona fide* is important to move the burden to approve the opposite to other parties.

Furthermore, this aspect is the most unpredictable for a complainant since it rarely recognises what proof exists to confirm a registrant's right to use a domain name, excluding

---

[552] *Douglas A. Rettew; Jonathan Uffelman, Maximising Success in UDRP Complaints, ibid, p73-79*

[553] *Ibid,, p73-79 .*

[554] *ibid. p73-79 .*

[555] *Howard B. Rockman, intellectual Property Law for Engineers, Scientists, and Entrepreneurs, ibid, p 684.*

[556] *Jacqueline D. Lipton,Internet domain Names, Trademarks and Free Speech, Edward Elgar Publishing, UK & USA, 1st edition,2010, p191,*

[557] *Howard B. Rockman, intellectual Property Law for Engineers, Scientists, and Entrepreneurs, ibid, p 684.*
- Douglas A. Rettew; Jonathan Uffelman, Maximising Success in UDRP Complaints, ibid, p73-79.

[558] *Ibid, p73-79*

[559] *Douglas A. Rettew; Jonathan Uffelman, Maximising Success in UDRP Complaints, ibid, p73-79*

[560] *Ibid, p73-79*

[561] *Mark Davison, Ann Monotti, Leanne Wiseman, Australian Intellectual Property Law ibid,,P 50*

[562] *Lanning G. Bryer, Scott J. Lebson, Matthew D. Asbell, ntellectual Property Strategies for the 21st Century Corporation: A Shift in Strategic and Financial Management, Publisher John Wiley & Sons,1st edition, USA 2011,p92,93.*

[563] *Mark Davison, Ann Monotti, Leanne Wiseman, Australian Intellectual Property Law, ibid P 50.*
- Lanning G. Bryer, Scott J. Lebson, Matthew D. Asbell, ntellectual Property Strategies for the 21st Century Corporation: A Shift in Strategic and Financial Management, ibid,,p92,93.
- Douglas A. Rettew; Jonathan Uffelman, Maximising Success in UDRP Complaintsibid ibid, p73-79
- mark j. thronson gabrielle s. roth jon d. grossman, Intellectual Property Legal Opinions, Publisher Wolters Kluwer new York , ,2nd edition, 2020, P 9-40.

where reasonable usage might be a critical factor.[564] This issue increases an inquiry below if the *bona fide* is enough in such an instance. Any legitimate interest arrangement for individual personal domain names must be composed differently. Most likely, the earlier-mentioned regulations may prevent some unapproved commercial uses of domain names if they are connected with a *bona fide* interest.[565] In line with this, the UDRP ruling, for instance, justified the evident arrangement to use a domain name related to a *bona fide* showing of products or services.[566] In this regard, it makes good sense in a trademark-based system, probably in different commerce locations, since it totals two legitimate competing interests in using the mark consisting of the personal name in a domain name.[567]

Suppose the plaintiff has signed the trademark 'Hypo' for clinical syringes. Another party has indeed enrolled *hypo.com* as a domain name for a company entailing the sale of examination questions related to method legislation. Also, he has registered the domain name *bona fide* for particular objectives. In that case, he should be qualified to use it.[568] On the other hand, if the practice and regulations behind the right of public advertisement hold any person from making any unjustified earnings from one more person's name or likeness, the mediation mechanism might not always enable enrolment of the personal names as a domain name is *bona fide* to benefit from that domain name based on a unique name as a trademark to promote his services or goods in cyberspace. However, it is not simple to consider a situation where a person would undoubtedly enrol a personal name as a domain name concerning such a purpose. Difficulties might occur under a new character legal rights framework where an individual name genuinely is a trademark, as wherever the individual concerned runs a business following his name. In these circumstances, trademark-based legislation should apply concerning the trademarked term. Why would anyone register, for example, the domain name *tomford.com*, to offer products or services unrelated to Tom Ford? It will undoubtedly confirm the assumption that people have an obligation to avoid unauthorised commercial earnings from famous internet characters, at the very least in the 'name.com' area.[569]

4.4 Bad faith

Bad faith plays a crucial role in deciding the rights and proves the violation against main stakeholders in cyberspace.[570] In this connection, paragraph 4 of the UDRP rules indicated that the domain name had been registered and used in bad faith.[571] The question that arises here is how bad faith matters can be approved. The essential characteristic of this element is whether the registrant is *mala fide*, as explained in part (c)and para 4(b) of the UDRP rules.

---

[564] *Douglas A. Rettew; Jonathan Uffelman, Maximising Success in UDRP Complaints,ibid, p73-79.*

[565] *Jacqueline D. Lipton,Internet domain Names, Trademarks and Free Speech, Publisher Edward Elgar Publishing, UK & USA, 1st edition,2010, p191,*

[566] *- Andrew Murray, Information Technology Law: The Law and Society,ibid,p426.*
- Lanning G. Bryer, Scott J. Lebson, Matthew D. Asbell, ntellectual Property Strategies for the 21st Century Corporation: A Shift in Strategic and Financial Management, ibid,,p92,93.

[567] *Jacqueline D. Lipton,Internet domain Names, Trademarks and Free Speech, ibid, p191,*

[568] *ibid, p191,*

[569] *ibid p192,*

[570] *Mark J. Davison, Ann L. Monotti, Leanne Wiseman, Australian Intellectual Property Law , ,Ibid,,P 554.*

[571] *Andrew Murray, Information Technology Law: The Law and Society, ibid,,p426*

In this context, it is indicated that the panelist may use it as proof that the enrolment and usage of a domain name are in bad faith.[572]

Some factors show that the registrant has enrolled or gained the domain name fundamentally for the intention of sale, hiring, or otherwise shifting the enrolled domain name to the complainant involved in the case, in which the other party is the owner of the trademark or service mark; or to a contender of that complainant, for worthwhile remuneration over documented real value or cost directly related to the domain name.[573] Or, the registrant has enrolled the domain name in order to block the trademark or service mark owner from using it in a corresponding domain name; Or, the registrant has been involved in related behaviours.[574] Another situation might indicate bad faith if the registrant has registered the domain name principally to prevent the contender from practicing his job[575] or using the domain name. It also indicates if the registrant has purposely endeavoured to draw, for profitable gain, web users to their website or cyber location by generating a case of possible confusion[576] with the complainant's mark.[577]

5. UDRP rules "in partice" – the example of bpost.com

In the case bpost vs. bpost.com, the suit has been applied to the arbitration and mediation center of the WIPO over the disputed domain name *bpost.com*, which was registered on April 16, 2001. On August 16, 2010, this trademark was certified, while the domain name registration was enrolled on February 4, 2010. According to the UDRP rules associated with paragraph 4(a), the complainant should verify that the domain name is confusingly similar to the complainant's trademark. Additionally, the complainant should verify that the domain name holder has no legal rights or legitimate interests concerning that trademark. In this context, the complainant was the proprietor of the trademark Bpost N.V.

Moreover, the complainant should verify that the contested domain name has been used and registered in bad faith.[578] The arbitration panel did not find it challenging to meet the first part of the policy's requirement related to the identical or confusingly similar nature of the domain name *bpost.com* and the trademark *BPOST*. Hence, it decided it had met the rules for the other conditions related to legitimate interests - registration and use in bad faith. The complainants claimed that the domain name holder was a squatter and had no legitimate interest in using the phrase 'bpost.'

Furthermore, the complainants argued that the domain name holder had never used the targeted domain name in good faith, to show goods or services. The sole goal of using

---

[572] *Fernand de Visscher, Christopher Dumont, the importance of prior rights in domain name disputes https://simontbraun.eu/wp-content/uploads/2021/02/News-domain-names-Importance-of-prior-rights-bpost-February-2021.pdf,February 2021, p1.*
- Mark Davison, Ann Monotti, Leanne Wiseman, Australian Intellectual Property Law Publisher Cambridge University Press,UK, 3rd edition,2016 ,P 50

[573] *mark j. Thronson gabrielle s. Roth jon d. Grossman, Intellectual Property Legal Opinions, ibid, P 9-40.*

[574] *ibid, P 9-40.*

[575] *Gonzalo Bleda Navarro ,Maria de Lourdes Aguirre, Quick Guide to WIPO domain Name Dispute Resolution Services for the .MX ccTLD, Geneva October 8, 2020, https://www.wipo.int/export/sites/www/amc/en/docs/cctld_mx.pdf, workshop, WIPOI Arbitration and Mediation Center p18.*

[576] *Julian S. Millstein, Jeffrey D. Neuburger, Jeffrey P. Weingart, Doing Business on the Internet: Forms and Analysis, ibid, p4-22*

[577] *mark j. thronson gabrielle s. roth jon d. grossman, Intellectual Property Legal Opinions, Publisher Wolters Kluwer new York , ,2nd edition, 2020, P 9-40.*
- Andrew Murray, Information Technology Law: The Law and Society, ibid,,p426

[578] *Fernand de Visscher, Christopher Dumont, the importance of prior rights in domain name disputes , https://simontbraun.eu/wp-content/uploads/2021/02/News-domain-names-Importance-of-prior-rights-bpost-February-2021.pdf,February 2021, p1.*

this domain name, it was argued, was to distract, confuse, and mislead the targeted consumers confusingly and take advantage of the reputation of the complainant's trademark. Instead, however, the panel was concerned about the time between registering the domain name (i.e., April 16, 2001) and the invoked right (i.e., August 16, 2010). In considering this, the panel found no suspicious behaviour that could indicate bad faith regarding the domain name *bpost.com*. The panel emphasised that holding several domain names is not, *per se*, proof of bad faith. The WIPO mediation committee highlighted that the domain name holder had no possibility of displaying the then-non-extant trademark of the complainant. The defendant did not target the complainant when enrolling the contested domain name.[579] This result clarifies established case law on trademark enrolment after a domain name is registered (or released by application). The behaviour in this case (registering the domain name) cannot be explained as being conducted in bad faith. The domain name holder cannot have been mindful of the complainant's trademark when they enrolled the domain name, as it did not exist at that time. As a consequence, the committee rejected the complaint.[580]

Chapter 3: ICANN Extra remedies

In incorporation with the world intellectual property organization, ICANN has created administrative mechanisms to solve contested domain names and other rights related to trademarks in cyberspace. In this context, the UDRP rules were limited to general top-level domain names during the emergence of the World Wide Web. The conflicts involved domain name chains such as .com, .org, and .net, with high trade value. Moving forward, in the face of massively increasing demand in the domain names industry, ICANN sought to pump new domain name chains into the market. However, this step increased the conflict. At the same time, the UDRP rules were limited to solving conflicts over top-level domain names. Consequently, ACANN had to find another mechanism to solve other conflict-related problems with the new gTLDs. This chapter highlights these remedies and their effectiveness in solving such conflicts.

Because of the considerable judicial costs, several disagreements over cybersquatting are resolved out of Court. The alternative UDRP rules became the favourite course for solving domain name disputes. In this context, to encounter the increasing demand for domain names and the colossal flourishing of the domain name industry, ICANN supplied 400 New gTLDs. Such new gTLDs might be unrestrictive or restrictive, or detailed attributes, for example, taking the following kind of gTLDs: [brand], [city], [community], [culture], [industry], or [language]. The domain name market increased further, with 200 more gTLDs delegated by January 2018. These New gTLDs caught around 22 million customers under second-level domain name[581] registrations.[582] The margin of gTLD domain names has, in turn, increased the conflicts over domain names. As a result, they are considering that UDRP rules were

[579] *ibid, p1.*

[580] *Fernand de Visscher, Christopher Dumont, the importance of prior rights in domain name disputes , ibid, p1.*

[581] *Wipo, World Intellectual Property Organization, Standing Committee on the Law of Trademarks, Industrial Designs and Geographical Indications Thirty-Eighth Session Geneva, October 30 to November 2, 2017 Update On Trademark-Related Aspects Of The domain Name System, WIPO, Geneva, 2017, p4.*

[582] *Frederick M. Abbott, Thomas Cottier, Francis Gurry International Intellectual Property in an Integrated World Economy, Publisher Wolters Kluwer, New York,4th edetion,2019 p550.*

limited to specific gTLDs.[583] The question arises whether new gTLDs are approved. What are the mechanisms of protection given to trademarks? Besides the UDRP that applies to all new gTLDs, ICANN has created mechanisms based on a wide margin of rights protection measures (RPMs). This umbrella includes, among others, a uniform rapid suspension system (URS), and trademark claims services.[584] These different remedies are presented in: the legal rights objection (LRO), Clearinghouse, the uniform rapid suspension system (URS), and the trademark Post-Delegation Dispute Resolution Procedure (PDDRP).

1. Right Protection Mechanisms

Right Protection Mechanisms (RPMs) are mechanisms based on the dispute resolution procedures listed below to support a trusted marketplace, and implemented for the New gTLD Program to mitigate potential risks to rights holders that could arise due to expanding the new gTLD namespace, and to help create efficiencies for registration service providers amid gTLD launches. As mentioned, UDRP rules are limited to gTLD. Thus, different mechanisms deal with the new generation of domain names. In this connection, RPMs combine corrective and precautionary procedures, including top-level and second-level domain names before and after ICANN's new gTLDs are handed over to the particular registry operators. Hence, RPMs comprehensively influence the intellectual property implementation related to global society.[585] In this regard, The ICANN supervisors adopt all the procedures and services related to its second-level domain name enrolment. Although ICANN's RPMs comprise an assortment of policies, they focus on preserving intellectual property rights, especially trademark rights.[586]

1.1 Legal right objection procedure

The right legal objection (LRO) approach is a crucial safety measure instrument that empowers a trademark holder to challenge an appeal for a gTLD chain that can infringe the trademark under normally approved and worldwide acknowledged law concepts.[587] Since it started in 2008,[588] ICANN has provided the legal rights objections procedure (LRO) to permit the complainants with standing to process disputes related to the new gTLD chains. In the relationship, as mentioned earlier, the priority will be given to the complainer by default. However, LRO can also be considered an effective tool to protect society's interests related to the Internet, particularly if the competitor fails to react to the objection; hence some

---

[583] *Wipo World Intellectual Property Organization, Standing Committee on the Law of Trademarks, Industrial Designs and Geographical Indications ibid,, p3.*

[584] *World intellectual property orgaanization, Frequently Asked Questions, (wipo.int).*

[585] *Hong Xue, Caveats of intermediary liability in the domain Name System: a review of the ICANN new gTLD right protection measures,Intellectual Property Perspectives on the Regulation of New Technologies Publisher Edward Elgar Publishing, , 2018 chapter 2 , p36*

[586] *Hong Xue, Caveats of intermediary liability in the domain Name System: a review of the ICANN new gTLD right protection measures, in Intellectual Property Perspectives on the Regulation of New Technologies Publisher Edward Elgar Publishing, 2018 chapter 2p3*

[587] *Justine Chew, update & consultation ON New gTLD Subsequent Procedures Consensus Building on Recommendations OBJECTIONS (v13) 25 August 2020, p4.*

[588] *World Intellectual Property Organization Report of the Director General to the 2020 WIPO Assemblies: Retrospective 2008-2020, Volume 1050 of WIPO Publication Publisher WIPO,swiazerland, 2020, P42.*

exclusions should be considered. For instance,[589] one case that has been widely examined shows how LRO can be used to protect the potential societal interest in a cyberspace-related domain name (.Lotto). Chain lawsuits presented concrete vital cases where the objector failed to confirm the probability of material harm. Therefore, the claimant party prevailed.

For the opportunity to prove the material damage, the objector declared that while European lotteries stick to strict requirements of responsible gaming, through decreasing potential damage to the community and particularly vulnerable individuals, the general accessibility of the *.lotto* domain name might confer upon unlawful operators the benefit of connecting their website with lottery games to those authorised by the state, thus damaging the interests of unwary customers.[590]

The plaintiff might file a formal action to the objection, subject to the dispute policy. The objector with the standing might submit standard arguments in "community opposition principles, legal rights, public interest, or confusion".[591] As for the *.int*[592] domain name, besides the other stakeholders and individuals, the observer bodies and other functional agencies of the United Nations are acknowledged as satisfying the requirements.[593] In this regard, because *.int* is considered to have the strictest policies of all TLDs, it requires that the holder is subject to international law and to provide evidence that it is indeed treaty-based by providing a United Nations treaty registration number and that it has independent legal status. Besides that, IGOs are also qualified to arrange a lawful rights argument if it matches the standards for enrolment of *.int* domain names.[594] IGO is an abbreviation of intergovernmental organisation. In this regard, an IGO is an entity created by a treaty involving two or more nations to work in good faith on issues of common interest. Without a treaty, an IGO does not exist in the legal sense. In this regard, the global treaty within or amongst national governments must recognise the organisations. Also, these recognised organisations must be widely considered an independent global legitimate entity and be the topic of and controlled by international legislation.[595] In the same context, IGOs are given 90 days as a service of claims notification for every new gTLD.[596]

In this situation, an effective argument will be filed against the correct application from being accepted or passed on by ICANN. For example, the new gTLD applicant might try to resolve with the objector or repeal the involved gTLD application. The question that can be left for discussion here is whether filing a response to a legal rights objection is

---

[589] *Hong Xue, Caveats of intermediary liability in the domain Name System: a review of the ICANN new gTLD right protection measures, ibid, p37*

[590] *Burkhard Hess, Maria Bergström, Eva Storskrubb, EU Civil Justice: Current Issues and Future Outlook, Hart Publishing., 1st edition ,2016, p71.*

[591] *Hong Xue, Caveats of intermediary liability in the domain Name System: a review of the ICANN new gTLD right protection measures, ibid, p37.*

[592] *Int. Treaty Organisations .int Domain Registration - .int is a sponsored top-level domain (gTLD) used on the Internet's Domain Name System.. According to current IANA policy, the .int gTLD is reserved for international treaty-based organizations, United Nations agencies and organizations or entities having Observer status at the UN. .int is considered the strictest gTLD in as much as it implies that the holder is a subject of international law. Hence, the Stockholm Convention on Persistent Organic Pollutants (POPs) saw its application for a .int domain rejected on the grounds that the Convention did not explicitly create an entity subject of international law. Additionally, .int was historically also used for "Internet infrastructure databases". The .eu.int sub-domain was used by the European Union-affiliated institutions.*

[593] *ICANN, gTLD Applicant Guidebook (v. 2012-06-04) Module 3 4 June 2012,P3-6 http://newgtlds.icann.org/en/ applicants/agb/objection-procedures-04jun12-en.pdf*

[594] *Ibid, P3-5*

[595] *ICANN, gTLD Applicant Guidebook ,ibid, P3-6 f*

[596] *Luc Seufer , The next round of gTLDs is around the corner, August 9, 2019, https://ebrandservices.com/the-next-round-of-gtlds-is-around-the-corner/.*

compulsory. In this connection, the reactions need to be sent online to the WIPO center, using the WIPO center's official LRO frame response to inform both ICANN and the objector. The reaction declaring cost should be listed when declaring the reaction.

On top of that, a reaction must include, at the very least, the applicant's name, complete contact information, and the full points that were answered to the declarations made in the objection[597] . From 2012 to 2013, the center received 69 compliant LRO requests, in which panelists decided on WIPO's LRO.[598] In this regard, ICANN must reduce the risk of inconsistent outcomes in the string confusion objection[599] process, especially where the objector seeks to object to multiple applications for the same String.[600] The question arises: What criteria will the panel use to determine the legal rights objection outcome?

1.1.1 The criteria to determine the legal rights objection

According to ICANN Applicant Guidebook section 3.5.2, potentially unjustifiable damages, unjustly taking the privilege of the distinct personality, or enrolled or non-enrolled trademark reputation related to the objector producing a possibility of confusion in linking the gTLD application to the objector trademark will all be vital criteria in deciding the result of legal rights objection.[601] To activate the objection mechanism based upon trademark legal rights, the panel will certainly consider the resulting nonexclusive circumstances: Whether the objector's mark is similar or identical, and whether the objector's use of rights in the mark has been *bona fide* or not.[602] Also, the panel will consider whether the relevant part of the available domain name is associated with the mark of the appellant, objector, or other stakeholders. Moreover, they will consider the purpose of the request for that gTLD by the applicant. For instance, the supposed contenders applied for or operated TLDs or registered them in bad faith. Alternatively, the domain name was identical or confusingly similar to the marks of others. Moreover, it will be crucial that the applicant or the contender has previous knowledge of the objector's mark at the registration or operation.[603]

Regardless of the degree, the panel will consider whether the competitor has utilised or done provable work to match the gTLD to a *bona fide* related presentation of services or product info in a manner that does not conflict with the reasonable and legal performance by the objector of its mark rights.[604] Besides that, the panel considers if the petitioner's behaviour beyond using the gTLD would create a possibility of confusion against the mark of objector as to the source, sponsor, association, or approval of the gTLD.[605]

---

[597] *World intellectual property orgaanization, Frequently Asked Questions, Frequently Asked Questions (wipo.int)*

[598] *World Intellectual Property Organization Report of the Director General to the 2020 WIPO Assemblies: Retrospective 2008-2020, ibid, P42.*

[599] *i. e. An objection made on the grounds that the applied-for gTLD string is confusingly similar to an existing TLD or to another applied-for gTLD. Definition of String confusion objection. In: Domain Name Dictionary. https://www.domainsherpa.com/domain-name-dictionary/string-confusion-objection/*

[600] *Justine Chew,update & consultation on New gTLD Subsequent Procedures Consensus Building on Recommendations objections ibid,,p10.*

[601] *World intellectual property orgaanization, Frequently Asked Questions, ibid,.*

[602] *Inid.*

[603] *World intellectual property orgaanization, Frequently Asked Questionsinid,ibid..*

[604] *ibid*

[605] *ibid*

1.1.2 Dispute settled under the legal rights objection

Supposing, based on the parties common desire to give a chance to solve their conflict using mediation, there is no legal obstacle, and they have just requested a 30-day suspension. In this example, the role of the WIPO center is limited to assisting in achieving this wish without any extra fees or costs.[606] In this connection, there is a requirement for their demand to consider joining a statute of limitations, an arbitration stage prior to settlement (as an example, to make sure that a subordinate infringing weblink might be eliminated without retrieving the domain name itself), and also enabling longer due dates to react to cases of the violation.[607] The requestor's objection is restricted to 20 pages or 5,000 words, whichever is less, except for any other extra attachments. The objector or claimant should likewise describe and submit any defending proof with any necessary attachments.[608]

1.1.3 LRO remedies

As for the possible remedies that the LRO can provide, the treatments are restricted to the gain or rejection of the objection. Furthermore, despite no financial damages, the dominating litigant is obliged to pay for the UDRP panel.[609] However, some reviewers have called to apply the rule that forces the loser to pay (similar to the practice in trademark opposition and cancellation proceedings in the EU[610]).

1.1.4 Retain the Court options

The legal rights objection is an alternative policy to solve the conflicts between the main stakeholders. It does not prevent the parties from choosing to go to Court as a possible further step to resolve the conflict. In this case, either of the defendants might send the conflict to court[611]. Additionally, the present system demands such cases to be appealed before a tribunal of the competent jurisdiction, which costs substantial money, time, and effort.[612]

1.2 Trademark Clearinghouse

TMCH (Trademark Clearinghouse) is an ICANN-mandated central database of information on trademarks to boost intellectual property defence in cyberspace.[613] In this respect, the data

---

[606] *ibid*

[607] *WIPO Magazine, Issue 6/2019 (December) World Intellectual Property Organization, p42*

[608] *World intellectual property orgaanization, Frequently Asked Questions, ibid*

[609] *ibid*

[610] *WIPO Magazine, Issue 6/2019 (December) World Intellectual Property Organization, ibid,p42*

[611] *World intellectual property orgaanization, Frequently Asked Questions, ibid.*

[612] *WIPO Magazine, Issue 6/2019 (December) World Intellectual Property Organization,ibid p43*

[613] *Barney Warf ,The SAGE Encyclopedia of the Internet, PublisherSAGE, 18th edetion, 2018, , 2018, P 262.*
- Frederick M. Abbott, Thomas Cottier, Francis Gurry ,International Intellectual Property in an Integrated World Economy,ibid, p551

source of legitimate brands will shield these trademarks, particularly when the new TLDs are launched.[614]

1.2.1 Clearinghouse Mechanism and Functions

TMCH has been developed to improve security and decrease the cost of protection for trademark holders. Also, the trademark Clearinghouse will certainly approve and confirm the legal rights information. It will unquestionably sustain trademark guarantee claims, and sunrise service is needed in an all-new top-level domain name introduced in ICANN policy. To this point, the sunrise period permits trademark holders an advanced possibility to enrol domain names corresponding to their marks before it is available to the general public.[615] The sunrise period is a minimum of 30 days. It is anticipated to play a crucial function in the new TLD program's launch and ensure that trademark legal rights can be smoothly protected.[616] In this connection, TMCH enables personal trademarks to do protective enrolment of new gTLDs related to these trademarks before opening the enrolment to the public.[617] It authenticates trademark information submitted by the right holders and provides the relevant information to the registry operators and registrars.[618] The Trademark Clearinghouse will certainly not demand that trademark proprietors declare ownership of all their trademarks openly in public. Rather, once a trademark has been sent to and verified in the main database, the trademark proprietor will be provided an advantage in enrolling pertinent domain names throughout the sunrise period.[619] The sunrise enrolment procedure gives priority and full accessibility to the trademark owner registering the domain name(s) similar to his trademark.[620] The trademark claims period follows the sunrise period. It runs for at least the first 90 days of an initial operating period of general registration. An attempt to register a domain name during the trademark claims period, matching a mark recorded in the trademark Clearinghouse, will prompt a notification to be sent to the proprietor ofthe relevant mark.[621] Suppose the applicant goes ahead and registers the domain name. In that case, the trademark Clearinghouse will send a notice to those trademark holders with matching records in the Clearinghouse informing them that someone has registered the domain name.

Moreover, the trademark Clearinghouse will not just be a resource of information that brand name proprietors can log into to see what has been trademarked;, it will also alert trademark proprietors who have sent their trademark info to the database.[622] Furthermore, if a

---

[614] *Bobbi Sandberg, Networking The Complete Reference, Third Edition,3rd edetion, Publisher McGraw Hill Professional 2015, p289.*

[615] *https://newgtlds.icann.org/en/about/trademark-clearinghouse/faqs*

[616] *Jennifer C. Wolfe, Anne H. Chasser, domain Names Rewired: Strategies for Brand Protection in the Next Generation of the Internet , Publisher John Wiley & Sons, USA, 1st edetion 2013 P68*

[617] *Shahrooz Pouryousef,Muhammad Daniyal Dar, Suleman Ahmad, Phillipa Gilll, and Rishab Nithyanand , Extortion or Expansion? An Investigation into the Costs and Consequences of ICANN's gTLD Experiments, Passive and Active Measurement: 21st International Conference, PAM 2020, Eugene, Oregon, USA, March 30-31, 2020, Proceedings, Springer Nature,swiszrland, 1st edition, 2020,p147.*

[618] *Jennifer C. Wolfe, Anne H. Chasser, domain Names Rewired: Strategies for Brand Protection in the Next Generation of the Internet , ibid, P68.*

[619] *Ibid, P68.*

[620] *Hong Xue, Caveats of intermediary liability in the domain Name System: a review of the ICANN new gTLD right protection measures, ibid, p38*

[621] *https://newgtlds.icann.org/en/about/trademark-clearinghouse/faqs*

[622] *Jennifer C. Wolfe, Anne H. Chasser, domain Names Rewired: Strategies for Brand Protection in the Next Generation of the Internet , ibid, P68. 9*

trademark holder wants to omit his mark from all new gTLD frames, it can do so by getting involved in each new 'sunrise duration.[623] In that situation, the trademark holders will obtain a direct alert via email or SMS from the trademark Clearinghouse to inform them if somebody else attempts to enrol a domain name similar or identical to their name or trademark under a new gTLD. The Clearinghouse's mission will certainly be based on two practical functions. The first is authentication and recognition regarding Clearinghouse's trademarks. The second is a data source to provide details to the brand-new gTLD registries to sustain pre-launch sunrise or trademark case services.[624]

1.2.2. Clearinghouse importance

There are three primary advantages of the trademark Clearinghouse. First, the trademark Clearinghouse will not allow trademark proprietors to state; they have all trademarks openly. For example, Nike will most likely not use the new 'sporting activity' gTLD to acquire the Nike domain name. Nevertheless, as soon as a brand has been sent and verified into the main database, the trademark proprietor will be given an advantage against other stakeholders to enrol appropriate domain names throughout sunrise durations.[625] Second, the sunrise enrolment procedure offers top-priority access to the trademark owner to register the domain name(s) as the trademark.[626] The trademark claim services alert the owner when a domain name meets the trademark enrolled by a person throughout the claim duration of an offered new gTLD.[627] In that instance, they will get a notification email from the trademark Clearinghouse to inform them if somebody else attempts to enrol domain names including their name, under the new gTLD. As for the third advantage, the trademark Clearinghouse for personal trademark proprietors permits the use of the Uniform Rapid Suspension System (URS). In this regard, the goal of the TMCH is to pave the way for both sunrise services and trademark claim services to take their position regarding trademark protection.[628] Among other European organisations and institutions, ICANN has chosen Deloitte as the TMCH in Europe.[629] This choice indicated ICANN's practical steps to give more momentum to the protection given to trademarks within new gTLDs in cyberspace.

Moreover, as a comprehensive database and alert, the trademark Clearinghouse's double mission will undoubtedly provide security against trademark violations. Even so, it still may not completely safeguard individuals enrolling in domain names, including trademarked ones.[630] According to available reports, the TMCH had indeed, by February

---

[623] *Hong Xue, Caveats of intermediary liability in the domain Name System: a review of the ICANN new gTLD right protection measures, ibid, p38*

[624] *Jennifer C. Wolfe, Anne H. Chasser, domain Names Rewired: Strategies for Brand Protection in the Next Generation of the Internet , Publisher John Wiley & Sons, USA, 1st edetion 2013 P68*

[625] *Ibid, P68*

[626] *Hong Xue, Caveats of intermediary liability in the domain Name System: a review of the ICANN new gTLD right protection measures, ibid p38*

[627] *ibid p38*

[628] *Luc Seufer, the next round of gTLDs is around the corner, ibid.*

[629] *Jennifer C. Wolfe, Anne H. Chasser, domain Names Rewired: Strategies for Brand Protection in the Next Generation of the Internet, ibid, P68.*

[630] *ibid, P68.*

2018, collected over 43,000 violations .[631] The Clearinghouse would make the registry responsible for any possible registration violation in any connected context. In this regard, before the clearinghouse's existence, the registries were exempt from liability related to any possible registration violation by prior offenders. In *WorldSport Networks v. ArtInternet*, the court originally declared that NSI does not allow anybody to enrol a name comparable to one already identified as as an infringement. Suppose the offenders sign up for a domain name. In that case, they are called to submit a record establishing that the enrolment does not break the order with the court and the complainants. Hence, the court established that NSI need not evaluate domain name enrolments to conform with the court order. The NSI behaviour seemed justified because NSI then did not have the tools and resources to decide whether these names infringed the trademark rights.[632]

As a further step, ICANN has incorporated two stipulations to aid trademark proprietors in shielding their brand names within the gTLD second-level domain name enrolment procedure: the Trademark Claims Service (TCS) and the sunrise stipulations. TCS is the rights protection mechanism described in the Trademark Clearinghouse model located in Module 5 of the ICANN Applicant Guidebook and the final Trademark Clearinghouse implementation model adopted by ICANN as later revised and implemented by ICANN from time to time. As set forth therein, the Trademark Claims Service must include notice to a prospective domain name registrant of a potential conflict between the domain name and an existing trademark and the scope of the rights, with a notice to the trademark owner if the domain name is registered following the registrant's representation of non-infringement[633]. Following the trademark claim service, at least 60 days after a gTLD release for a specified duration, the trademark Clearinghouse will certainly alert registrants whose potential second-level domain name matches their mark in the Clearinghouse.[634] The center commented that the TMCH needs to deal with stakeholders fairly and not obstruct rights holders in dealing with trademark registrations acquired through evaluation and legal registration systems used in numerous international jurisdictions. If and where pertinent, practical steps might be taken to recognise any illegal invocation related to contested rights in particular contexts.[635] Although the Trademark Claim Service is not the best system when combined with the obligatory sunrise arrangements, it may decrease the possibility of extensive violation within registrations of second-level domains. Under the sunrise arrangements, for a minimum of 30 days before the general public launch duration for a new general TLD, the Clearinghouse registered mark can prioritise the right holder to register the domain names that contain his mark.[636]

---

[631] *Frederick M. Abbott, Thomas Cottier, Francis Gurry ,International Intellectual Property in an Integrated World Economy, ibid, p551.*

[632] *domain Name Case Law, Existing domain Name Case Law (harvard.edu), accesses 13/7/2021.*

[633] *https://www.lawinsider.com/dictionary/trademark-claims-service*

[634] *Jennifer C. Wolfe, Anne H. Chasser, domain Names Rewired: Strategies for Brand Protection in the Next Generation of the Internet, ibid, P69.*

[635] *Frederick M. Abbott, Thomas Cottier, Francis Gurry ,International Intellectual Property in an Integrated World Economy, ibid p551.*

[636] *Jennifer C. Wolfe, Anne H. Chasser, domain Names Rewired: Strategies for Brand Protection in the Next Generation of the Internet, ibid, P69.*

1.3 Uniform Rapid Suspension (URS) System

Besides the uniform domain name dispute resolution policy, ICANN offers another mechanism to facilitate dispute resolution. The uniform rapid suspension system mechanism (URS) is a dispute resolution forum. In this context, even though most dispute cases are subject to be resolved through the UDRP rules, using the advantage given by common law trademark claims, besides having a very simple procedural frame, the Uniform Rapid Suspension system can be used only in narrow domains limited in registered trademark holders with very clear infringement claims.[637] The URS is planned to offer an expedited treatment for dealing with clear violation cases versus trademarks. The URS is also developed to provide a faster, more economical tool to prevent violations of rights related to websites. At the same time, the UDRP rules limit treatment to transferring the objected domain name or cancelling it.[638]

ICANN has designed a special tool to meet new domain-name industry challenges and deal with specific second-level RPM cases.[639] However, in a URS case context, once it is shown that a domain was confusingly similar with or identical to an authorised mark currently under usage, and the domain name owner has no natural right or legal interest regarding the objected domain name,[640] the domain name that was enrolled and utilised in bad faith will be suspended in the network resolution. However, it was developed as a fast-track modification of UDRP rules, and URS's effectiveness is yet to be seen.[641] The complainant reports their objection through an allowed URS policy. Moreover, the complainant should pay fees or cancel within 24 hrs of submitting. In this, the complainant has to submit particulars of the objection as laid out in the URS proceeding.

Along with the UDRP rules, three crucial elements must be declared, and all must exist.[642] Despite some similarities with UDRP rules, there are huge distinctions in URS choice, which makes it different from the UDRP rules, particularly in the margin of decisions or choices given upon the legal holder's request. In this regard, the complainant can request not to transfer the contested domain name. Furthermore, the complainant does have an extra choice to extend the registration duration of the suspended domain name in the market area. Another vital difference that would make URS more practical and preferred is an appeal procedure that the UDRP rules still lack, such as this further practical step.[643]

The URS is expected to bring greater accountability of evidence for claimants. The URS likewise consists of various extra registrant defences over an increased duration. The

---

[637] *Frank B. Cross, Roger LeRoy Miller, The Legal Environment of Business: Text and Cases, Publisher Cengage Learning, UK & USA, 11th edition, 2021, p172.*

[638] *Jennifer C. Wolfe, Anne H. Chasser, domain Names Rewired: Strategies for Brand Protection in the Next Generation of the Internet , ibid, P68.*

- Hong Xue, Caveats of intermediary liability in the domain Name System: a review of the ICANN new gTLD right protection measures, ibid p38.

[639] *Frederick M. Abbott, Thomas Cottier, Francis Gurry ,International Intellectual Property in an Integrated World Economy, ibid p551*

[640] *Mark Jeftovic, Managing Mission - Critical domains and DNS: Demystifying nameservers, DNS, and domain names, Publisher Packt Publishing Ltd, 2018 p56.*

[641] *Hong Xue, Caveats of intermediary liability in the domain Name System: a review of the ICANN new gTLD right protection measures, ibid p38.*

[642] *Mark Jeftovic, Managing Mission - Critical domains and DNS: Demystifying nameservers, DNS, and domain names, ibid, p56.*

[643] *ibid p56.*

only other advantage a URS panel might give is that URS provides efficient protection for trademark proprietors versus cybersquatting. The significant distinction between both methods is that the URS is quicker and more economical than the UDRP rules.

Moreover, the URS substantive criteria resemble the UDRP rules. [644] Unlike the UDRP rules, however, which are widely used for top domain name conflict, the URS is mainly utilised for the new gTLD domain names and is intended for short-term suspension of the targeted domain name.[645] Accordingly, the disputed domain name is kept by the domain name registrant.[646]

1.4. Post-delegation dispute resolution procedure (PDDRP)

PDDRP is a preventive mechanism that enables enrolment marks pre-emptively by trademark holders recorded in the Clearinghouse. To this point, the PDDRP is fundamentally made to operate as a higher-level executive device to ensure the registry operators' legal practice and ICANN.[647] Certainly, the PDDRP mechanism's function has levelled secondary administrative liability against trademark infringement by the registry operator.[648]
This tool can be considered a turning point in ICANN's relationship with the registry operators of domain names, shrinking the registry operator's immunity against the other main stakeholders and holding them responsible for their faults . As mentioned previously, the main reason that ignited the conflict between trademark holders and domain name owners was the immunity that registries have against the other main stakeholders.
The committee's experts will determine whether the registry operator is negligent, and they will suggest treatments. In line with this, there are three post-delegation dispute resolution procedures. These kinds of PDDRPs are specifically: The trademark post-delegation dispute resolution procedure (TM-PDDRP), the registration restriction dispute resolution procedure (RRDRP), and the public interest commitments dispute resolution procedure (PICDRP).[649]

1.4.1 Trademark Post-Delegation Dispute Resolution Procedure (TM-PDDRP)

The TM-PDDRP is a procedure that allows a brand holder to impose claims wherever one or more of its brands have been violated by the registry operator's operation or the gTLD usage. Moreover, TM-PDDRP needs proof of the registry operator's particular bad faith or intrigue in brand name violation (i.e., benefiting from motivating violation in addition to the normal registration charge) within the second or first level of a new gTLD. A specialist panel figuring out a TM-PDDRP case might suggest a range of resolutions to ICANN, including cancellations or ending the registry contract.[650]

---

[644] *bid, p 5-99*
[645] *Barney Warf, The SAGE Encyclopedia of the Internet, Publisher SAGE,1st edition, UK & USA, 2018, p263.*
[646] *Ibid, p263.*
[647] *Hong Xue, Caveats of intermediary liability in the domain Name System: a review of the ICANN new gTLD right protection measures, ibid p38*
[648] *Jaani Riordan The Liability of Internet Intermediaries, Publisher Oxford University Press, UK,1St edition, 2016, p 214.*
[649] *Hong Xue, Caveats of intermediary liability in the domain Name System: a review of the ICANN new gTLD right protection measures, ibid p39*
[650] *ibid p39*

In this regard, the registry operator is not responsible under the TM-PDDRP for any domain name registration that is enrolled by an individual or body that is unaffiliated with the registry operator; or is enrolled without the indirect or direct motivation, temptation, initiation, or instructions of any individual or entity related with the registry director; and grants no direct or indirect advantage to the registry. In that case, the plaintiff is required to demonstrate, by convincing and clear proof, that the registry operator is endorsing behaviour, such as there is a certain pattern or practice of particular bad faith purpose by the registry administrator to benefit from the trade of trademark infringing domain names; and that the registry operator has an intent of bad faith to benefit from the organised enrolment of the domain names related to the gTLD that is similar to or comparable with the claimant's mark, which takes unjust benefit of the distinct character or the trade reputation of the claimant's mark; or hinders the distinct character or the reputation or credibility of the claimant's mark; or creates or increases a possibility of confusion with the claimant's mark.[651] Even when the request is completely accepted, the operator might be obliged to monitor enrolments. Moreover, in uncommon conditions where the operator showed bad intent, the contract might be in jeopardy. Aside from the unclear and extremely subjective standards for the documented behaviour, this procedure will charge a liability indirectly against the operator on the gTLD register to force him to control the domain enrolled in their operating system. It will certainly not simply restrict the capability of new gTLD operators. Rather, it might oblige them to take their major responsibilities more seriously by obliging them to monitor the information and track the sites for which the domain name is utilised, as well as the chains of domain names for evidence of good faith and honesty.[652]

1.4.2 Public interest commitments dispute resolution procedure (PICDRP)

PICDRP is an instrument that addresses complaints that a registry operator may not comply with the Public Interest Commitment(s) in Specification 11 of their registry agreement (RA). The public interest commitments dispute resolution procedure (PICDRP) enables complaints against a registry operator that might oppose the Public Interest Commitments (PICs) made in the stipulation of its registry arrangement. The PICs comprise ICANN's obligatory provisions and the registry operator's proposed dedications. After an initial evaluation, ICANN sends the PIC's announcement to the operator and allows 30 days to provide an effort to solve the dispute. If the parties stop settling, ICANN will ask the registry operator to describe how it complies with its PICs.

Furthermore, suppose that the operator does not want to cooperate, or otherwise continues not committing to legal measures made by ICANN. In that case, ICANN will put a determination in force and take remedial procedures. [653] On top of that, anybody can submit a limited public interest objection. Due to the comprehensive position base, complainants undergo a quick vetting procedure developed to identify and remove malicious or foolish

---

[651] *ibid p41*

[652] *Jan Rosén ,Individualism and Collectiveness in Intellectual Property Law, PublisherEdward Elgar Publishing Cheltenham, UK,1st edetion, 2012,P264.*

[653] *Hong Xue, Caveats of intermediary liability in the domain Name System: a review of the ICANN new gTLD right protection measures, ibid p40*

objections. An objection discovered to be misguided or an offense of the right to dispute might be removed at any time. Such unfounded objections will be considered as clear objection right abuse. [654] The objection might be formed to fall within the accepted classifications for limited public interest objection. However, other evidence might later reveal the objection to be illegal and submitted in bad faith. Numerous objections submitted by the associated or same parties against the applicant might constitute harassment of the claimant instead of a genuine defence of legal standards acknowledged under basic concepts of general or international legislation. Furthermore, the objection that assaults the applicant might violate the right of the legal objection.[655]

1.4.3 The registration restriction dispute resolution procedure (RRDRP)

RRDRP is a mechanism intended to cover trademark post-delegation dispute resolution proceedings generally. It addresses a registry operator's complicity in trademark infringement on a New gTLD's first or second level. RRDRP is planned to deal with situations in which the registry operator of a new gTLD related to community interests differs from the registration limitations detailed in its registry arrangement.[656] In this connection, the importance of the RRDRP function is to deal with complaints related to behaviours that cause harm to society or other public characters or individuals because a community-based limited gTLD registry operator did not satisfy its commitments to control and monitor the registration and usage of domain names within the limitations specifically related to the gTLD registry contract.[657] The requirement for such a treatment is based upon the concept that it would not be reasonable and fair to provide a choice in the new gTLD frame allotment procedure to a claimant based upon a dedication to limiting use of a gTLD to specific communities, groups, or other stakeholders or organizations. The registry operator's inappropriate actions may damage public society or members of organisations and other associations.[658]

2. Remedies and Liability

This factor has an important role in resolving the conflict successfully. It observes the level of effectiveness based on consistency of the remedies and accountability. To this point, the author reviews this connection.

Under the TM-PDDRP, PICS, and the PICDRP, the RPMs force the new gTLD registry operators to implement IP rights into their registration policies and services. The question is whether new intermediary accountability is produced in the DNS. The RPMs require the

---

[654] *Ibid P3-6.*

[655] *bid 3 7 .*

[656] *Hong Xue, Caveats of intermediary liability in the domain Name System: a review of the ICANN new gTLD right protection measures, ibid p40*

- Luc Seufer, the next round of gTLDs is around the corner, ibid.

[657] *Joost Pauwelyn, Pierre Véron, Edouard Treppoz, Julie Bertholet, Pierre-Alain Killias, Torsten Bettinger, Bernard Hanotiau, Sarah Theurich La resolution des litiges de propriété intellectuelle / Resolution of Intellectual Property Disputes, Publisher Université de Genève, Genève ,1st edition,2010, http://archive-ouverte.unige.ch, p 56*

[658] *ibid, p 56*

registry operators of new gTLDs to take a certain level of responsibility for the actions related to their domain name registrants. The offered RPMs in ICANN's systems are executed within the DNS frame. The future intermediary liability might affect the international community's benefits and intellectual property enforcement.[659]

According to the trademark post-delegation dispute resolution procedure related to remedies and liability offered by ICANN, and based on the fact that registrants are not an original party subject to actions taken with the originals parties of the conflict, ICANN has declared that the operators generally cannot be subject to the form of 'suspending, transferring or, deleting registrations, except to the extent registrants are directors, officers, employees, agents, or entities under common control with a registry operator.'[660] Furthermore, according to suggested remedies, statutory procedures will not impose any financial sentences to any party except the fees and other costs granted based on the regulations.[661]

Chapter 4: The domain name economy: Domain names' value and their financial impact on domain name conflicts

There is no doubt that domain names have formed a new digital business world equal to the geographical one. Everyone has aimed to gain a share in such a borderless world (cyberspace). From this moment, a public conflict has begun to appear between the stakeholders of cyberspace over contested domain name rights.

1. Background

Although this conflict is taking shape legally, this legal view is hiding severe financial fights. Moreover, when we say there is a financial conflict between the main stakeholders, we mean that profit, loss, and costs come from this conflict. As a result, every legal conflict has its financial equivalent if it can be coded into financial values.

Domain names are the main key to the digital financial community, so the legal conflicts reflecting contested financial rights are important. For instance, it was noticed that potential cybersquatting was one of the reasons that raised the value of domain names. More often than not, the domain name conflict has long been viewed from a legal point of view as just a legal matter without finding a direct connection to the equivalent financial effect of such legal conflicts on the main stakeholders in this industry. Building on this, the author will try to find such a connection by coding the legal conflicts into their equivalent financial value and analysing their financial cost to the economy of the domain name industry.

[659] *Hong Xue, Caveats of intermediary liability in the domain Name System: a review of the ICANN new gTLD right protection measures, ibid p41*

[660] *trademark post-delegation dispute resolution procedure (trademark pddrp) regulation,4 JUNE 2012, article 18, 18.1, https://newgtlds.icann.org/en/applicants/agb/pddrp-04jun12-en.pdf, p 9*

[661] *Ibid, p .*

2. Financial effect of domain name conflict and the financial cost

It was noted that conflicts over domain names emerged throughout the 1990s as e-commerce increased globally.[662] In this context, Melton believes that the registration of domain names will increase conflict.[663] As a result, conflict over domain names would threaten the stability of the domain name industry, and the conflict between main stakeholders would also have a negative financial effect. The instability would also jeopardise investment in the domain name industry. As we can see, any investment needs a stable financial environment.

Although the result is the same, the types of this conflict may take many forms, starting with holding domain names illegally and passing through using domain names to trade certain fake goods[664] without ending at a certain limit. However, it was believed that borderless cyberspace might lead to more types of domain name clashes.[665] This practice, cybersquatting, appears to be one of the instabilities of the domain name industry.[666]

Cybersquatting lowers the return on such investments and systematically decreases firms' rewards for establishing them.[667] Cybersquatting develops with more threats to trademarks from new registration practices.[668] This conflict between the main stakeholders will be exhausting and expensive.[669] Besides the original stakeholders, domain name owners, and trademark holders, another stakeholder will engage in this conflict (UDRP rules). Understanding the potential financial effect can be achieved through the main stakeholders as follows.

2.1 Cybersquatting as the prototype to evaluate the financial effect of domain name conflict over stakeholders

Within this framework, because the economic effect of conflict is hard to count accurately, online business does not have a stated level of profit and loss account alike. As a result, it would be hard to evaluate the economic effect of illegal profit or profit loss for all conflict types. Accordingly, cybersquatting would be used as a prototype of conflict to understand the economic effect of domain name conflict over main stakeholders.

---

[662] *Miller, R. L., Clarkson, K., Jentz, G., and Cross, F. West's Business Law (10th ed.) (Cengage Learning, 2006), 158.*

[663] *Lipton, J. D. Internet Domain Names, Trademarks and Free Speech. (USA: Edward Elgar Publishing, 2010), 3.*

[664] *Miller, R. L., and Hollowell, W. E. Cengage Advantage Books: Business Law: Text and Exercises (6th ed). (Mason, Ohio, USA: Cengage Learning, 2011), 79.*

[665] *Wass, E. S. Addressing the World: National Identity and Internet Country Code Domains. (Lanham, MD: Rowman & Littlefield, 2003), 34.*

[666] *Droit, A. de. Recueil Des Cours/Collected Courses (2000). (Netherlands: Hachette, 2000), 296.*

[667] *United States. Congress. House. Committee on the Judiciary. Subcommittee on Courts and Intellectual Property. (2000). Internet Domain Names and Intellectual Property Rights: Hearing Before the Subcommittee on Courts and Intellectual Property of the Committee on the Judiciary, House of Representatives, One Hundred Sixth Congress, First Session, July 28, 1999. (Washington: U.S. Government Printing Office), 87.*

[668] *Lindsay, D. International Domain Name Law: ICANN and the UDRP. (Oxford, Portland & Oregon: Bloomsbury Publishing, 2007a), viii.*

[669] *Bruce A. Lehman. Intellectual Property in the Global Marketplace. Intellectual Property in the Global Marketplace, 1998. 3, 7.*

To enable understanding of the financial effect of this issue, the legal conflict must be coded into equivalent financial value. In that light, the financial effect of domain name cybersquatting can be seen through illicit proceeds or profit gained by illegitimate contenders at the expense of the legitimate trademark holder on the one hand and loss of profit on the other hand. It is difficult to know the exact amount of illegal profit or of profit loss, due to the business running online and the profits being changeable. Accordingly, this difficulty is considered one obstacle to fair compensation.

In light of this situation, the legal owner will be the biggest loser, due to insufficient protection and the fact that every second costs him unjustified loss. The legitimate owner could end up paying more money to have his domain name returned, because resolving such a conflict would not give the legal party fair compensation. Within this framework, the question arises as to whether the legitimate owner can get back his right to his domain name with fair compensation for his lost profits. This conflict can be handled under UDRP rules or the Lanham Act, based on the nature of the domain names.

2.2 Financial effect of domain name conflict resolution cost under UDRP rules

According to WIPO regulations, this dispute shall be handled under a uniform dispute resolution policy (UDRP).[670] ICANN has also established the UDRP rules' mechanism to solve the conflicts of main stakeholders over domain names' contested rights.[671] The variety of domains moot is extremely small compared to all licensed domains. For example, via the current upgrade (2019), 4,287 .com domain names[672] and 5,578 domain names in general were the subject of UDRP rules in 2019.[673] There are 144 million registered .com domains, so only one in 42,000 .com domains were the subject of UDRP rules that year.[674] With this in mind, one may wonder whether UDRP rules extend to damage claims. Back to UDRP rules, it was concluded that if a trademark-owning lawsuit is effective under the uniform policy, the domain owner loses the right to be the registrant of the contested domain name and, in addition, the domain is transferred to the legal holder of the trademark that started the issue or, conversely, the trademark holder can ask that the domain enrolment be terminated instead.[675] Deeply analysing the legal text indicates that UDRP rules do not extend to compensation or statutory damage.

---

[670] *Lindsay, D. International Domain Name Law: ICANN and the UDRP. (Bloomsbury Publishing, 2007), 451.*

[671] *Halt, Jr., G. B., Donch, Jr., J. C., Stiles, A. R., and Fesnak, R. Intellectual Property in Consumer Electronics, Software and Technology Startups. (Springer Science & Business Media, 2014), 63.*

[672] *World Intellectual Property Organization. (2020).*

[673] *Ibid.*

[674] *Andrew Allemann. Cybersquatting cases at WIPO trending up in 2019. https://domainnamewire.com/2019/10/24/cybersquatting-cases-at-wipo-trending-up-in-2019/*

[675] *Garzaniti, L. J. H. F., and O'Regan, M. Telecommunications, Broadcasting and the Internet: EU Competition Law and Regulation (3rd ed.). (Sweet & Maxwell, 2010), 369.*

- Schwabach, A. Internet and the Law: Technology, Society, and Compromises (2nd ed.). (ABC-CLIO, 2014), 58. Ibid

On the other hand, solving the dispute under UDRP rules entails payment of specific fees. For these purposes, the question arises: What is the financial cost of resolving a conflict under UDRP rules? The answer to the question needs to be between the legal text and the fee amount, because one of the parties might gain illicit profit and the other lose potential legitimate profit. Besides, the potential legal owner might lose the lawsuit despite his legitimate right to the contested domain name. Consequently, the economic effect of domain name conflict resolution will be connected to the amount of loss and profit, and it will be open to the following possibilities.

First, the legal owner of the domain name can get the domain name back. The economic effect of the cost will be limited to the amount of profit loss, which may range between some hundreds and some millions of dollars. In addition, he will be exempted from paying the required fee. However, he will not be able to get fair compensation for illegitimate revenue gained by the other party, who will not pay more than the resolving administrative fee. Another anticipated scenario of the economic effect of resolving a dispute's cost is that the legal owner of the contested domain name would fail to get that domain back. Also, the consequences will not be limited to his lost profit but also extend to anticipated profit, forcing him to pay the required fees. See Figure 7, which shows the potential scenarios.

In this context, the WIPO reports from 2019 indicate that 28 cases have been cancelled, and in 190 cases, the complaint was denied. The number of transferred domain names was 2,426. By applying these scenarios over the number of cases in 2019, the first scenario was applied to 2,454 (2,426 transferred + 28 cancelled), while the second scenario was applied to 190 cases.

Figure 7: The potential scenarios expected to be applied during UDRP rules and the financial value of the cost conflict.

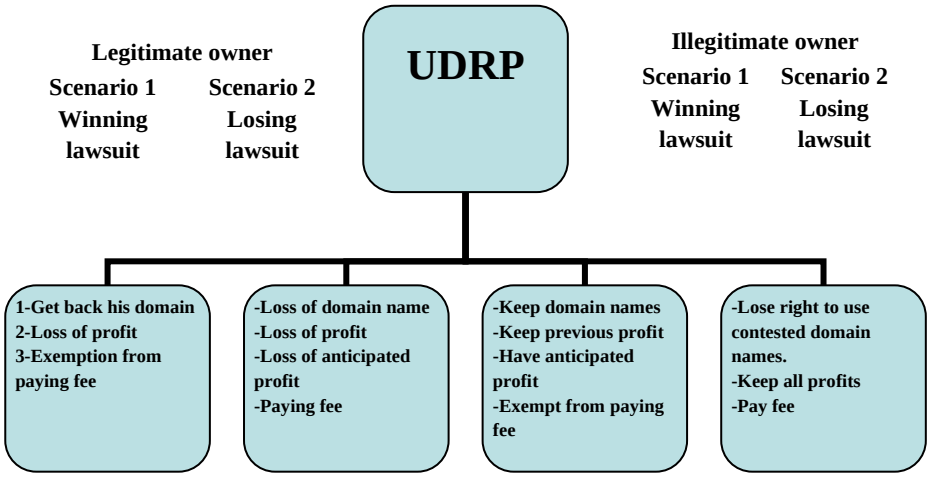


Table 2: Case outcome (consolidated): 2019, source WIPO[676]

Outcome	Number of Cases	Percentage
Cancellation	28	1.06%
Transfer	2426	91.82%
Complaint denied	190	7.19%

Since their establishment, UDRP rules have dealt with roughly 36,283 cases up to 2019. During this period, the WIPO reports indicated that around 31,799 domains were transferred and 3,912 cases had the complaint denied. By applying these scenarios over the number of cases up to 2019, the first scenario would be applied in around 32,311 cases (31,799 transferred + 572 cancelled), while the second scenario would be applied over 3,912 cases (WIPO).

2.2.1 The financial cost of conflict resolution under UDRP rules

Because domain name conflicts can emerge in several ways, the UDRP rules have been developed by ICANN to solve such conflicts related to domain names.[677] Accordingly, the WIPO arbitration centre provides adjudication and mediation services that provide time-saving and inexpensive alternatives to court lawsuits of IP conflicts.[678] According to UDRP rule management, the dispute resolution is conducted by 400 panellists from over 50 regions.[679] On the other hand, the UDRP rules and regulations enforce a responsibility on all panellists to be unbiased and independent.[680] The UDRP rules have determined the cost of an administration fee based on the number of domain names per case and the number of panellists as follows.

2.2.2 UDRP rules' fee

These charges link with any domain name cases launched on or after December 1, 2002. The WIPO Center will carry that out under ICANN management on September 28, 2013. For cases that include between one and five domains, the cost for cases to be decided by a single

[676] *https://www.wipo.int/amc/en/domains/statistics/decision_rate.jsp?year=2019*

[677] *Halt, Jr., G. B., Donch, Jr., J. C., Stiles, A. R., and Fesnak, R. Intellectual Property in Consumer Electronics, Software and Technology Startups. (Springer Science & Business Media, 2013), 63.*

[678] *World Intellectual Property Organization. Report of the Director General to the 2019 WIPO Assemblies (Vol. 1050). (WIPO, 2019), 16.*

[679] *Riis, T. User Generated Law: Re-Constructing Intellectual Property Law in a Knowledge Society. (Edward Elgar Publishing, 2016), 210.*

[680] *Radin, M. J., Rothchild, J. A., and Silverman, G. M. Intellectual Property and the Internet: Cases and Materials. (Foundation Press, 2004), 161.*
- Kaufmann-Kohler, G., and Schultz, T. Online Dispute Resolution: Challenges for Contemporary Justice. (Kluwer Law International B.V.), 47.

panellist is $1,500, and it is $4,000 for cases in which three panellists make the decision.[681] For cases that include between six and ten domain names, the charge for cases to be determined by a single panellist is $2,000, and it is $5,000 for cases to be determined by three panellists (WIPO, n.d.).[682]

Table 3: Schedule of fees under the UDRP rules (WIPO, n.d.)[683]

No.	No. of domain names	No. of panellists	Fee
1	1–5	1	1,500 [panellist: 1,000; WIPO Center: 500]
2	6–10	1	2,000 [panellist: 1,300; WIPO Center: 700]
3	More than 10	To be decided in consultation with the WIPO Center.	
4	1–5	3	4,000 [Presiding panellist: 1,500; Co-panellist: 750; WIPO Center: 1,000]
5	6–10	3	5,000 [Presiding panellist: 1,750; Co-panellist: 1,000; WIPO Center: 1,250]
6	More than 10	To be decided in consultation with the WIPO Center.	

Table 4: Minimum financial cost over domain names (WIPO, n.d.)[684]

Year	219	Financial cost 3d Q 2019	
No. of domain names	5,578	1–2, 732 *minimum domain number * maximum 1 benaltis	2–2, 732 *minimum domain number * maximum 3 benaltis
No. of domain names .com	4,287		
No. of cases	2,723	*$1,500=4,098,000	$10,928,000

2.3 Financial cost of conflict resolution under ACPA

Suppose either both parties in the conflict or just one was not satisfied with UDRP's policy for resolving the dispute. In that case, they might appeal to the court for their rights under the ACPA. This act enhances the Lanham Act (the primary government trademark statute in the United States). It enables a civil cause of action against the bad-faith enrolment of confusingly similar domains or the same or dilutive of unique or well-known marks.[685] According to the Lanham Act (ACPA), the plaintiffs are eligible for legal damages between

[681] *Wegner, H. C., and Poplawski, E. G. Understanding the new patent law: how the changes affect your patent practice and portfolio. (Practicing Law Institute, 2000), 71.*

[682] *WIPO. WIPO Guide to The Uniform Domain Name Dispute Resolution Policy (UDRP). (World Intellectual Property Organization, n.d.). Retrieved January 29, 2020, from https://www.wipo.int/amc/en/domains/guide/#i*

[683] *Ibid.*

[684] *Ibid.*

[685] *Kurtzman, T. The Continued Hijacking and Ransoming of The Domain Name System by Modern-Day Corporate Privateers. (American Association Bar, June 20, 2019). https://www.americanbar.org/groups/business_law/publications/blt/2016/06/cyber_center_kurtzman/*

$1,000 and $100,000 from anybody that 'signs up, merchandises, or utilizes a domain that is the same or confusingly comparable to a distinct mark or that is dilutive of a popular mark, in addition to those who make money from that mark in bad faith' under 15 U.S.C.[686],[687] From the financial point of view, analysing the text code of the ACPA reflects part of the financial cost of $1,000–$100,000 per every single domain name, contrary to the UDRP rules that deal with a range of 1–5 or 6–10 domain names. The financial cost will be between $1,000 and $100,000 per domain name. Suppose domain name cases are applied according to the Lanham Act. In that case, the cost of dispute resolution will range from $80 million to $8 billion, depending on the number of domain names.

[686] *Stewart, G. S., and Weiler, M. S.. Emerging Issues in Statutory Damages. Jones day / Www. Jonesday. Com. (2011, January). https://www.jonesday.com/en/insights/2011/07/emerging-issues-in-statutory-damages*

[687] *Anti-Cybersquatting Consumer Protection Act, § 1125(d). (1999).*

PART FOUR: RESOLVING DOMAIN NAME DISPUTES BY JUDICIAL FORUMS (IN PARTICULAR IN AMERICAN JURISDICTION)

The conflicting parties almost always aim to resolve their conflict far away from the courthouse due to the considerable time and effort involved; besides, going to court is expensive.. Accordingly, the decision to seek a solution via the court is often a last resort. To this point, the author illustrates the conflicts between stakeholders under the court by considering the Lanham Act.

Chapter 1: Domain Names vs. Trademark in judicial proceedings

Based on the information thus far presented, it can be reasonably established that the relationship between the main stakeholders in cyberspace is unstable. Within this general instability, the financial factor is dominant in the conflict between the trademark holder and domain name owner. Before approaching the court, parties have the opportunity to solve the conflict via a preliminary step, incarnated in UDRP rules and ICANN's different mechanisms. The main question then, is whether ICANN's alternative remedies have completely solved the conflict. What must be considered is that, in the domain names industry regulation, the court was intended as the second choice to be used, only if ICANN remedies fail.

In this connection, it is believed that the motivation pushing the stakeholders to the Ccourt system was because ICANN remedies ignored the monetary statutory damage and compensation. At the same time, the judicial policy, among other approaches, offers this option. This chapter will answer whether there is a relationship between the domain names' legal character and jurisdiction. Moreover, the author focuses on the American jurisdiction area. But why the American jurisdiction area in particular? The answer is simple: The courts in Germany, Canada, New Zealand, and the United Kingdom have spontaneously given relief to trademarks against cybersquatting cases using trademark law, sometimes without a requirement of usage or even intent. For instance, a Belgian Court took advantage of a service change. Outside the cybersquatting frame, registering well-known marks have been considered a violation in some countries such as France, Germany, and Italy.[688]

1. Anticybersquatting Consumer Protection Act (ACPA): a new legal framework

The Anticybersquatting Consumer Protect Act (ACPA) became part of federal legislation passed by the American Senate in 1999[689]. Moreover, spontaneously,[690] the ACPA is designed to act in favour of trademark holders against the bad faith of those domain name owners who seek to extract illegal profits from trademark holders. In this context, the

[688] *domain Names and Trademarks, March 5, 2000 https://cyber.harvard.edu/ property00/domain/main. Html #discussion*
[689] *Ibid..*
[690] *Howard B. Rockman, intellectual Property Law for Engineers, Scientists, and Entrepreneurs, Publisher John Wiley & Sons,2nd edition, 2020, Ibid P786.*

umbrella of the Act has extended to include protecting the mark based on personal names.[691] The effectiveness of this act assumes that the trademark has full distinctiveness when the identical confusing domain name has been enrolled. Moreover, this act takes for granted that the mark is well known because the ACPA uses a dilution approach to protect famous brands against domain name owners further.[692]

The ACPA has constructed a road map in the frame of domain name conflict. It gives solid support to the court to deal with bad faith matters, including domain name registration. An industry lobby consisting of trademark holders, in particular, who expressed concerns over traditional trademark law's effectiveness in protecting their rights and interests, successfully forced Congress to pass anti-cybersquatting legislation.[693] Because the New ACPA targets the bad faith matter with the UDRP rules mechanism, some experts argue that the UDRP rules mechanism must be given enough time to practice its mechanism and a chance to bridge the gaps before using the judicial solution based on ACPA.[694] The question that needs further analysis is whether there is any margin of integration or harmonisation between these two mechanisms. Conducting a simple comparison shows that the new act has built over the UDRP rules mechanism and taken further steps beyond it. For instance, the ACPA gave more solid protection to "untrademarked names *in rem* jurisdiction."

Furthermore, besides transferring and cancelling, the ACPA seriously considered the civil remedy's importance as a solution to resolve the conflict. Moreover, it provides monetary compensation ranging from $1,000 to $100,000 per every name violation.[695] The ACPA also gives the registry authorities an immunity against any responsibility for lost profit concerning the enrolment or upkeep of the domain name unless there is a proving of bad faith purpose to gain from such enrolment or upkeep.[696] In the same context, the question can be discussed oppositely whether the UDRP rules could have the chance to develop themselves by benefiting from ACPA tools. It is worth imagining if the UDRP rules could adopt the ACPA tools approach, particularly having monetary damage as ACPA; certainly, the UDRP rules would effectively protect the stakeholders' rights, particularly those of the trademark holder. Moreover, there is the concern that other states may enact similar legislation, with the possible result that domain name registrants will be subjected to multiple jurisdictions with different laws.[697]

On top of that, if one of the main stakeholders locked a mark and did not wilfully register it to prevent the other stakeholder from registering this mark or name as a domain name, can ACPA treat this case? In real practice, the judicial system deals with this case; for instance, the US District Court for the Middle District of Florida heard the case of*Davies vs. Afilias Ltd*[698] over the registry for the domain name *hotel.info.* . As mentioned by the Court,

---

[691] *Ibid P786.*

[692] *Ibid P786.*

[693] *domain Names and Trademarks, ibid March 5, 2000*

[694] *Ibid.*

[695] *Richard A. Mann, Barry S. Roberts, Essentials of Business Law and the Legal Environment PublisherCengage Learning, 13 edetion 2018, P 834.*
- Thronson, Roth, Grossman ,intellectual Property Legal Opinions, Publisher Wolters Kluwer new york,2Nd edition, 2020, P9-38.

[696] *Richard A. Mann, Barry S. Roberts,*

[697] *domain Names and Trademarks, March 5, 2000 ibid.*

[698] *US District Court for the Middle District of Florida - 293 F. Supp. 2d 1265 (M.D. Fla. 2003) December 2, 2003*

the complainant enrolled the contested domain name with an affiliates-authorised registrarConsequently, the opponent Afilias realised that the plaintiff did not possess the trademark legal rights and 'locked' the names to prevent the other party from using them. The Court of Appeals dismissed the complainant's claim based on an ACPA violation. Moreover, the plaintiff did not take legal action against the mark holder who locked his name.[699] Rather than that, he took legal action against the registry, which desires to offer untrademarked names fairly to the public under its procedures. Furthermore, this act did not limit dealing with bad faith matters but also included other issues of domain name disputation, such as dilution and confusion. In this correlation, whether the judicial system could effectively deal with these threats to domain names and other related trademark rights in cyberspace arises. Answering this question needs to explain the conflict grounds over contested domain names.

2. Conflict ground according to the ACPA (dilution and confusion)

According to the Lanham Act, the ground of conflict between the main stakeholders in cyberspace acquired different areas of conflict, including confusion and dilution.

2.1 Confusion

Besides cybersquatting and its peer, reverse domain names hijacking, a new rule of conflict has emerged in tandem with increasing commercial use of the world wide web and new ways of profiting from domain names. More legal challenges have existed with these new shapes of conflicts, and legislative solutions have been found through the American Lanham Act. This act paid much attention to cybersquatting, which may be relatively easier to deal with than the other foundations in which the dispute between the trademark and domain names was classified. In this term, the ACPA has established a new role of dispute frame based on confusion and dilution. In terms of confusion, the intrusion of a trademark happens when an individual without authorisation employs an indistinguishable or very similar brand likely to mislead or deceive. Additionally, encroachment happens if a substantial number of otherwise judicious buyers are likely to be misled or confused about the source of the merchandise. In choosing whether infringement has happened, the Courts consider different components, measuring the quality of the trademark, the aim of the unauthorised client, the degree of similitary between the two marks, the connection between the two items or services, the marks distinctiveness, and the promoting channels through which the merchandise or services are obtained.[700] As the basis of the dispute, it is not limited to registering the domain name to sell it to the trademark owner. It is enough that it has resulted in customers' confusion and reduced the value of the registered trademark as a domain name.

On the other hand, it became clear that the Lanham Act considered those foundations that would be the reason for such a dispute should be stipulated explicitly. This chapter analyses the new rules based on the courts' decisions and their legal and financial effect on the main stakeholders. Moreover, some issues need to be addressed, such as detention, domain name confusion, geographical territory, and the main standards that indicate confusion.

---

[699] *Henry H. Perritt Digital Communications Law, Publisher Wolters Kluwer , New York 2nd edition, 2021, p7-236.*

[700] *Richard A. Mann, Barry S. Roberts, Smith and Roberson's Business Law, Publisher Cengage Learning, ,16 edetion2014,p863.*

2.1.1 Confusion definition and criteria

Confusion's essence is presented in misleading the consumer resulting from the registration of a domain name in a similar manner or conformity with a trademark so that such mixing may affect the mark and cause a loss of consumer focus in making decisions.[701] In this term, the legal protection of trademarks and domain names is given under the unfair competition principle despite the absence of confusion regarding the service or items.[702] The main question that arises here is how the confusion can happen. Answering this question entails researching the criteria to be considered for confusion.

Many criteria can be taken into account by courts to determine whether confusion has occurred and proved a trademark's violation. However, the most important criteria are the extent of the similarity of the domain name to the trademark, the extent to which the trademark is known, and the ability to prove confusion.

2.1.2 The extent of the similarity of the domain name to the trademark

One of the most subjective criteria related to the confusion is how the domain name is similar to the trademark. In this context, the court considers the extent to which the registered domain name is similar or identical to the trademark, which may confuse the consumer, especially in certain usages, e.g.[703] "Whoever knowingly uses a misleading domain name on the Internet to deceive a person into viewing material constituting obscenity shall be fined under this title or imprisoned not more than two years or both."[704]

In US trademark law, confusing resemblance entails more than a simple likeness between visible and aural features.[705.] Substantially, it needs an examination into the most likely recognised significance of the marks. Moreover, the interpretation of the definition is not simple. In particular, similarity and confusion should be evaluated through the eyes and ears of typical consumers, not legal professionals or semanticists. For instance, are the marks GULP and also GULPY confusingly comparable? We would end their confusing similarity if we contrasted the look and the marks' sound. Nonetheless, when considering the marketplace context of using the marks, we might conclude that the definition point of the confused resemblance trilogy in trademark legislation has been removed from the confusion resemblance evaluation under the UDRP rules[706].

The author believes that despite the marketplace playing a crucial role in judging confusion, it also needs to consider that customers, by and large, are not experts and can be naive. Contrary to professionals, many consumers only care about getting the product or service, no matter the mark. This confusion might harm this market rather because most

---

[701] *Gilbert, Irwin & Harley S Tropin. LexisNexis Practice Guide: Florida Business Torts (New York, USA: LexisNexis, 2020). Irwin Gilbert, Harley S Tropin, LexisNexis Practice Guide: Florida Business Torts, , LexisNexis New York, USA, p 9-68.*

[702] *Morton F Daller, Business Torts: A Fifty-State Guide, 2020 Edition (IL), Wolters Kluwer Law & Business, New York 2019, p 467..*

[703] *Roger LeRoy Miller, William E. Hollowell, Business Law: Text & Exercises, Cengage Learning, USA 9th edition, 2018, P 72.*

[704] *18 US Code § 2252B.*

[705] *Roberto Moro-Visconti, Startup Valuation: From Strategic Business Planning to Digital Networking, PublisherSpringer Nature,swiszirland, 1st edition 2021, p86*

[706], *Christine Haight Farley, Confusing the Similarity of Trademarks Law in domain Name Disputes ibid, p621.*

customers depend on search engines to deliver these products or services. Besides that, it is not the mission of the customers or the buyers to analyse if the gulp or gulpy has a different meaning according to market facts.

The essence of the ACPA is to prevent registering or using a domain name that may dilute the values of a famous mark or cause trademark confusion.[707] The complaint is often based on the margin of bad faith, confusion beyond the domain name, and similarity to the questioned trademark. On top of that, the domain name in dispute has no legal rights. It is vital to enable all main stakeholders to prove malicious behaviour and legal rights. Therefore, the focus is not on confusion, dilution, or any harm to the public or brand owners as the main goal. The focus is the malicious intent of the registrant.[708] For practical instances of bad faith behaviour, it will be noted that the defendant enrolled the domain name to mislead customers away from the plaintiff's website to another site, or the litigant owns many domain names that are highly identical or confusingly similar to well-known marks.[709] In this regard, the matter of fame is decided by estimating all related circumstances, including the scope of real realisation of the mark and the extensive usage of a domain name that is identical or confusingly similar to a distinctive trademark, including individual names.[710]

The trademark proprietor might run a domain online instead of common trade ruled in a geographical area. However, particular proprietors have participated in various market industries. One instance presented in a case at the Court of Virginia, *Roadrunner Computer Systems v. NSI Inc*[711], to answer the critical question of whether the domain name's top suffixes as a common term can create a trademark with full protection.[712] The Virginia Court indicated that the trademark registration criteria could not be separated from the essence of the mark to the relevant consumers[713]. The Virginia Court supported registering domain names with generic terms added to the top-level suffix in several events and considered it legally registerable.

Moreover, the mentioned court has no longer ruled that incorporating a common term with a high-level domain name *.com* always produces a common compound, irrespective of the customer's belief. Besides that, the Supreme Court of The United States justified this decision by indicating that only one entity can inhabit a specific online domain name at once, as in the case of *USPTO v. Booking.com B. V, 140 S. Ct. 2298 (2020); David Byer & Eric W. Lee, U.S.*[714] On another occasion, the court emphasised that the possibility of confusion must be established even if competition is related to the same products. The court denied the trademark violation based on the domain name goods' competition with the trademark holder goods. On top of that, the Court considered the post suffix added to the domain name *http://wmv.fredsbeverages.com/pepsicola* did not violate the famous trademark Pepsi-Cola

---

[707] *David P. Twomey, Marianne M. Jennings, Stephanie M Greene, Anderson's Business Law & The Legal Environment - Comprehensive Edition, Publisher Cengage Learning, 2021, p169.*

[708] *Christine Haight Farley, Confusing the Similarity of Trademarks Law in domain Name Disputesibid, p613,*

[709] *Irwin Gilbert, Harley S. Tropin, LexisNexis Practice Guide: Florida Business Torts, p 9-68*

[710] *David P. Twomey, Marianne M. Jennings, Stephanie M Greene, Business Law: Principles for Today's Commercial Environment, ibid, p 160.*

[711] *Trademark Law in cyberspace - The Battle for domain Names(*) Torsten Bettinger IIC - International Review of Industrial Property and Copyright Law - Volume 28 No. 4/1997, p. 508, Torsten Bettinger, p111.*

[712] *Shilling, Lawyer's Desk Book, 2nd Edition, Publisher Wolters Kluwer, 2018 p10-52-53.*

[713] *ibid p10-52-53*

[714] *ibid p10-52-53*

because the post domain suffix aims to organize files within an online server[715](*see "Interactive Prods. Corp. v. a2z Mobile of fice Solutions, Inc., 326 F.3d 687 (6th Cir. Corp. v. a2z. Mobile Office Solutions, Inc., 326 F.3d 687 (6th Cir. 2003).*

Among other approaches, the confusion criteria determine the degree of similarities between domain names and trademarks to be investigated; accordingly, among other factors involved in determining the domain names confusion, the mark's distinctiveness, the time that the trademark was in use, the level of the mark's fame, and the nature of the services and products used under the mark umbrella[716].

2.1.3. Offline trademark confusion vs. online domain names confusion

When considering the relationship between domain names and trademarks, it must be remembered that the trademark is often connected to a geographical area. In contrast, the domain name's scope is related to cyberspace which is free from borders. On the other hand, one of the main keys to the confusion related to trademarks is the scope of products or service similarities. Accordingly, in its decision, the English tribunal supported a lawsuit introduced through the proprietor of the KODAK mark for cameras in opposition to another party using the identical slogan to sell bicycles in 1898.[717] The concern is whether a trademark holder can restrain the use of the mark on noncompeting products. One hundred years earlier, an English cycle maker, Griffiths, started to sell Kodak bikes. Kodak was, since that time, a well-known trademark possessed by the Eastman Business and registered for cameras and photographic products.[718]In this case, the judge based his decision on the fact that the two types of these companies' products created real confusion. The defendant's opportunistic use of the mark and the possibility of damage to the plaintiff's mark's reputation and distinctiveness would be adequate grounds for legal action. Nevertheless, in 1898, Judge Romer J's decision indicated that the registered trademark was not infringed upon by any use of the mark outside the registration parameters under the Trade Marks Act, which was in effect at the time. The judge set up his decision based on two possible causes of action, including infringing on a registered trademark and common law liability for passing off, which had constituted the foundation of the case[719]. The importance of that case is that,[720] according to the judgment, doing business under the established similar contested mark would give an undue advantage.[721]

The confusion that may be happening in the consumer's mind when deciding because of the strong similarities between the two brands has been affirmed in the case of *Veuve Clicquot Ponsardin v. Boutiques Cliquot Ltée*. In this case, the Court investigated the correlation between the senior mark in use and junior goods. Furthermore, finding such a connection is

---

[715] *ibid p10-52-53*

[716] *, Christine Haight Farley, Confusing the Similarity of Trademarks Law in domain Name Disputes ibid, p615.*

[717] *Michael Karanicolas, The New Cybersquatters: The Evolution of Trademark Enforcement in the domain Name Space, Fordham Intellectual Property, Media and Entertainment ,ibid, p 408.*

[718] *dawson, n. m. "trade mark law and the creation and preservation of well-known brands." northern ireland legal quarterly, vol. 49, no. 4, winter 1998, pp. 343-362.p351*

[719] *ibid.p351*

[720] *ibid, p 408.*

[721] *ibid, p 408.*

crucial to find real confusion.[722] Moreover, the fame factor's extent is vital in determining confusion processes. For this, in the case *Mattel, Inc. v. 3894207 Canada Inc. The* Supreme Court of Canada considered the mark's scope in its decision of mark infringement based on confusion.[723] In this context, the correlation between the offline geographical world and the online borderless world is present because of the interlacing elements of the two worlds. In other words, the increasing use of cyberspace combined with the fact that trademarks became the main components of domain names raised legal challenges regarding infringing these elements in cyberspace within confusion and dilution grounds.[724] Moreover, there is confusion over the specific product category to which the brand belongs and the jurisdiction in marketing.[725]

For instance, there is supposed to be no dispute between firmsholding the brand name *Delta* and various other *Delta* businesses in multiple sectors, such as *Deltabank*, *Deltairlines*, or *Deltahotels* because the possibility of such confusion between these entities is not expected. Furthermore, there are not, nor have there ever been, reliable systems to deal with conflicts between these two entities that have contending genuine claims to a domain name. Moreover, as an outcome, the common legal norm of the first-come, first-served principle is still in use. This is bearing in mind that only one trademark in cyberspace can be carried out by one domain name in the digital world, for instance, *HotelCalifornia.com*[726.]

Usually, the courts in the United States have sought to resolve trademarks and domain name conflicts related to trademark rights based on confusion grounds according to the subjective fact presenting that the internet browser customers suppose the .com string after the corporation name will send him directly to the home page related to the domain name.[727] In this connection, the question arises of how confusion could happen with domain names. Should there be any commercial activity to make confusion happen? It is different in cyberspace, even though commercial activity is expected to be a vital issue in terms of confusion. Moreover, it is expected that deliberately confusing behaviour could be present if the user finds difficulties reaching the targeted web page because of similarities between domain names. According to section 1114, the Lanham Act did not stipulate that the defendant's commercial activity should decide confusion. In this practical example, the *United States District Court for the Southern District of New York* declared confusion in *Planned parenthood federation of America Inc v Bucci,* where the plaintiff was a charitable organisation interested in advising about birth control on its website. ACPA forbids "registering confusing enrolled or nonregistered mark or dilutive of a well-known mark in bad faith to intent profits."[728]

Furthermore, bad faith matters can be considered if the individual intends to draw away customers from the mark proprietor's online location to a website under the domain

---

[722] *Ibid, p 408.*

[723] *Michael Karanicolas, The New Cybersquatters: The Evolution of Trademark Enforcement in the domain Name Space, Fordham Intellectual Property, Media and Entertainment , Ibid, p 408.*

[724] *ibid p 411.*

[725] *ibid p 411.*

[726] *ibid p 411.*

[727] *Ibid, p 414.*

[728] *Thronson, Roth, Grossman, Intellectual Property Legal Opinions, ibid, p9-35.*

- Howard B. Rockman Intellectual Property Law for Engineers, Scientists, and Entrepreneurs ibid, ,p688.

name. It can damage the good reputation stood for by the mark. Bad faith can be considered if someone acts for commercial profit or intends to taint or slander the mark by developing a chance of confusion, likely regarding the website's resource, sponsorship, association, or recommendation. While the numeric character of internet language is aimed to prevent confusion by allocating one domain name of its kind in cyberspace[729] , interlacing relationships and interaction between semi-similarities of domain names from one side and products, services, or goods' trademarks that related to these domain names from other sides have kept the door open for confusion possibilities in cyberspace.

2.1.4 Generic top-level domain Names and Confusion

In that context, the UDRP's confusion approach might differ slightly from the confusion approach under the trademark law.[730] In this regard, examining the confusion based on the similarity criteria is usually conducted according to the visual comparison of the domain name to the questionable trademark.

Based on the rooted legal rule, a trademark cannot be identical or similar to another mark based on the reasonable outcome of confusion.[731] Despite the clear effect of the new gTLD released by ICANN, there is doubt in the domain name industry regarding the colossal effect of the new gTLD program over confusion in cyberspace's domain names. In this regard, Christine Farley's point of view indicates that the new gTLD will lead to a new level of dispute where the new suffix plays a crucial role based on confusion.[732] Besides unfair competition, consumer confusion was usually the basis for establishing trademark infringement rights[733]. As the main principle found in the American Trademark Act, section 14(2)(1) indicates that making use of an indicator that is the same as a trademark can be banned if the services and products provided under such an indication are the same as those for which the trademark is shielded[734]. The UDRP rules mechanism excluded domain name suffixes from the equation of confusing similarity[735]. This approach raises the main question of the new gTLD program suffix that would be important to resolve confusion in domain names of cyberspace.

2.1.5. Criticism suffix vs. free speech right

The new gTLD program related to the new suffixes has added crucial players in conflict over disputed domain names and trademarks and opened the door to new issues. For instance, there is much debate about whether registering domain names with suffixes related to criticism is set under free speech as one of the fundamental human rights or goes beyond the

---

[729] *Elizabeth R. Leggett, Digitization and Digital Archiving: A Practical Guide for Librarians, Publisher Rowman & Littlefield, London, new York ,2nd edition, 2021, p 143.*

[730] *, Christine Haight Farley, Confusing the Similarity of Trademarks Law in domain Name ibid, p615.*

[731] *Frank B. Cross, Roger LeRoy Miller ,The Legal Environment of Business: Text and Cases, ibid,,p 355.*

[732] *, Christine Haight Farley, Confusing the Similarity of Trademarks Law in domain Name ibid, p609*

[733] *theodore l. banks frederick z. banks, corporate legal compliance handbook, wolters kluwer , new york.3rd edition2021,p 9-33.*

[734] *Trademark Law in cyberspace - The Battle for domain Names, Torsten Bettinger IIC - International Review of Industrial Property and Copyright Law - Volume 28 No. 4/1997, p. 508.*

[735] *, ibid, p609.*

infringement of trademark rights. In this context, the United States Court of Appeals has experienced this issue related to the dispute over a domain name that included a critical suffix to the domain names. In this context, the court commented on the case *Mishkoff vs. Taubman*, indicating that Taubman's mark embedded in the *taubmansucks.com* domain name is justified under the principle of free speech.

However, the court attempted to balance using the first amendment that grants protection to commentary criticising other businesses with the caveat that there is no possibility of confusion. In this case, the court believes that it does not appear proper to use human rights decided by the constitution as the sole criteria to decide this case as long as it is related to a domain name dispute on the one hand. Such a dispute goes beyond the applicable laws within the national borders of the state, on the other hand[736].

Furthermore, the court considered that applying this law in such a case would lack freedom and fail litigation. Besides, it would cause concern for foreign parties[737]. Consequently, the court has established a new frame for dealing with such cases concerning the interlocking of national and international rights in disputed domain names. Moreover, the court called for the solution of the conflict of regulation based on the global governance arrangements and for full integration with these. This context calls for the regulation in those circumstances to be consistent with legal guidelines as a new substantive norm[738].

2.1.6. Domain name confusion according to "gripe site."

Often, it is quite simple to set up an infringement case based on confusing resemblances. Further, according to this effective factor alone, just a few instances are expected to be rejected. Accordingly, the evaluation should compare the complainant's mark and the concerned domain name.[739] In some instances with a pejorative phrase, for instance, concerning *www.fuckcalvinklein.com*, UDRP panelists decided there was no 'confusing resemblance' because the derogatory word indicated that the domain was not connected with the trademark. In the case of *www.fuckcalvinklein.com*, the UDRP panel indicated that the litigant's domain name is not confusingly comparable to the complainant's Calvin Klein mark under UDRP rules 4(a)(i) because the term *fuck* shows that the respondent is not associated with the complainant and that internet users accessing the domain could not possibly assume the complainant to be associated with such a derogatory domain name[740].

Nevertheless, the global nature of the internet admits various exceptions, among other legal and technical challenges. In this regard, the relationship between the so-called 'gripe sites'and confusion[741]. leads to several questions that need to be answered. For example, who is the populace that might be expected to be confused by the domain name? It is assumed to be any specific regional, ethnic, religious, or political group within the one-state borders. The matter has risen expressly over these 'gripe sites,' which ostensibly aim to express

[736] *Poul F. Kjaer The Law of Political Economy: Transformation in the Function of Law Publisher Cambridge University Press,uk,1st edetion 2020, p369.*
[737] *ibid, p369.*
[738] *Poul F. Kjaer The Law of Political Economy: Transformation in the Function of Law ibid, p369.*
[739] *Douglas A. Rettew; Jonathan Uffelman, Maximising Success in UDRP Complaints World Trademark Review,ibid.*
[740] *Ibid, p38*
[741] *Akash Kamal Mishra, Intellectual Property Rights in cyberspace, Publisher Notion Press1st edetion, 2020 p67*

dissatisfaction against famous companies and people or product quality[742]. In this context, the case seems simple if it is explained, for example, that averagely educated American citizens would not be expected to feel confused by *walmartsucks.com*, such that they would believe would drive them to an official Walmart site. Still, the case would be more complicated if related to foreign citizens or non-English speakers. For instance, there is more possibility that Japanese or Chinese people will be victims of the confusing similarities between *walmartsucks.com* and *walmarts.com*.[743]

The effect of this case is not limited to such expected confusion, or the expression of the dissatisfied customers of their bad opinion toward those companies' policies, behaviours, or products. It also extends to consideration of harm to the reputation of those companies or individuals' brands and trademarks when such a 'gripe site' domain spreads publicly. Hence, most of these companies have usually established an internal process to receive complaints about their policy or products and deal with them discreetly to protect their trademark from reputational damage or defamation. In this context, the courts took a different path. It considered that if the domain name is dedicated completely to expressing the dissatisfaction of the user, the consumer, or the customer over the product trademark or the company policy, then their unauthorised use of the trademark does not establish bad faith, including a purpose to gain benefit[744].

The author believes these cases must be established based on more advanced approaches because the possibility of confusion is highly affirmed irrespective of bad faith investigation or the attempt to gain benefit beyond registration, such as this identical domain name that includes a gripe site suffix. In this context, confusion must be established based on defamation. This new approach supports the point of view that any complaints or expression of dissatisfaction expression must be conducted within the internal complaints policy of the companies concerned. Hence, the court must decide the confusion based on defamation even if the domain name owner behaved well. What supports this view is that the confusing registered domain name effect is not temporary; rather, it extends beyond time into creating lasting negative beliefs in customers' minds about the company brands or products. Furthermore, new and prospective customers often base their decisions on existing customers' feedback, which may lead themto buy or reject those brands' products or services.

Contrary to this opinion, the US Court of Appeals for the Eleventh Circuit considered that registering and using a domain name identical to a trademark is inadequate to prove confusion, especially of a weak trademark, as seen in *Planetary Motion, Inc. v. Techsplosion, Inc.*, 261 F.3d 1 188 (11th Cir[745]. Nevertheless, according to ICANN's latest gTLD suffixes, the added info presented by the suffix will probably be considered more than just an extra phrase. It might be perceived as a title for the website's content connected with that domain. As an outcome of this new perception, the evaluation will approximate the possibility of the confusion criterion[746]. The practical application of this approach will lead to different results

[742] *dana Shilling, Lawyer's Desk Book, 2nd Edition, Publisher Wolters Kluwer, 2018 p10-52-53*

[743] *Akash Kamal Mishra, Intellectual Property Rights in cyberspace, ibid, p67.*

[744] *Shilling, Lawyer's Desk Book, 2nd Edition, ibid p10-52-53 .*

[745] *Ibid,p10-52.*

[746], *Christine Haight Farley, Confusing the Similarity of Trademarks Law in domain Name Disputes ibid, p620.*

in confusion evaluation. For instance, according to these new criteria, *delta airlines* vs. *Delta Faucets* would be deemed similar[747].

In trying to conduct a deep analysis related to the mentioned criteria, Dana Shelling, goes beyond the classic idea that constructs the confusion based on criteria of similarity. asserting that the use of another party's trademark after the main domain name, within the URL (e.g., http://www.fredsbeverages.com/pepsicola) cannot be established as trademark infringement, regardless if the new domain name involves any level of competition related to the same category of products or services[748]. In this context, Shelling cast doubt if this suffix or any extra phrase could confuse consumers regarding the source of these products or services, since the post-domain-name portion is a standard feature of online servers' file organisation. The US Court of Appeals for the Sixth Circuit judged in 2004 that using another party's mark in the domain of a gripe website (a website consisting of negative comments regarding a service or product) does not, on its own, comprise a behaviour based on bad faith incuding to gain revenue from such conduct[749]. On the other hand, incorporating such words has improved the opportunity for confusion when the registrant has included common words that refer to business carried out under the complainant's same brand mark. As an example, in the Case No. D2001-0110 *Ansell Healthcare Products Inc. v. Australian Therapeutics Supplies Pty., Ltd.,* WIPO Arbitration and mediation center's administrative panel indicated it was confusingly comparable to the mark ANSELL because "the term defines the complainant's items, and the enhancement of 'prophylactics' [was] likely to enhance confusion." The confusing resemblance was reviewed just in the second-level section of the domain. When considering whether the domain name is 'confusingly comparable' to the guarded mark, the concern is the possible influence of the gTLD suffix. Historically, UDRP rule instances have looked largely at the second-level section of a questioned domain. UDRP rules panelists might not overlook the gTLD in assessing the confusing resemblance of the tested domain name. There is much less cause for the general public to think that, for example, Mercedes-Benz owns any of these domains. However, various other panels with comparable realities have concluded that the info within the gTLD suffix increased the resemblance in these last circumstances. For instance, a UDRP panel considering a confusing likeness to the PORSCHE Trademark concluded that the customer 'might consider that the complainant is making Porsche trademarked automobiles.[750.']

Traditionally, under judicial and UDRP rules administrative approaches, the ACPA and UDRP's evaluation, panelists, and courts have disregarded the high-level domain name in the likelihood of confusion[751]. The fact that the top-level suffix is just a mandatory element for registration would usually be ignored under the investigation cases of confusing similarity, but in special circumstances where the appropriate suffix may constitute part of the trademark will be considered. On top of that, top-level domain indicators generally add nothing to the distinctiveness of the appellation as a trade or "service mark."[752] The author

---

[747], *iibid p620.*

[748] *dana Shilling. Lawyer's Desk Book , Wolters Kluwer Law & Business (2nd ed.) (2021). New York, p10-52*

[749] *Ibid , p10-52*

[750], *Christine Haight Farley, Confusing the Similarity of Trademarks Law in domain Name Disputes ibid, p620.*

[751] *Stephen F. Reed, Entrepreneurship Law: Cases and Materials, Publisher Wolters Kluwer Law & Business, 2nd edition,2021, p148*

[752], *Christine Haight Farley, Confusing the Similarity of Trademarks Law in domain Name Disputes ibid, p620, note no 47*

agrees that a top-level domain indication cannot distinguish the sources from each other, and therefore, has no trademark importance. Such a top-level domain indicator cannot serve any trademark purpose in distinguishing.

Furthermore, according to the experts, the non-distinctive modifiers used in domain names are unimportant, such as 'http://www' and 'HTML.' Ordinary people who are familiar with using the web are aware of the format of a domain name and know that the classes of the ' HTTP,' 'www,' and a TLD like '.com' are included in all domain names and, thus, based on this opinion the functions of the TLD component '.com.' in the borderless World Wide Web is just a generic indicator comparable to 'Inc.,' 'Co.,' or 'Ltd.' in the geographical company chain. In this regard, the courts traditionally have ignored the domain names' upper portion when it comes to investigating the confusion possibility in terms of conflict between domain name owners and trademark holders based on confusion criteria such as .com, .net, or .org. [753]

2.1.7. Cybersquatting and Confusion

Cybersquatting was the first extensive intellectual property infringing use of the domain name and covers circumstances where the enrolment and use of a domain are confusingly similar or the same as a third party's trademark[754]. In the cybersquatting case under the ACPA, 'confusion' indicates that the complainant's mark and the opponent's domain name are comparable in insight or meaning. [755] Under section 43(a) of the Lanham Act, trademark violation and unfair competitors are characterised as the false designation of sources and false marketing under section 43(a) of the mentioned act. The act is frequently a crucial basis for Internet domain match claims. The probability of confusion is the keystone for unfair competitors and trademark infringement.138 Because the legal scope of protection of a trademark versus violation by others is specified as a "probability of confusion," a trademark holder has a property right insofar as is essential to avoid client confusion regarding who produced the items and (2) to help with the distinction of the trademark owner's products. When the web domain name holder is utilising the domain name to confuse customers [756]. Suppose the letter string of the domain name is similar to the trademark. In that case, it will be examined to determine similarity confusion. For instance, in the case *Harry Winston Inc. and Harry Winston S.A. v. Jennifer Katherman*[757], the WIPO panel ignored the reaction of users and the marketplace factor. The traditional rule in the dispute's first generation adopted the gTLD neglection approach to evaluate the confusion possibility. However, this rule was sometimes broken. On one occasion, it was judged that the suffix added to the domain name was confusingly similar in the case *Limited v. Mat Feakins*[758]. The WIPO panel justified the decision because the gTLD considered confusion process analysis[759]. In Intermatic

---

[753] *ibid, p620, note no 47*

[754] *Susy Frankel, The Object and Purpose of Intellectual Property ,Publisher Edward Elgar Publishing, 2019,P290*

[755] *, Christine Haight Farley, Confusing the Similarity of Trademarks Law in domain Name Disputes ibid, p623.note no 60.*

[756] *g. peter albert, jr., right on the mark: defining the nexus between trademarks and internet domain names, 15 j. marshall j. computer & info. l. 277 (1997),p297*

[757] *WIPO Case No. D2008-1267, Complaint Denied, § 7 (Oct. 18, 2008), https://www.wipo.int/amc/ en/domains/decisions/html/2008/d2008- 1267. html [https://perma.cc/SE7J-N4Q2]*

[758] *WIPO Case No. DCO2013-0017*

[759] *Christine Haight Farley, Confusing the Similarity of Trademarks Law in domain Name Disputes ibid, p632.*

v.Toeppen, the Court held that registering a domain name with the intent to sell the domain name is sufficient to establish commercial use under the Federal Trademark Dilution Act[760]. In the case of Australian telecom, Telstra specified that a "TLD suffix might not generally identify a domain from the questionable trademark, on the principle that the gTLD suffix normally should not be thought about or influence the confusion similarity analysis, given the existence of technical factors." The WIPO panels concluded the domain name to be similar to the plaintiff's trademark Marriott as an outcome. These panels have overemphasised the relevant principle. Because they create components of the mark or associate with the mark proprietor's company, it is no longer the situation that gTLDs are unrelated to a confusing similarity evaluation. Panels restrict their recommendations to the issue at hand. With new gTLDs released into the market, domain name registrants face a severe lack of predictability in UDRP rules[761] .

2.2 Domain names dilution

The Federal Trademark Dilution Act of the United States defines dilution as the lessening of the capacity of well-known marks to identify and distinguish services and goods, regardless of the presence or absence of competition between the famous mark holder and other parties; or the likelihood of confusion, mistake, or deception. This statute provides for claims against non-competing and non-confusing uses which diminish or dilute the effectiveness of the mark's distinctiveness.

A dilution theory may also be appropriate or necessary when the site's content denoted by the domain name is utterly unrelated to the trademark allegedly infringed. Congress has provided a Federal remedy to deal with these situations[762]. The Federal Trademark Dilution Act of 1995 provides remedies for the dilution of 'famous marks.' It is designed to protect marks against diminishing their 'marketing value.' The Lanham Act amendment provides remedies for the dilution of 'famous marks.' Under dilution section 43(c) of the Lanham Act[763],several factors are to be considered, such as whether a mark is famous, the degree of distinctiveness, the duration and extent of use of the mark concerning goods and services or advertising and publicity, and the level of recognition of the mark in the areas of trade in which infringement is alleged.

One crucial component of the Trademark Dilution Act is that competition between the parties or evidence of the possibility of confusion are unnecessary in dilution[764]. Considering the statute's enactment, numerous Internet domain name cases have been filed charging dilution under the law. Numerous points are apparent concerning the Trademark Dilution Act, which might directly affect this statute's application to other domain name conflicts.

---

[760] *g. peter albert, jr., right on the mark: defining the nexus between trademarks and internet domain names, 15 j. marshall j. computer & info. l. 277 (1997),p304*

[761] *monika zalnieriute, beyond the governance gap in international domain name law: bringing the udrp in line with internationally recognized human rights, forthcoming stanford journal of international law vol 56 (1) 2020, p36.*

[762] *Julian S. Millstein, Jeffrey D. Neuburger, Jeffrey P. Weingart, Doing Business on the Internet: Forms and Analysis p4-17.*

[763] *Ibid, p4-17.*

[764] *g. peter albert, jr., right on the mark: defining the nexus between trademarks and internet domain names, 15 j. marshall j. computer & info. l. 277 (1997),p303*

In November 1996, the US District Court for the central District of California held that intentionally registering the plaintiff's trademarks as domain names for exacting payment from the plaintiff in exchange for termination of the domain name registrations had diluted the plaintiff's trademarks in violation of the Federal Trademark Dilution Act of 1995 and the California Trademark Dilution Statute. In reaching its decision. The Court acknowledged the value of trademarks as Internet domain names, stating that, "having a known or deducible domain name[765] is important to companies seeking to do business on the Internet, as well as to consumers who want to locate those businesses' websites." The Federal Trademark Dilution Act applies only to famous marks; the act requires showing more than simply distinctiveness to meet the threshold element of fame. To this point, the mark must be truly prominent and renowned under the act.' The act lists eight non-exclusive considerations for the 'famousness inquiry' including the degree of inherent or acquired distinctiveness of the mark; the duration in which the mark has been used in connection with the relevant associated goods or services; and the duration and extent of advertising and publicity together with the geographical extent of the trading area in which the mark is used[766].

The plain significance of this statute law is that it can be used despite the presence or lack of competitors between the famous mark owner and other parties, or confusion, deceptiveness, or likelihood. Hence, the problems regarding which items or services a web domain name recognises, if any, would seem irrelevant. Likewise, this law might be an important weapon for 'well-known' mark owners. The law only safeguards 'popular' marks, and the factors determining what makes up a 'popular' trademark are included. While the statute law may benefit big multi-national businesses that expend significant sums advertising and promoting their products and services, or for trademark owners with strong, well-recognised marks, the regulation will probably not safeguard lesser-known or unknown trademarks from being held ransom by the domain 'grabbers [767].' The earliest appearance of the dilution fundamental was in 1898 with the KODAK decision mentioned above[768]. Unlike trademark infringement, a dilution case does not require evidence that consumers are likely to be confused when comparing the unapproved use and the mark. Because of this, the items included need not be comparable, as the Illuminate case shows[769].

Therefore, irrespective of whether the unapproved use of a trademark would confuse or deceive the public, its use could be forbidden if it stains a mark's reputation or dilutes a mark's value. The dilution concept has often succeeded in protecting the utilised trademark in a derogatory or unwholesome context[770]. The Coca-Cola Company brought an action to prevent the defendant from printing, distributing and selling commercially a poster which consisted of an exact blown-up reproduction of the plaintiff's familiar "Coca-Cola" trademark and distinctive format, except for the substitution of the script letters "ine" for "-Cola", so that the poster read "Enjoy Cocaine." The signboards were issued in a script and colour identical

[765] *ibid, p4-18.*

[766] *Julian S. Millstein, Jeffrey D. Neuburger, Jeffrey P. Weingart, Doing Business on the Internet: Forms and Analysis,ibid, p4-19*

[767] *g. peter albert, jr., right on the mark: defining the nexus between trademarks and internet domain names, 15 j. marshall j. computer & info. l. 277 (1997),p303*

[768] *Ipid, p 408*

[769] *William E. Lee, Daxton R. Stewart, Jonathan Peters, The Law of Public Communication, ibid, p286.*

[770] *ibid, p286.*

to those utilised by Coca-Cola. The sticker company, in its defence, stated that the banners were only a satirical spoof. However, the US District Court for the Eastern District of New York considered that the harmful association of Coca-Cola with an unlawful narcotic could dilute the Coca-Cola trademark's value. [771]

The court did not recommend that clients would confuse Coca-Cola with illegal drugs. Rather, the court reasoned that customers might be affected by a resultant false belief that the Coca-Cola firm dealt with a harmful drug. About half the states have anti-dilution statutes, and American federal trademark laws also protect the aura and uniqueness of famous trademarks from dilution. However, the main criterion that must be considered is that the trademark shall be famous. As a result, the domain name cannot dilute nonfamous trademarks.

In order to prevail on a claim of trademark dilution, a plaintiff must also show that the defendant's use of the mark is used in commerce and that the defendant is 'capitalising on its trademark status.' Most domain name disputes have involved domain names identical to registered trademarks. However, when a domain name is similar—but not identical—to a registered trademark, it may be more difficult to prove that it infringes or dilutes the trademark owner's rights.[772] For example, the United States Supreme Court held that Victoria's Secret trademark owners could not bring proof that the Victor's Little Secret domain, an adult video and novelty store, diluted the Victoria's Secret trademark value[773].

In the case of *Hasbro, Inc. v Internet Entertainment Group Ltd*, in the 1990s, Brian Cartme and Internet Entertainment Group Ltd. used candyland.com as an adult website domain. The name string candyland.com is an internet domain that provides net users access to that website Any individual who performed a serach using the words 'Candy' and 'land' together was guided to this adult site. Hasbro launched lawsuits based on trademark dilution. The Court sought an irreversible order to prevent the offenders from abusing the Candy Land trademark. In the court's assessment, Hasbro demonstrated a probability of verifying that defendants, Internet, Entertainment Group Ltd., Brian Cartmell, and also Internet Entertainment Group, Inc. (jointly referred to as "the offenders") had indeed been diluting Hasbro's Candy Land mark by utilising 'Candyland' to operate a sexually explicit Internet website.. To this point, Hasbro successfully demonstrated that the offenders' use of the Candy Land name and the domain candyland.com in connection with their internet site, triggered permanent injury to Hasbro[774].

Chapter 2: Domain Names vs. trademark jurisdiction

The World Wide Web became a global tool in the late 1990s, and states worldwide, using enacted legislation, intended to handle the components of cyberspace within their jurisdictions. However, no substantive examination procedures exist for domain name

[771] *ibid,, p286*
[772] *ibid, p4-20*
[773] *ibid, p286.*
[774] *Kenneth W. Clarkson, Roger LeRoy Miller, Business Law: Text and Cases, Publisher Cengage Learning, United Kingdom & United States 15th edition, 2020, p174*

applications. Therefore, generic and descriptive names, unlike trademarks, are registrable as long as they are not identical to any existing domain name registration[775]. Selecting regulatory procedures for the broad internet converts cyberspace into affiliated jurisdictions where each state attempts to use its regulations, guidelines, and social cultures to police cyberspace activity within its territorial jurisdiction. Subsequently, problems with laws inevitably arise. Applying global regulations and policies is complex because these have typically appeared only after individual states have already regulated these on the internet, in various ways. This raises questions regarding which geographical regulations design to use. In the late 1990s and early 2000s, several national courts were asked to identify whether and if so when enrolment or usage of domain names, including another stakeholder trademark, comprised an infringement of intellectual property rights. While the tribunals revealed a readiness to apply and, undoubtedly, expand existing international concepts of trademark violation rules and passing off in regard to domain names, many stakeholders yet turned to various national courts to deal with conflicts concerning international domain name usage. Since the domain name generates international visibility, conflicts frequently feature trademarks issued in numerous jurisdictions, possibly calling for a trademark proprietor to bring different court actions in several countries. Also, where there is no multi-jurisdictional agreement, lawsuits are expensive and taxing in both outright and relative terms, as WIPO remarked in 1999[776]. In this context, the author will try to illustrate the issue by explaining the cause of *in rem* jurisdiction conflict and then analysing *in rem* jurisdiction's reality based on the USA and EU, to facilitate discussion of how international corporate activities have produced new obstacles for nation-states and their territories based on jurisdiction regulations, choice of legislation, and recognition of judgments[777.]

1. Background

Tribunals in numerous countries have applied their territorial trademark regulations to tackle the abuse of domain names in territorial ccTLDs and .com domains. Courts in New Zealand, Canada, the United Kingdom, and Germany have effectively granted relief to trademark holders in cybersquatting cases, often without requiring usage or intent. Enrolment of famous marks in cybersquatting cases has been identified as a violation in Israel, France, Germany, and Italy.[778] Jurisdiction will be a very important issue for a foreign party. In this regard, the author will illustrate the concept of the jurisdiction related to domain names conflict and then explain the judicial requirement as well as the causes of *in rem* jurisdiction conflicts. Finally, the author will suggest an alternative mechanism to resolve the jurisdiction issue.

[775] *g. peter albert, jr., right on the mark: defining the nexus between trademarks and internet domain names, 15 j. marshall j. computer & info. l. 277 (1997),p*

[776] *Sam Ricketson,Research Handbook on the World Intellectual Property Organization: The First 50 Years and Beyond, Publisher Edward Elgar Publishing,UK & USA, 1st edition, 2020, p268..*

[777] *Peer Zumbansen, The Many Lives of Transnational Law: Critical Engagements with Jessup's Bold Proposal, Publisher Cambridge University PressUK 1ST edetion, 2020,p240.*

[778] *domain Names and Trademarks, March 5, 2000 https://cyber.harvard.edu/property00/domain/main.html#discussion*

There is no doubt that domain names and trademarks are legal interests that deserve to be protected and are qualified as a reason to justify relief through the tribunal[779]. In most jurisdictions, the courts have initially justified the protection of trademarks based on preventing deception[780]. The question arises here as to whether a particular court has the power to hear a case. To what extent can jurisdiction be applied over the conflict between the main stakeholders in cyberspace (trademark holders and domain name owners)? Moreover, what are the reasons beyond the *in rem* jurisdiction over the domain names conflict?

2. The causes of *in rem* jurisdiction conflict over domain names

The *in rem* jurisdiction in this regard sounds different from other approaches because it needs to apply the national laws within geographical aspects over the online conflict in cyberspace while understanding the international legal nature of domain names. In this regard, one of the main reasons that led to *in rem* jurisdiction conflict is the deterritorialisation of cyberspace and the surge of domain name mediators. In this situation, it pays to ask these basic questions and reshape the main concept of jurisdiction conflict laws for the new internet era that is already changing our world[781]. While cyberspace lacks physical borders and domain name systems can be matured without geographical roots[782], typical jurisdictional conceptions are devoted to establishing standards to determine when jurisdiction over an internet site proprietor or operator in another geographical area is valid[783]. In this context, countries and national borders always have limited regulations. To this point, resolvability is constantly disputed, with a group of jurisdictional codes still extremely embedded in territorialism[784].

2.1 ICANN lacking policy

In rem jurisdiction is important in reaching a practical solution for the conflict in cyberspace between the trademark holders and domain name owners. The author believes the conflict arose increasingly due to the UDRP lacking practical policy rules to deal with this conflict. This lacking policy can be noticed in some cases; for instance, it did not consider the nature of the domain name as property, which would allow the court to practice jurisdiction over this property's place. Furthermore, its decision is lacking in that it does not force the parties to accept its decisions compulsorily. As a result, if one of the parties is not convinced of its decision, he can go to court, increasing the duration of the dispute.
On top of that, ICANN permits the judiciary's use as an alternative solution, and the *in rem* jurisdiction conflict emerged. It can state within the registration contract that any conflict that arises from using domain names shall be limited and settled within the UDRP rules resolution policy. And then, the parties' agreement will not authorise them to go to Court. As a result, it

---

[779] *Roger LeRoy Miller, Mary Meinzinger, Paralegal Today: The Legal Team at Work, Publisher Cengage Learning,8th edetion 2021, p169.*
[780] *dawson, n. m. "trade mark law and the creation and preservation of well-known brands." northern ireland legal quarterly, vol. 49, no. 4, winter 1998, pp. 343-362.p351*
[781] *Peer Zumbansen, The Many Lives of Transnational Law: Critical Engagements with Jessup's Bold Proposal, ibid, ,p242*
[782] *Michigan Telecommunications and Technology Law Review Volume 20 | Issue 2. 2014 Jurisdictional Limits of in rem Proceedings Against domain NamesMichigan Telecommunications and Technology Law Review [Vol. 20:467,p468.*
[783] *Roger LeRoy Miller, Mary Meinzinger, Paralegal Today: The Legal Team at Work, ibid, p169.*
[784] *Michael Xun Liu, Jurisdictional Limits of in rem Proceedings Against domain Names, ibid,p468*

is expected that the court will respect such a contract regarding ICANN policy related to jurisdiction. The question of jurisdiction may arise, however, if there is no such restriction. It might not be an issue if the parties belong to the same territory. However, it will become a real problem if they belong to different territorial areas. From a legal perspective, most trademark holders have registered their trademarks as domain names. They could not do that without pre-agreement that if the conflict arises from misuse of domain names or infringement on other related rights, the parties must predominantly use the UDRP rules mechanism to solve this conflict.

2.2 Permit the Court to initiate the conflict

ICANN policy permitted the stakeholder parties to bring the case to court if they were not fully satisfied with the UDRP rules decision. This permission raises more questions about the reason beyond this decision. One of these questions is whether the ICANN mechanism admitted that it could not settle the conflict perfectly using its devices devoted to solving it. Moreover, why does it force the parties to use the UDRP rules mechanism before going to Court? Regarding the right of the lawsuit, there will be no problem using this right in the territory of both parties if they belong to it.

Nevertheless, there might be an issue if the parties belong to different jurisdictional areas. The question arises whether the parties can go directly to court without using the UDRP rules mechanism. Will the court initiate and accept the claim or reject it based on the respect of the contract that states parties shall initiate the claim using UDRP rules first before going to court? It seemed that the court did not consider this hierarchy. It did not even task itself with investigating whether UDRP rules bid the parties. For instance, in "Heathmount A.E. Corp. v. Technodome.com," the complainant launched mediation under the UDRP rules, which resulted in filing a claim to the US District Court of Virginia. The court indicated the claim and announced its *in rem* jurisdiction over the questioned domain names regardless of UDRP rules[785]. The author believes that the court must predominantly investigate whether the parties have respected the UDRP rules according to the contract of registration that forces parties to initiate the claim using UDRP rules, before initiating any claim related to domain names conflict or any infringement trademarks rights related to domain names before the court. Moreover, the question arises if the Court can practice *in rem* jurisdiction over foreign parties regarding domain names conflict in cyberspace. Moreover, does the Court decision have power over foreign parties?

3. Types of jurisdiction

3.1 Personal Jurisdiction of domain names

Courts must have authority over the parties entailed or the contested property in disagreement. In this regard, individuals undergo 'personal jurisdiction' while the property

[785] *Jane K. Winn, Benjamin Wright, The Law of Electronic Commerce, ibid, p11-62.*

undergoes '*in rem* jurisdiction[786]. As for hearing the claim, it is expected that the court can hear the claim even if the parties are in different areas, thanks to the technology that now allows the court to hear the claim virtually and give a chance to remote connection. Personal or individual jurisdiction over domain name conflicts has been taken for granted for a long time. The plaintiff cannot obtain a judgment in his favour if the court fails to exercise individual jurisdiction over a foreign citizen or non-resident defendant[787]. On the other hand, if an individual or firm does not have adequate minimum relations with a state, the claim cannot be subjected to individual jurisdiction.

Furthermore, it is particularly problematic when conflict develops in cyberspace. In this context, jurisdiction is always readily found in a defendant's country of residence. A complainant might often choose to submit the claim to the defendant's state. Nonetheless, legal and practical worries typically push complainants to offer a lawsuit in their own country[788]. It is believed that claims concerning jurisdiction, according to website actions, usually apply the formal jurisdictional criteria delineated. The growth of the World Wide Web has raised the question of whether exercising jurisdiction in cyberspace is still valid[789].

Regarding domain names, customers frequently regard commercial value sites with '. Com' as much more trustworthy or credible. In this context, the tribunal will offer '*in rem* jurisdiction' to where the registry headquarters is located. The US trademark and the ACPA legislation are conditions for using the globe's most well-known TLD. These conditions enforce a much higher concern on non-US website operators who should use less tempting and famous top-level domain names, or encounter the responsibility of lawful foreign procedures. For instance, the legal frame related to US legislation, such as trademark law and ACPA, will be more restricted if applied during *in rem* jurisdiction[790].

The development of the Internet as an international network has essentially elevated significant administrative and legal concerns[791]. For instance, personal jurisdiction analysis is particularly difficult for a virtual space defendant who utilises a domain name outside his country or area. A virtual space defendant might be anywhere and nowhere in the same real-time. In addition, the mere acts of placing content on the Internet that any person can access anywhere in the globe suffices to achieve 'personal jurisdiction.' Any person establishing a web page would certainly take the possibility of liability throughout the country or indeed, the globe. Thus, it is necessary to analyse 'personal jurisdiction' in the shadow of these difficulties[792].

Nevertheless, while tribunals have heretofore modified and clarified the examination for jurisdiction, including trade and technology, all improvements have considered the existence of geographic borders. In this connection, and because cyberspace has no

---

[786] *, ibid, p470.*

[787] *ira s. Nathenson ,showdown at the domain name corral: property rights and personal jurisdiction over squatters, poachers and other parasites ,pittsburgh law review,1997 cite as 58 u. Pitt. L. Rev. 991 (1997).. Showdown at the domain name corral: property rights and personal jurisdiction over squatters, poachers, and other parasites (doc.gov)*

[788] *ira s. Nathenson ,showdown at the domain name corral: property rights and personal jurisdiction over squatters, poachers and other parasites ibid.*

[789] *Christof Siefarth, International Distribution Law, Publisher brill, 2021, p 175.*

[790] *Michael Xun Liu, Jurisdictional Limits of in rem Proceedings Against domain Names,ibid, P493.*

[791] *das, jatindra kumar, law of copyright, ,ibid p413*

[792] *ira s. Nathenson ,showdown at the domain name corral: property rights and personal jurisdiction over squatters, poachers and other parasites ibid.*

geographical boundaries, some questions must arise about whether the classic jurisdictional criteria should be purified to serve cyberspace. Likewise, tribunals must decide if cyberspace or the World Wide Web connection is adequate to fulfill the 'minimum contacts' condition[793].

Furthermore, tribunals have developed intelligible criteria for jurisdiction related to cyberspace. This issue is particularly evident in the statute of the domain system, where companies with identical, similar, or duplicate names contest to enrol these names. [794]In this context and at this point, tribunals may discover good bases for personal jurisdiction regarding the defendant's purposeful harmful behaviours based on bad faith. Furthermore, this approach must be narrow and limited to bad faith behaviour related to cybersquatting[795]. *Panavision International v. Toeppen*, already discussed above, is considered an important classic case related to different legal issues in cyberspace, including jurisdiction issues. This case was related to cybersquatting behaviour, where the defendant required money to return the domain to the plaintiff. The Court exercised its authority based on personal jurisdiction. The Court established that personal jurisdiction existed where "[t]he brunt of the harm ...was felt in California," and the defendant "knew Panavision would likely suffer harm there because, although at all relevant times Panavision was a Delaware limited partnership, its principal place of business was in California" [796].

Despite any theoretical obstacles to categorising the domain names as intangible property, this narrative enables Courts to apply in rem jurisdiction over domain names based on where the domain name is certified. In this regard, the query of where the property has the existent domain name plays a crucial role in practicing *in rem* jurisdiction over these domain names. These questions need a fundamental understanding of what domain names are[797]. The main challenge to any Court in terms of practicing its jurisdiction over domain names must go through finding the property in its territory on the one hand and finding any legal connection with the main stakeholders, not only the trademark holder or domain name owner but also the registry agency[798]. For instance, in Kremen v. Cohen[799], the Court found the contact with its territory in the fact that the registry agency VeriSign was located within the court district[800]. Furthermore, the court decided that the "registrant has an intangible property right in his domain name"[801] Probably most notable concerning all of *in rem* jurisdiction

---

[793] *Christof Siefarth, International Distribution Law, ibid,, p 175.*

[794] *Michael Xun Liu, Jurisdictional Limits of in rem Proceedings Against domain Names, ibid ,p469*

[795] *ira s. Nathenson ,showdown at the domain name corral: property rights and personal jurisdiction over squatters, poachers and other parasites ibid.*

[796] *Panavision Intern., LP v. Toeppen, 938 F. Supp. 616 (C.D. Cal. 1996) U.S. District Court for the Central District of California - 938 F. Supp. 616 (C.D. Cal. 1996) September 19, 1996 938 F. Supp. 616 (1996) panavision international, L.P., a Delaware Limited Partnership, Plaintiff, v. Dennis TOEPPEN, an individual, Network Solutions, Inc., a District of Columbia Corporation, and Does 1-50, Defendants. No. 96-3284 DDP (JRx). United States District Court, C.D. California. https://law.justia.com/cases/federal/district-courts/FSupp/938/616/2596612/*

[797] *Stephen Gillers, Regulation of Lawyers: Problems of Law and Ethics, Publisher Wolters Kluwer, newyork,8th edition,2021,p321.*

[798] *Ibid,,p321.*

- Warren, E., Westbrook, J.L., Porter, K., Pottow, J.A.E, The Law of Debtors and Creditors: Text, Cases, and Problems, , Publisher Wolters Kluwer,new York,8th edition, 2021,p 321.

[799] *337 F.3d 1024, 1029 (9th Cir. 2003)*

[800] *Stephen Gillers, Regulation of Lawyers: Problems of Law and Ethicsibid ,p321.*

- Warren, E., Westbrook, J.L., Porter, K., Pottow, J.A.E The Law of Debtors and Creditors: Text, Cases, and Problems,ibid,p 321.

[801] *Stephen Gillers, Regulation of Lawyers: Problems of Law and Ethicsibid,,p321.*

- Warren, E., Westbrook, J.L., Porter, K., Pottow, J.A.E The Law of Debtors and Creditors: Text, Cases, and Problems,ibid,,p 321.

situations is that it observes in the legal choices significant interaction with the doctrines, concepts, norms, as well as procedures that traditionally underlie the jurisdiction related to the law conflict in cyberspace doctrine, selection of law, or acknowledgment of judgments. Instead, courts tend to think that because something is perhaps situated within a territorial border, that suffices to claim jurisdiction or apply local legislation. In other words, based on the perception that the local application of a legal system is ideal, applying that same rule around the world is likewise appropriate. Alternatively, they seem to think regional public laws automatically treat and defeat other problems in recognising an international judgment.[802]"

For trademark proprietors, among the effective weapons to apply intellectual legal rights given by *in rem* jurisdiction is enabling *ex parte* procedures versus the domain names violation, hence removing the demand for 'personal jurisdiction' over the registrant and illustrating domain names as intangible property topics them for civil forfeit, an approach utilised to handle many of the domain names. Under the ACPA, trademark proprietors can obtain *in rem* jurisdiction versus a domain name owner if the contested domain name dilutes or even infringes the reputation of the legitimate trademark. Such processes do not go against the due procedure requirement, and this interpretation of jurisdiction is irregular with fundamental reasonings to restrict jurisdiction. Additionally, exerting 'in rem jurisdiction' over domain names not enrolled in bad faith goes against the ACPA spirit[803]. Suppose the mark proprietor cannot get 'personal jurisdiction' against the registrant. In that case, and according to legal doctrine, jurisdiction can be done where the "domain registrar, registry, or other domain name authority that designated the domain or signed up name lies.[804]"

3.2 In Rem jurisdiction

Some legal commentators believe that cyberspace is borderless, so it cannot be subject to the sovereignty principle.[805] [806] Therefore, *in rem* jurisdiction can be crucial in resolving disputes over domain names. On top of that, for *in rem* jurisdiction, a complainant can initiate legal action over property possession in the courts local to where the property lies, whether physical or intellectual. Nevertheless, complainants may utilise this choice just if the domain name registrar is exempt from individual territory in the relevant country. Therefore, when Porsche declared privilege to Porsche.net, porsche.com, and various other domain names, it appealed to the Court in Virginia since that was the registrar's location for the domain name owners. To the degree the conflict entailed certain domains enrolled by a British person, Porsche can seek the cases *in rem* jurisdiction against the domain. Note that even though the

[802] *Peer Zumbansen, The Many Lives of Transnational Law: Critical Engagements with Jessup's Bold Proposal, ibid, ,p242.*

[803] *Michael Xun Liu, Jurisdictional Limits of in rem Proceedings Against domain Names, ibid,p481.*

[804] *, Ibid,p470*

[805] *Binxing Fang, cyberspace Sovereignty Reflections on Building a Community of Common Future in cyberspace, Science Press and Springer Nature Singapore Pte Ltd. 1st edetion, 2018,p106.*

[806] *Howard M. Erichson Inside Civil Procedure: What Matters and Why? Ibid, P54.*

anticybersquatting act admits *in rem* jurisdiction, it restricts it to circumstances that the personal jurisdiction cannot be applied in that conflict[807].

The Internet is considered a power in the international economy, and has become a part of the lives of millions of people. In the physical world where people sue each other, cyberspace is qualified to be where the main stakeholders interact with a conflict of interests online. The need to resolve the dispute over the contested rights becomes a real matter. The question arises: Where is the judicial authority of the lawsuits, and where is the zone of the mistakes upon being sued? Where can the complainant make the defendant present themselves?[808]The difficulty is serving justice to the offender in light of *in rem* jurisdiction. The dilemma is presented in the situation that the defendant is everywhere, at the same time, possibly nowhere. Should someone who causes injury be held to suit anywhere on the Internet? In this regard, technical modification in transportation and interaction has commonly shaped visions of due process. It is highly recommended to consider the early Internet instances on jurisdiction [809].

4. Practical issues over domain names *in rem* jurisdiction

Some practical cases reflect the difficulties of practicing *in rem* jurisdiction in cyberspace; in this regard, the author will analyse some cases to understand some of these difficulties as follows.

In 2000, the French tribunal of Paris provided an initial injunction against Yahoo.com, instructing the website to carry out all possible procedures to protect against and discourage gaining access to Yahoo.FR, which is a public auction website that offers Nazi memorabilia or other things considered to be Nazism or to comprise Holocaust rejection.[810] The French court established that there were sufficient links with France to give it full jurisdiction to hear the complaint. In particular, since, the auctions of Nazi memorabilia were open to bidders from any country, including France, the display of such objects in France, caused a public nuisance and was forbidden under French criminal law; Yahoo! Inc. was aware that French residents used its auction site, as it displayed French-language advertisements on its pages when they were accessed from computers in France.[811]. Yahoo decided, instead of appealing against the ruling in France, to take the case before the United States District Court for the Northern District of California, asking it to find that the French ordinance is not effective in the United States. According to the District Court's ruling, the French court's decision was inapplicable in the United States. Two other companies appealed the decision before the U.S. Court of Appeals for the Ninth Circuit. In 2004, the latter court reversed the earlier holding, after finding that the district court did not have personal jurisdiction over the appellants. It argued that exercise of jurisdiction under such circumstances is possible only if (1) the non-resident defendant has purposefully directed his activities or consummated some transaction with the forum or a resident thereof, or performed some act by which he purposefully availed

[807] *ibid, P54.*

[808] *Barbara Allen Babcock, Toni M. Massaro, Norman W. Spaulding, Civil Procedure: Cases and Problems, Publisher Wolters Kluwer, 7th edetion 2021, p 224.*

[809] *ibid, p 224.*

[810] *Peer Zumbansen, The Many Lives of Transnational Law: Critical Engagements with Jessup's Bold Proposal, ibid, ,p242*

[811] *ibid, ,p246*

himself of the privileges of conducting activities in the forum, thereby invoking the benefits and protections of its laws; (2) the claim arises out of or relates to the defendant's forum-related activities; and (3) the exercise of jurisdiction is reasonable. Criteria (1) is satisfied when the defendant is alleged to have engaged in wrongful conduct targeted at a plaintiff whom the defendant knows to be a resident of the forum state. However, Yahoo! made no allegation that could lead a court to conclude that there was anything wrongful in the organisations' conduct. As a result, the District Court did not properly exercise personal jurisdiction in this case.

5. Practical challenges in the choice of jurisdiction

The ACPA states that a trademark holder might move against cybersquatter behaviour based on personal jurisdiction. The question that deserves to be answered is: does this approach increase the property's examination (i. e. against the approach that acquiring a domain name only means contractual relationship)? Furthermore, *in rem* jurisdiction, as was explained above, is exclusively constitutional in those cases where it offers minimal contacts enough for personal jurisdiction. The court denies this argument and concludes minimal basic connection with supporting personal jurisdiction exists only in *in rem* procedures where the underlying root cause of action is associated with the property in the state. In this context, the domain names present the property correlated to the reason for action and its whole subject matter. Therefore, minimal connections do not fulfil personal jurisdiction standards. To the level that minimum connections are needed, *in rem* jurisdiction is constitutional when the rem offers minimum contact adequate for personal jurisdiction. The Court denies this disagreement and also states that there needs to be a minimum correlation between sustaining personal jurisdiction merely where the implicit reason of activity is unconnected to the property within the country of the Court. As necessary, minimal contacts do not have to fulfil personal jurisdiction criteria to the degree that minimal connections are needed *in rem* jurisdiction[812].
The domain names' jurisdiction is more complicated than other legal issues in terms of which court has the authority to hear the claim, and which law must be applied. Besides, these issues are related to the natural core of the domain name itself. Is it a property or something else? In this context, the case is associated with *CRS. Recovery, Inc. v. Laxton 600 F.3d 1138 (9th Cir. 2010)* which reflects the complex relationship with domain names jurisdiction. This case is related to Dale Mayberry, a citizen from Virginia who registered the domain name *rl.com* by NSI, Inc. and transferred the ownership of it to another person, Mr. Qiang. The local Court noticed the main question about which law must be chosen: Virginia's or California's law. In other words, the defendant law, in this case, is Mr. Laxton for whome Tthe prevailing law was California law, while the plaintiff law, in this case, will be Virginia law, where Dale Mayberry lives. Both plaintiff and defendant urged the Court to apply their own local rules. Both directions have different approaches regarding the essence of the domain names' nature. On top of that, the domain name is just a contractual relationship

[812] *R. Lea Brilmayer, Jack L. Goldsmith, Erin O'Hara O'Connor, Carlos Vázquez Conflict of Laws: Cases and Materials,Publisher Wolters Kluwer Law & Business,, 8th 8, 2019,p462.*

under Virginia law, whileinn contrast, California law considers domain names intellectual property and grants the plaintiff the full right to personal property. Mayberry, a Virginia plaintiff, wanted California law to prevail. The plaintiffs claimed that he had only a contract under Virginia law. The Court executed an analysis based on governmental interest, concluding that California has legitimate jurisdiction based on the legitimate interest to apply California law when delivering the judgement[813].

This case would need more attention; for instance, if the defendant behaved in bad faith, the plaintiff caused this situation, or it was a third-party mistake. Furthermore, this case reflects the importance of determining the legal nature of the domain name as a property, particularly in light of *in rem* jurisdiction. The UDRP rules do not prevent a domain owner restrained by it or a plaintiff under the UDRP rules process from bringing a claim before a court. Nonetheless, it sometimes claims to enforce jurisdictional constraints on the stakeholders. Under Para 4(k) UDRP rules, if a committee decides to transfer a domain or terminate a name, its holder may stay clear of implementing that choice by starting a claim. For the situation to create such impact under Para 4(k), it has to be obtained "in a jurisdiction to which the plaintiff has been sent under Para 3(b)(xiii) of the regulations of Procedure[814]."

According to Para 3(b)(xii) of the rules, the complainant is called for in its complaint to send any challenges concerned to a UDRP rules judgement moving or cancelling the domain name, "to the jurisdiction of the tribunals in at the very least one specified mutual jurisdiction." Part of the rules specifies 'mutual jurisdiction,' which suggests a court at either the major headquarters of the registrar that offered the website to the domain holder or to that jurisdiction or the domain name owner's address as displayed in the registrar's record at the time the problem was sent. The importance of the referral to that certain court of laws in Part 4(k) appears to be restricted in that only a claim brought on the trial among those jurisdictions in 10 calendar days creates the effect of avoiding the transfer or termination of the domain asked for in the panel choice. It restrains the jurisdictions where the domain owner might bring a suit to benefit from the protection device offered in Part 4(k). Hence, the jurisdiction statute requires applying that particular defence system. Under the last indent of passage 4(k), an ordering 'from such court' rejecting the suit carried by the legal holder or requesting that he has not the right to proceed to use the domain name will set off the termination of the contested domain name. In practice, tills might be used as an aspect to say that, at least for ICANN as well as the appropriate registrars taking care of domain names to which the UDRP rules use are concerned, a decision from a jurisdiction specified in Part 4(k) ought to dominate possible contrasting decisions concerning the enrolment of the domain name rendered moot in various other jurisdictions.[815,816] The UDRP professes to enforce extra restraints on the jurisdiction, especially trademark proprietors, if they decide to bring an issue under the UDRP rules. The rightsholder intends to do well in his grievance, in principle. Because in certain situations, he will be bound by his declaration submitting concerning any difficulties to a choice of the UDRP's committee transferring or cancelling the domain name to the jurisdiction of

[813] *Ibid, p361.*

[814] *Pedro de Miguel Asensio, Conflict of Laws and the Internet Publisher Edward Elgar Publishing, 2020, para para 5.10*

[815] *iid para 5.10*

[816] *ibid, para 5.39*

the Court of Laws at the very least, once they have defined mutual jurisdiction (Passage 3(b)(xii) of the rules). The credibility of such a jurisdiction argument can be questionable in particular situations if utilised to challenge jurisdiction in tribunal proceedings in various other states. Such submissions remain pertinent from the standpoint of the UDRP rules and revocation or transfer of the domain based on it. Also, as to Part 3(b)(xii) of the regulations, the plaintiff chooses the jurisdiction according to his submission. It is the domain name in practice[817]. The tribunals of mutual jurisdiction are just those of the central places of the domain name owner's address or the registrar's, according to the meaning in Paragraph 1 of the UDRP rules.

A well-established method in this respect, which the 1999 WIPO final report sustains, is to refer, if essential, to the legislation of the region of the common regular residence of the parties, specifically if the domain name was registered with a registrar in that state. The proof of bad faith registration and domain name usage relates to tasks in the same country. The tribunals of common jurisdiction may be mainly from the plaintiff's area.[818] The potential threat is that the domain name owner influences the appropriate linkages to prohibit the competent jurisdictions to the homeland where he is specified.

The potential danger shows that the domain name owner affects the pertinent links to restrict the competent jurisdictions he selects and the interplay with national regulations and decisions[819]. According to paragraph 15 of the UDRP rules, a panel will determine the case following the UDRP rules and any applicable legislation. The panel also avoids selecting a national regulation relevant to supplement the uniform UDRP rule part five, no 40[820]. Beyond applying basic mark regulations and unjust competition rules to respond against violent registration and the use of domain names, some regions have adopted them. Specific regulation in this area differs between violation actions and the UDRP policy. Hereof, a particular reference is the anticybersquatting consumer protection act (ACPA), which contains certain jurisdiction rules pertinent to cross-border scenarios.[821]

The stakeholder may bring a declaratory verdict action under the ACPA to recuperate the contested domain name shed in the UDRP rules. Moreover, the party that grants a tribunal's jurisdiction under the ICANN plans goes through that tribunal's jurisdiction for all relevant claims. Nevertheless, it does not suggest that the party undergoes jurisdiction for an action obtained by a third party, even if it connects to the same subject, particularly the domain in dispute. The previous choice is believed not to bind the Court to determine an ACPA lawsuit under the UDRP rules[822]. Based on the domain name's global nature, resolving the related conflict will fall under multiple jurisdictions. As a result, the trademark holder finds himself forced to bring suit in various states[823]. European Union states with ADR rules

[817] *Ibid,, para 5.39.*
[818] *ibid, para 5.45*
[819] *ibid, para 5.40*
[820] *ibid, 2020, para 5.41*
[821] *ibid, 2020, para 5.41*
[822] *Michael D. Scott, Scott on Multimedia Law, Wolters Kluwer , New York. 4th Edition,2022,p5-124.*
[823] *Sam Ricketson ,Research Handbook on the World Intellectual Property Organization: The First 50 Years and Beyond, ibid, P268.*

have built an incorporated general structure where the European Parliament and the council of the EU embraced the consumer ADR rules and customer ODR.[824.]

6. The reality of in rem jurisdiction

Among other things, resolving the conflict over a contested domain name via a court usually contains a foreign party, which entails that the court can exercise its competencies over the conflict through *in rem* jurisdiction. Moreover, *in rem* jurisdiction needs to be applied over the property. Hence, the author supports the point that considering domain names as property facilitates and paves the way for Courts to use *in rem* jurisdiction over contested domain names. A practical example of this vision is present in the case of T*ucows.Com Co. versus Lojas Renner S.A., 2011, ONCA 548*. In this regard, the Main Court of Ontario considered whether to accept jurisdiction over the questioned possession of the contested domain name. To this point, Tucows is a corporate body with its office headquarters in Ontario. Meanwhile, Renner is a Brazilian corporate body running a series of retail outlet stores. Tucows obtained 30,000 domain names, including renner.com.

Tucows' firm registered that domain with ICANN. Renner petitioned WIPO, and in reaction, Tucows filed a claim in Ontario, looking for a declaration affirming that it was the legal proprietor of the domain name. Renner questioned Ontario's jurisdiction over the conflict. The core difficulty was whether this dispute concerned individual property in the district of Ontario. The Court assessed numerous academic papers on the concern worldwide and considered jurisprudence from other countries, including the USA, Australia, and the UK. It concluded that the arising agreement seems to be that domain names are a form of property. After further evaluating the individual property's legal character, it was concluded that a domain is indeed a private property. The attaching variables favouring the place of the domain name in the Ontario district were the domain name registrant, the registrar's place, and the web servers as middlemen. On this ground, the tribunal discovered the domain in the concern to be individual property in Ontario. It therefore, took jurisdiction under the procedure in Van Breda[825.] In a modern-day practice of *in rem* jurisdiction doctrines, disputes over internet domain names (for instance, www.apple.com) might fall into the domain registrar's territory[826].

6.1 In rem jurisdiction and territorial links

Suppose there are adequate minimum links or connections with the State. In that case, the general concept is that countries may exert jurisdiction over non-residents. Under conventional notions of justice and substantial justice, allowing the State to work out personal jurisdiction is practical. For instance, Burger King's corporation is a Louisiana firm. It might be sued in any state because it is a company in all states. By serving in a state, Burger King

---

[824] *Tulus Suryanto, Hamzah , Samsudin Wahab , Yulia Chernysheva, Ali Juhary, Jie Ferry, ICETLAWBE 2020 Proceedings of The International Conference on Environmental and Technology of Law, Business and Education on Post Covid 19 Bandar Lampung, Indonesia 26 September 2020 Publisher European Alliance for Innovation, 2020 ,p325*

[825] *Michael Xun Liu, Jurisdictional Limits of in rem Proceedings Against domain Names, ibid,482*

[826] *Deborah E. Bouchoux, A Practical Introduction to Paralegal Studies: Strategies for Success, ibid, P101*

approves the advantages and benefits of operating in the State; therefore, it is sensible and fair that Burger King is subject to any state tribunal's jurisdiction. On the other hand, if a company or individual does not have adequate minimum communication with a state, it cannot go through personal jurisdiction in the State. Hence, if a firm operates only in Louisiana, it cannot fight for itself in other areas[827].

Parties can also give their consent to jurisdiction. For instance, numerous agreements have jurisdiction clauses in them. If there is any disagreement about the arrangement or its terms, between parties and main stakeholders, then lawsuits might be obtained in a designated court in a selected area. Therefore, personal jurisdiction depends on citizenship, physical visibility, a long-arm statute paired with minimal contacts, or approval. Under the umbrella of 4(e)(1) from the civil procedure of American Federal rule, the court may exercise individual jurisdiction whenever the area in which it lies has personal jurisdiction.[828] The question is whether this agreement is effective regarding domain name disputes. The author believes this agreement has nothing to do with practicing personal jurisdiction over domain names because the litigants from the outset do not know each other to have such an agreement. This vision is more likely related to the violation of contractual issues.

On top of that, the best-closed adoption is the UDRP rules frame in which parties must agree to use UDRP rules to solve their conflict related to domain names, as will be discussed later in the alternative jurisdiction suggestion. Likewise, the judicial practice developed a kind of jurisdiction called *in rem* jurisdiction when an action is associated with property situated within a region. Therefore, if there is a disagreement between parties connecting to property in California, the act might be obtained in California, regardless of the where events and parties are located. Tasks and actions concerning real estate and individual property, such as vehicles, watercraft, and other properties are executed where the property lies. In a modern-day application of administrative principles, conflicts over internet domain names (for example, www.audi.com) may be brought into the jurisdiction of the domain name registrar. A Chinese news company filed a claim against VeriSign in Virginia. Nearly all of its users were found in China but VeriSign's domain name registry was located in the Virginia district.

Thus, *in rem* jurisdiction acted as an alternative to personal jurisdiction in *Cable News Network, LP v. CNNews.com, 162 F. Supp. 2d 484 (E.D. Va2001* and *56 F. App' x 599 (4th Cir. 2003)).*[829] The ACPA resolves jurisdiction in domain names disputes by attending to *in rem* jurisdiction. Based on the ACPA, the owner of a trademark may submit an *in rem* civil measure against an individual having a domain name in the national judicial district in which the domain names registrar, domain registry, or other domain authority that signed up or appointed the domain name is *in rem* jurisdiction and is determined as an example where jurisdiction cannot obtain over the opposition or where an appellant, after due persistence, cannot be situated[830.] Venue somewhat pertains to the concern of the place of the jurisdiction, specifically identifying the region in which a criminal or civil action is to be carried out. The platform appears in any state where the opposition lives, where the acts triggering the action

[827], *ibid,, P101.*

[828] *ibid, P101*

[829] *Deborah E. Bouchoux, A Practical Introduction to Paralegal Studies: Strategies for Success, ibid, P101*

[830] *Mark J. thronson, gabrielle S. roth, jon D. grossman, Intellectual Property, Legal Opinions, Wolters Kluwer. 2nd edition, 2020, p 9-37.*

happened, or where the main parties have recently concurred venues. Thus, in a violation of the agreement case, the system may be appropriate in a pair of locations: the defendant's residence and where the deal was violated. In such cases, the complainant can choose the venue, typically based on whether the place is proper in the region where the property is situated if an action includes real property[831]. An opposition might ask for a change of location; an adjustment is generally permittedonly when there is a good reason; additionally, a test may be relocated simply to a tribunal with proper jurisdiction. As a whole, if a litigant does not challenge the medium, the defendant will certainly be held to have normally forged the right to oppose any judgement made by the Court. Altogether, jurisdiction obliges the authority to consider the venue associated with the specific region where an issue will be discussed[832]. Applicability and sanctions of the ACPA use all domain name registrations of trademarks. Successful complainants in claims obtained under the act can collect real damages and earnings or choose to receive legal losses varying from 1000 to 100,000 US dollars. Although some firms have efficiently filed a claim under the ACPA, there are obstructions to pursuing such legal actions. Some domain name registrars offer privacy solutions that hide the true proprietors of sites, making it difficult for trademark proprietors to determine cybersquatters.

Thus, a trademark owner must ask the tribunal for a subpoena before bringing a suit[833]. Web and jurisdiction usefully determine the pitfalls of extraterritorial exertion of national internet-related regulations and attempt to decrease unplanned normative consequences of federal measures upon international procedures via advancing global due process structures and administrative concepts for cyberspace[834].

Sovereign jurisdictions are still important ways to classify norms, amongst various things, for the rule of region obligation (regions stay liable for particular cyber tasks rising from their sovereign area) and the no-harm principle for the web's public core. As earlier debated, the transborder nature of cyberspace presents a significant obstacle to typical lawful organisations enforcing jurisdiction over conflict. Still, it does not change the importance of collaboration and synchronisation in jurisdictionally difficult inquiries[835]. There is tension between nationwide jurisdictions to impose and prescribe, according to sovereignty, and the cross-border circulations of information and solutions online. It is acknowledged that, time delay in procedures will follow as a consequence.[836]

6.2 In rem jurisdiction challenges

Jurisdiction in cyberspace has brought more challenges than solutions to the domain name conflict. For instance, one of these challenges is if the defendant’s residence is unknown

---

[831] *Deborah E. Bouchoux, A Practical Introduction to Paralegal Studies: Strategies for Success, ibid, P101*

[832] *, Ibid, p102*

[833] *Roger LeRoy Miller, Business Law Today, Comprehensive: comprehensive edition text and cases, Publisher Cengage Learning, 13rd edition,2021, p200.*

[834] *Matthias C. Kettemann, The Normative Order of the Internet: A Theory of Rule and Regulation Online Publisher Oxford University Press, UK, 1st edition, 2020, , p217.*

[835] *, ibid, p217.*

[836] *ibid, , p216.*

residence. The question arises: Can the court exercise its jurisdiction over the contested domain name if the defendant has no residence or his residence is unknown?[837]

The particular courts' jurisdiction can omit various other countries' tribunals from exerting jurisdiction over the same situation. Because there are no unique stipulations for global jurisdiction on any issue related to intellectual property conflict, all the issues concerning intellectual property are exempt from the special jurisdiction of any single Ccourt of another country, even though the legitimacy of registered intellectual property rights undergoes sole jurisdiction in other foreign legal procedures such as the procedure under article 24 (4) of the Brussels I regulation of the European Union.[838]

In this regard, jurisdiction over domain names needs deeper analysis. For instance, if the domain name runs a website involving infringement on trademark rights. In this case, would the court have legal jurisdiction? Usually, the court's jurisdiction is established based on attaching nationality, domicile, and individual residence. In this respect, the case ADNDRC in Hong Kong versus its Taiwanese owner is demonstrative. The proprietor launched a claim in the State of Taiwan to pursue a judicial affirmation that the domain registration did not infringe exactly on the mark of the television company BS combination. The first instance tribunal judged that Taiwanese tribunals had no jurisdiction, while the court of the second instance reversed this judgement and asserted that Taiwanese tribunals did have legal jurisdiction. The Supreme Court promoted the second-instance decision. According to the Supreme Court's judgment, the background to sustain the Taiwanese Courts hds the legal right to jurisdiction because the domain name was linked with the registered trademark and safeguarded under Taiwan trademark law. To this point, in the case Tai-Kang-Tzu No 256 of 2019, the Taiwanese plaintiff filed a claim against the Japanese offender's firm in a Taiwanese Court, insisting that some counterfeit products were sold in the offender's shop in Japan and also on the opponent's internet website, that was accessed from Taiwan using the Internet while announcing overseas orders will not be refunded[839]. The first-instance court ruled that Taiwanese Courts have no jurisdiction overseas, while the second instance court ruled that Taiwanese tribunals do have legal jurisdiction. The Supreme Court supported the second instance court ruling and mentioned that the jurisdiction power would be granted to Taiwanese Courts based on the consequence of such violation in Taiwan. In light of the universality of the internet and the fact that the internet site was designed for online purchasing within Japan, it is proposed that the principle of IP territoriality might function as a legal ground for the Taiwanese jurisdiction[840].

The author believes that even if domain names do not contain confusingly or similar trademarks but run a website that contains or is related to infringement on intellectual property rights such as trademark rights, it might be a legal ground for the court to exert its jurisdiction over domain name conflict.

---

[837] *P70*

[838] *ibid,P71.*

[839] *Ibid, P73.*

[840] *Ibid,,P74.*

6.3 In rem jurisdiction over the domain names: website content approach

The conflict over domain names can be expanded to contain the website run by the contested domain name to protect fundamental intellectual property rights that are likely to be infringed upon. On top of that, the illegal website that infringes on IP legal rights, particularly trademarks, continues through the website hosting provider. So, it can be conveniently determined via IP addresses connected with each domain and website. Once the web hosting has been recognised, reports of infringement or misuse can be submitted with proper complaint contact. Suppose they all utilise the same web hosts or IP addresses. In that case, it is viable to correlate individual domain names within unlawful internet sites. All domain name enrolment authorities (including both registrars and registry operators) are contractually committed to releasing an abuse factor of call. Registrars are called to "take punctual and affordable steps to explore and react suitably to any reports of trademark misuse"[841]. The conflict over domain names was not limited to cybersquatting, as much of the traditional literature of legal views illustrated. Instead, the conflict over domain names went deeper than merely someone trying to register some domain names to resell them to the legal trademark holder to gain some money. The conflict over domain names seems more related to the owner's underlying website content and the business's scope. In this context, there is a strong correlation between the website content and the domain name that runs this site or domain name registrant.[842] By exercising jurisdiction over a questioned domain, the Court effectively finds which party can utilise the mark on the website to symbolise their services and items. American District Courts are more familiar with judging trademark conflicts and efficiently use the Lanham Law in the digital world. The issue is that several cases involving a domain name under the ACPA include international or nonlocal parties that would never undergo the US trademark regulation..

Simply put, the ACPA permits courts to apply United States' trademark regulation to worldwide legal disputes between foreign stakeholders. Such a wide conferral of authority weakens the typical law's reasoning behind jurisdictional limitations in two crucial means: jurisdiction over domain names allows United States Courts to overextend into international and worldwide legal disputes. Second, *ex parte* procedures versus domain names violate stakeholders' rights and lead to business unpredictability. They have provided some challenges linked with the present *in rem* jurisdiction[843].

6.4 Bad faith and in rem jurisdiction

One of the suggestions to address the challenges related to *in rem* jurisdiction over the domain names is that courts should require trademark holders to show that the domain name owner has bad faith as a condition for exercising *in rem* jurisdiction by the court. *In rem*, American courts have the jurisdiction authority to overreach right into foreign disputes. *In rem* jurisdiction over the domain names is incompatible with systemic gains for jurisdictional

[841] *Battersby, Grimes, Licensing Update 2020 Edition, Publisher Wolters Kluwer,10th edetion, 2020,p 20-29.,*

[842] *Michael Xun Liu, Jurisdictional Limits of in rem Proceedings Against domain Names, ibid P489*

[843] *ibid P490*

limitations since it allows district courts to adjudicate any conflicts with even the tiniest link to the United States. In this context, the Harrods case would help to shed light and explain this situation. In that instance, *Harrods BA vs. Harrods UK* the Harrods trademark was used in the Argentinian market and the UK independently. Although Harrods BA may have enrolled several domains in bad faith, the fundamental conflict still entailed two international businesses with no significant relationship with the United States working out *in rem* jurisdiction over the domain names. The District Court of Virginia applied American regulation to settle a conflict between foreign parties accomplishing business outside states. The ACPA *in rem* arrangement's wide extraterritorial reach can also result in inappropriate legal responsibilities. To this point, the Virginia district Court ordered the VeriSign agency to disable the contested domain name regardless of an inconsistent foreign Court verdict in *Globalsantafe v. Globalsantafe.com*.[844]

6.5. In rem jurisdiction and reverse jurisdiction

In the case *Globalsantafe v. Globalsantafe.com*, the Korean company Fan registered the key name. The domain name was correspondingly registered via a formal Korean registrar. The Court decided against VeriSign and ordered the Korean registrar agency to move the contested domain name to GlobalSantaFe. Meanwhile, Mr. Fan encouraged the Korean Court to prevent transferring that domain name by the Korean registrar since Virginia had the legal authority to have jurisdiction over the conflict. Regardless of the foreign demand, the American Court judged the order forcing the VeriSign agency to disable the domain unilaterally. The tribunal kept in mind the possible universal comity matter. It declined to deliver jurisdiction since "the foreign procedures did not begin until the issue had been fully adjudicated below" and since "the Korean proceeding was started with the intent of obstructing the Judgment." By making inappropriate legal responsibilities for foreign parties, exerting *in rem* jurisdiction over the domain weakens the organised administration of laws. A state's sovereign passion for using its policies in its domiciliaries is a basic part of a worldwide legal routine and a fundamental mandate of territorialism. As such, the Korean Court in Globalsantafe was interested in settling the Internet businesses' legal rights in Korea. By working out *in rem* jurisdiction at the registry rank, the United States Court imposed US trademark legislation on both the Korean registrant and registrar of the domain name, threatening the Korean Court's power to regulate manners within its geographical borders[845].

6.6 In rem jurisdiction and stakeholders' interests

Based on the legal point of view, *in rem*'s jurisdiction increases the challenges toward solving the conflict over domain names in cyberspace. In this regard, some legal experts believe *in rem* jurisdiction jeopardises the stakeholder's fundamental interests. In addition to overreaching into international disputes, the practice of *in rem* territory under the ACPA damages individual passions by disabling parties' assumptions and creating procedural

[844] *,ibid P490.*
[845] *ibid P490.*

unjustness for foreign litigants. Because there is often no connection between the registrant's real activities and the domain name, *in rem* territory undermines stakeholders' speculations. In launching an internet presence, companies and people deal with online hosting companies to create areas in cyberspace, enrol domain name, and various other services. The physical place of each service supplied[846] but usually, it has little effect on the internet site's performance accessibility. This is particularly true for domain name systems (DNS), where the registry's place is virtually useless in any practical sense. Common TLDs such as *.com* and. *.org* are considered separate from any geographic area. Many non-United States websites that exclusively target non-United States audiences use the *.com* TLD since customers perceive it even more positively, despite geographic location. Provided the absence of a link between the area of the registry as well as a firm's online tasks, registrants must not fairly anticipate defending their fundamental rights in a foreign country just because their domain finishes in *.com*. One of the cases that most reflects the complicated situation of *in rem* jurisdiction in such a situation is the case of CNN News. This case was present in the domain name cnnews.com, and a Chinese registrant enrolled to run a collection of internet sites with domain names that ended in *.com*. The websites' contents used the Chinese language, targeted Chinese browsers, and received payment from China exclusively. The websites' material and any possible trademark infringement birthed no connection with the physical area of the *.com* registry. The registry's place was insignificant before the CNN company sued. Therefore, it is hard to envision that the Chinese registrant predicted being hauled into an American Court.

By compiling the registrant to prosecute in Virginia, the Court enforced the challenges of litigating in an international online forum on a party that had little reason to anticipate a Trial in the US. This technique likewise deteriorates businesses' lawful predictability to structure their online conduct. Even if registrants should predict United States lawsuits for a *.com* domain name, specifying the situs of a domain name related to the registry area is still procedurally unjust for non-United States registrants. In this regard, under the ACPA, a foreign registrant is compelled to choose between using non-based TLDs or dealing with prospective litigation in a US Court. The trouble is that the *.com* TLD, based in the US, remains the gold criterion. Offering the lack of a link between a firm's place and the registry's online tasks, registrants should not fairly expect to defend their civil liberties in a foreign forum just because their domain name finishes in *.com*. In that instance, the Chinese registrant of cnnews.com ran a series of websites with domain names that ended in *.com*, assuming that registrants need to predict US litigation for a *.com*. Under the ACPA, an international registrant must choose between using non-US-based TLDs or dealing with potential lawsuits in a US Court [847].

6.7 In rem jurisdiction in the USA

Regarding the United States jurisdiction approach, it noted that the parties may invoke the *in rem* provision against domain names owned by legitimate foreign businesses. In this context,

[846] *,ibid P490.*
[847] *ibid P492*

the ACPA was a power tool used effectively by litigants to protect the rights related to their trademarks in cyberspace via *ex parte* proceedings[848]. Regardless of the ACPA, the property condition of the domain offers for *in rem* jurisdiction trademark violation in the tribunals of the area where the domain registrar or domain registry (or other pertinent domain authority) is situated. However, this relies on the Court to find the plaintiff's identity and obtain personal jurisdiction over the registrant[849]. There is no major campaign initiative about online conflicts, and the issue is dispersed in judiciary decisions forming precedents In the United States. As a result of its federalist type, in the United States, the states have the independence to arrange their Courts and enforce laws on specific issues, specifically in trading and civil instances. With a higher grade of independence, the federal states have the power to determine their legislation of interior bodies. Significantly, the US Constitution mentions some of the rules, consisting of the 14th Amendment, which establishes the principles of due procedure as well as the protection of the regulation to those under the umbrella of the US jurisdiction, also recognised as a right that is not to be attempted by unlawful authorities.

6.7.1 Sanctions of the ACPA

Pertinence, as well as Sanctions of the ACPA, applies to all domain enrolments of trademarks. Effective complainants in suits obtained underneath the act can collect real statutory damages and revenues or select to receive legal injuries varying from $1,000 to $100,000. Some firms have recently efficiently sued under the ACPA, and there are obstructions to seeking such legal actions. Some registrars of domain names offer personal privacy services that conceal the content of domain names' proprietors related to questionable sites, making it hard for trademark proprietors to recognise cybersquatters. Therefore, before bringing a match, a trademark proprietor has to request the tribunal for a subpoena to uncover the proprietor's identity of the infringing website. Due to the high costs of Court procedures, exploration, and even adjudication, several conflicts over cybersquatting are resolved out of court. Usually, conflicts are resolved in the UDRP rules and the URS systems. More conflicts are solved via the UDRP rules, enabling common law trademark cases and fewer procedural demands. The URS system can be used only by enrolled trademark holders with precise infringement lawsuits.[850]

6.7.2 Jurisdiction conflicts

The jurisprudential principle is most frequently used in the legal systems with an Anglo-American practice. United States law is created mainly via statute for classification within the common law system. In this regard, judicial decisions make criteria and direct the application and analysis of the statute for similar situations in the hereafter. It is the so-called forum non-convenient, which develops that a court might refuse to work out jurisdiction over a lawsuit according to an optional evaluation, to stay clear of an unjust or ineffective service to the

[848] *ibid P490*

[849] *ulia Hörnle Internet Jurisdiction Law and Practice, publishe Publisher Oxford University Press,UK, 1st edition, 2021,, p410.*

[850] *Kenneth W. Clarkson, Roger LeRoy Miller, Business Law: Text and Cases, , ibid, p172.*

suits, to the hindrance of the decision by another tribunal that would certainly be taken into consideration convenient for the resolve of the conflict. Recurringly, in the United States legal argument, there is individual jurisdiction, which objects, as a guideline of jurisdiction, to a selection of jurisdiction linked to the location where the thing/property lies *in rem* jurisdiction. When personal jurisdiction is used, the court uses the so-called minimum contact test (see the Yahoo France case above) to justify its verdict. [851]

6.7.3 Applicable law

From online purchases, several problems might emerge, such as disparagement, customer legal rights, copyrights, and others. When faced with the recurring truth that the involved parts are situated in various jurisdictions, how to settle a legal problem about the internet frequently shows up. After identifying the competent jurisdiction, the next action is to launch a legal issue resolution regulation. In the United States, like in Europe, two main regulations prevail: complimentary options and the absence of a choice of legislation. Regarding the relevant regulation to contractual commitments, party freedom is the concept that ensures the flexibility of the code selection. There are clear guidelines for selecting regulations in the EU, developed under Rome I regulation, which is different from the United States, where there is no organised legislation on this topic. In the United States, there is no uniform code to subjugate the matter throughout the country; therefore, it mentions the uses of its jurisprudence. The second restatement establishes that the law picked by the parties will subjugate the contract. This liberty of choice can be limited if the rule is not strongly associated with the legal connection or a basic or state regulation. There is a conditioning aspect between the agreement and the related legislation.
A comparable arrangement is likewise found in the Uniform Commercial Code (UCC). It is a codification of commercial regulations embraced by states, which predicts the power of the parties to select the law relevant to the contract - generally because there are no detailed policies for digital transactions. Likewise, specific transaction rules exist, such as the Uniform Information Transaction Act (UCITA) licensing software applications. Also, it is only adopted by two American states. UCITA establishes the choice of regulation for those contracts, with reservations about consumer protection. Upon the parties' silence, some regulations substitute the lack of ability to choose law. For the UCC, the most substantial partnership to the agreement is selected.

The American Courts will often exert jurisdiction over domain name infringing and other related trademark rights, even if these domain names are possessed by foreign groups or parties or run by foreign internet site users. On top of that, it is worth mentioning that the ACPA gives this power over *in rem* jurisdiction, which grants it over the location of the domain name's registry or domain name owners. Suppose the trademark holders fail to obtain this personal jurisdiction over the domain name owners. In that case, the ACPA gives the trademark holders the right to file a lawsuit *ex parte* against domain name owners[852] even

[851] *Laila Damascena Antunes,Matheus Rosa,Bruno de Oliveira Biazatti,Pedro Vilela,Odélio Porto, Jurisdiction and conflicts of law in the digital ageRegulatory frameworkof internet regulation, , Institute for Research onInternet and Society, 2018, https://hu1lib.org/ireader/5214415 p12.*
[852] *Michael Xun Liu, Jurisdictional Limits of in rem Proceedings Against domain Names, ibid p491.*

though this jurisdiction activity might correspond with the constitutional measure for *in rem* jurisdiction proceedings related to regular property. Such *ex-parte* activities against domain names can weaken the essential policy behind limitations on jurisdiction. These broad assertions of jurisdiction get into the international sovereignty, threaten the ability of the stakeholders to follow their legal responsibilities, and jeopardise the equality principle of the foreign parties. To resolve this concern, it suggests that, instead of terminating any international domain name that violates trademark holders under American laws, courts must impose *in rem* jurisdiction over the domain names that were enrolled in bad faith to benefit from another's trademark. Imposing this infringement of contract demand would support rational plan interests and be more constant with the context and aim of the ACPA[853]. For jurisdiction, a plaintiff may have the requisite partnership with the United States authorities but certainly not with the governance of any personal state. To this facet, two ideas are signified in the primary. First, personal jurisdiction requires a forum-by-forum or even self-governed through sovereign evaluation. The concern is whether an offender adheres to an agenda of routine directed at the community or even economises under the jurisdiction umbrella of a given sovereign to ensure that the sovereign can subject the applicant to judgement concerning that conduct. Naturally, personal jurisdiction limits statutory power not as a concern of, although as a matter of personal freedom, for due process guards the individual's right to become subject simply to an authorised agency.

The defendant might be under the authority of the US tribunals; however, not of any particular state. For jurisdiction, a plaintiff might have the requisite relationship with the United States Federal Administration but not with the state and the federal government of any private state. That would certainly be an extraordinary instance. The State Courts are readily available and exercise general jurisdiction if the opponent's residence is domiciliary; furthermore, if one more state insists on the jurisdiction in an improper case[854].

The registrars and registry have a real-world existence, and the domain name is not territorial and virtual. Because the domain name is unique, it has worldwide validity, and the legal owner can only use the exact domain name. This memorability and originality of domain names make them comparable to trademarks since they operate as resource indications. Domain names are useful as they are qualified to be auctioned, offered, and transferred for useful factors to be considered. Domain names are also left out because the registrant has fully exclusive usage of the domain names.[855] These attributes make domain names comparable to intellectual property. Several United States Court choices have considered whether the domain is a type of immaterial property. To this point, the well-known judgement (Kremen v Cohen) declared by the Court of Appeals considered domain names as intangible property,[856] such that they can be the subject of conversion activity. It is worth noting that *in rem* jurisdiction can be related to whether domain names are property because, *in rem* jurisdiction, exertion needs to know the place of this property. Accordingly, the US Court of Appeals for the Ninth Circuit in the case Office Depot v Zuccarini states that

---

[853] *iBid,p470.*

[854] *Barbara Allen Babcock, Toni M. Massaro, Norman W. Spaulding, Myriam E. Gilles,*
Civil Procedure: Cases and Problems, Publisher Wolters Kluwer, new York, 7th edition,2021,p143.

[855] *Julia Hörnle Internet Jurisdiction Law and Practice, ibid, p408.*

[856] *ibid, p408.*

the US District Court for the Northern District of California can work out *in rem* jurisdiction over property located within their geographical border. Verisign, the main registry of *.net* and *.com,* remained in the pertinent area, enabling a receiver's consultation to satisfy the financial debt.

Contrary to this decision, in *NSI v Umbro Internationa1*, the Virginia superior tribunal held that a garnishment demand could not be connected to domain names, as they are not a kind of responsibility or an option of property action. According to the registration arrangement, the Court held that utilising a domain for a particular duration is a contractual right. However, it must also be explained that the Court of Law did not directly oversee the standing of domain names. Similarly, the Kentucky Court rescinded a judgement by the first instance court, which had ordered the forfeiture of 141 domain names utilised for gambling sites, on the cause that the wording of the regulation did not include domain names amongst the things reliant on being seized. In 2012, the German Superior Court indicated that an authorised domain, *gewinn.de,* did not make up an outright property right as defined by German law; rather, it was held to only provide equal rights that involve the parties concerned. Thus, the German tribunals have recognised economic and legal rights in the domain.[857]

Furthermore, the German Constitution does not suggest that domains, as safeguarded, are property in a civil regulation sentiment. While the law might shield certain economic and legal rights in domain names, this does not always relate to domain names as being property. The standing of a domain as immaterial property is ultimately uncertain and varies substantially between jurisdictions. Under English regulation and case-law, no instance has been noted that domain names are classified as property or that an unjustified loss of a domain can amount to the tort of transformation (see for example the decision of the High Court in the case *Patel v Allos Therapeutics*).[858.] Domain names are also omitted if the registrant has the unique use of the domain name.

Another considerable conflict regarding the ACPA arose from the legislation's point of view connected to the domain *barcelona.com.* This domain had been enrolled individually by someone who lived in Spain and operated a website for travellers who desired to explore the city. The registrant later developed *Barcelona.com, Inc*., a Delaware association, and moved the name. The Municipality Council initiated a UDRP rules case and got a positive judgement requesting the domain name to be transferred. In this regard, in the case *Barcelona.com Incorporated v. Excelentísimo Ayuntamiento de Barcelona,* the court turned around the previous judgement that was in line with the status of the UDRP rules committee. The US Court of Appeals for the Fourth Circuit argued that the domain holder had truthfully developed a valid reverse domain pirating beneath the ACPA (15 USC versus the city council) because of the council's successful prosecution of a UDRP's case against the operator. The Fourth Circuit declared that the district tribunal incorrectly used Spanish regulation rather than US regulation based on the essential doctrine of territoriality. It concluded that under US regulation, a party could not have a valid trademark for a

[857] *ulia Hörnle Internet Jurisdiction Law and Practice, ibid, p409.*
[858], *ibid, p409.*

geographical location; the plaintiff's enrolment of the *barcelona.com* domain name was legal and also qualified for protection under 15 USC[859].

6.8 In rem jurisdiction in the EU

In the EU, a legal environment was created to minimise disputes arising from virtual space interaction. The European Commission acknowledged this task as vital for the continuation and growth of the profession and economic combination, offering an additional enhancement to the Digital Single Market policy. It is necessary to examine the European approach regarding jurisdiction over domain name conflicts. In terms of EU jurisdiction rules, the Brussels I Recast regulation 1215/2012 (hereinafter brussels I Recast regulation or Regulation 1215/2012), played an essential role in organising the dispute over the domain in EU cyberspace. At this point, the council and the European Parliament approved this regulation, which wass necessary to recognise the digital due procedure in the EU. Regulation 1215/2012 replaced regulation 44/2001 (Brussels I). The latter was believed to be satisfactory; however, it was necessary to clarify and explain the policies regulating jurisdiction and acknowledgment of choices, advertise the free activity of options, and support access to justice. It is believed that the regulation was very meaningful as it applied a solid structure for creating a worldwide personal rule in Europe. It is essential to mention that, based on Article 1 of this regulation, fiscal customs, and administrative issues are not applicable. The Brussels I Recast regulation will develop the jurisdiction relevant to conflicts entailing civil and business issues further.

6.8.1 Conflicts of Jurisdiction

In the European Union, the jurisdiction's directions are based on the *forum defensor* principle. As a basic rule, the European regulation appoints jurisdiction to the tribunals of the member state where the offender is domiciled, regardless of his citizenship. The handling of web lawsuits needs to be set as the domicile of an electronic and digital provider taking legal action against in tribunal. It is not consistently simple to establish its domicile. Suppose a business involved in the online sales section, based in France with web servers in Spain, yet which faces problems from a German customer regarding shipping time and the consistency of the negotiated products. The simple question arising from this complicated situation is, where is this business or firm domiciled? [860]

The European Union's Directive on electronic commerce (2000/31/ EC) identifies the domicile of a business offering services over the Internet as the area that bears its financial activity. If financial activity is offered from various regions, one must specify the facility regarding service arrangements. Generally, the decision about proficient territory obeys the principle of *forum defensor*. There are exceptions to this main principle, mentioned in articles 7 to 24 of the Brussels I regulation. These are special proficiencies, capability in insurance

[859] *Pedro de Miguel Asensio, Conflict of Laws and the Internet Publisher Edward Elgar Publishing, 2020,ibid*

[860] *Laila Damascena Antunes,Matheus Rosa,Bruno de Oliveira Biazatti,Pedro Vilela,Odélio Porto, Jurisdiction and conflicts of law in the digital ageRegulatory frameworkof internet regulation ibid,p9.*

coverage matters, consumer agreements, competence in specific contracts concerning work, and extension of competence. As regards the concept of *forum defensor*, regulation 1215/2012 establishes, as mentioned in Article 7(1), that the defendant might have a claim filed against them in the location where a specific obligation was or ought to be satisfied. To be sued in a state besides the one in which they lie, it must be noted in the warrant that any dispute will certainly be settled in the member state where the contract has been wrapped up. Article 7(2) concerning disputes regarding a non-contractual nature indicates that the lawsuit must determine where the hazardous event occurs. Situations regarding sales of services or goods are prevalent on the web, making these rules necessary in fixing administrative problems.[861]

6.8.2 Applicable law

In the EU, when resolving the conflict over domain names in cyberspace, the first step must specify the jurisdictional power. The second step requires determining the applicable law. The EU has developed effective legal instruments for domain name conflicts, including Rome I and II regulations. To this point, Rome I regulation No 593 / 2008 on the law applicable to contractual obligations and Rome II regulation No 864/2007 regarding the conflict of laws on the law applicable to non-contractual obligations was limited to treating only civil and commercial subjects. Article 3(1) of the Rome I regulation provides that the law chosen by the parties shall govern the contract[862].

The author believes that the overwhelming majority of domain name conflicts do not stem from contract breaching; hence, Article 3(1) that provides the law chosen by the parties shall be shown[863] has no place here unless a new alternative mechanism has set the position in this matter. The author illustrates this issue as seen below.

The Rome II regulation manages non-contractual obligations and determines that the regulation relevant to non-contractual responsibilities will certainly be the state where the damages occur. Article 4(2) states that if the parties reside in the same place, the relevant regulation will certainly be where they have residence. Accordingly, applying Rome I and II regulations to cyberspace conflicts goes over the connection between substantive legislation and policies to harmonise with the EU legal system completely. In this regard, there may be disputes in cyberspace that do not directly attach to the abovementioned principles. Also, courts cannot apply the regulation of Rome I or Rome II in such situations. Relating to the place of the damages, Alexandre Libório Pereira suggests that there will certainly be "the application of the state's regulation where the injury happens referring to both the causal

---

[861] *Laila Damascena Antunes,Matheus Rosa,Bruno de Oliveira Biazatti,Pedro Vilela,Odélio Porto, Jurisdiction and conflicts of law in the digital ageRegulatory frameworkof internet regulation, ibid, p10.*

[862] *Ibid, p11.*

[863] *David W. Bowker, David P. Stewart, Ristau's International Judicial Assistance A Practitioner's Guide to International Civil and Commercial Litigation s, oxford press, UK,,2nd edition,2021, P115.*

- Yvonne Baatz,Ainhoa Campâs Velasco,Charles Debattista,Özlem Gürses,Johanna Hjalmarsson,Andrea Lista,Filippo Lorenzon,Andrew Serdy,Michael Tsimplis, Maritime Law fifth edetion. Publisher Taylor & Francis, 1st edition,2021 ,P 61.

- Scott J. Shackelford, Anjanette H. Raymond, Eric L. Richards, Legal and Ethical Aspects of International Business Publisher Wolters Kluwer Law & Business,New York 10th edition, 2021,P161.

- Graham Stephenson, Core Statutes on Contract, Tort & Restitution 2021-22,
red globe press, London, 6th edition, 2021 P 129.

- Francis Rose, Blackstone's Statutes on Contract, Tort & Restitution 2021-2022, Publisher Oxford University Press, UK, 32th edition,2021,P 391.

event and the damage." [864] Article 202 of commission regulation (EC) No 874/2004 of April 28, 2004, declared that the court could have those laws or agreements to practice international jurisdiction according to protective and provisional measures based on international agreements and EU legislation.

6.8.3 Rome regulation mechanism related to in rem jurisdiction

Articles 6 and 8 are not the only mechanisms that the Rome I regulation has to ensure the application of required regulation shields weaker contracting parties. Articles 3 and 4 of Rome I restrict individual autonomy, intending to protect against events unnaturally connecting the contract to any country to which it does not have any link, with the only objective of preventing the application of the necessary nationwide or European stipulations. According to Article 3(3), Rome I, when a case is only linked to one solitary Member State, the stakeholders' choice of international law need not influence the application of the locally compulsory arrangements of the national law. Similarly, according to Article 3(4), Rome I indicates that if the matter is only linked with one of the numerous member states, the option of non-member state legislation by the events will certainly not influence the use of non-member state regulation by the main litigants. It will not impact the use of necessary EU regulations. This arrangement is also a potential device for protecting the legal interest of stakeholders, and they will certainly be stopped from preventing the relevance of mandatory provisions stemming from EU regulations in intra-EU circumstances. Furthermore, Article 9 of Rome I guarantees the use of the so-called overriding necessary arrangements, which should be internationally mandatory no matter the legislation suitable to the contract. Overriding obligatory formats is specified in Article 9(1)[865]

6.9 In rem jurisdiction in Latin America

Latin America's legal structure is complex because, while Brazil and Colombia have developed publicly accessible and clear regulations online, states such as Uruguay, Argentina, and Chile have no rules or specific laws for controlling conflicts on the net; instead, they represent a huge basic collection of private global legislation, which was not evaluated by this research. The scarce instance legislation typically does not present instances entailing conflicts in the online world with international elements, making it difficult to determine how they are resolved. Besides jurisprudential and legal research, elaborating an index of disputes is required to understand problems in the online world. Via a possible index of conflicts, with information on judicial conflicts concerning the internet, the legislator's job becomes less complex by making it feasible to seek advice from a specialist.[866]

---

[864] *Laila Damascena Antunes,Matheus Rosa,Bruno de Oliveira Biazatti,Pedro Vilela,Odélio Porto, Jurisdiction and conflicts of law in the digital ageRegulatory frameworkof internet regulation ibid, p112.*

[865] *María Campo Comba, the Law Applicable to Cross-border Contracts involving Weaker Parties in EU Private International Law, ibid,,p99.*

[866] *Laila Damascena Antunes,Matheus Rosa,Bruno de Oliveira Biazatti,Pedro Vilela,Odélio Porto, Jurisdiction and conflicts of law in the digital ageRegulatory frameworkof internet regulation,ibid, p22.*

7. The alternative for the jurisdiction dilemma and the main challenges.

Because *in rem* jurisdiction encounters many difficulties in resolving the conflict in the digital world to keep the right of the main stakeholder, some challenges need to be eliminated before the court initiates the procedure to solve the conflict. Among other challenges, the visibility of numerous parties in different parts of the globe, who have only virtual relationships, could be the main challenge. Such challenges could push legal commentators to think seriously about the best alternative solution for such jurisdiction issues in cyberspace. In this regard, the author explains these challenges and tries to suggest a solution to this problem.

7.1 Challenges

The most notably concerning of all *in rem* jurisdiction situations is that it observes the legal choices in very significant interaction with the doctrines, concepts, norms, as well as procedures that traditionally underlie the jurisdiction related to the law conflict in cyberspace doctrine, selection of law, or acknowledgment of judgment[867]. The challenge with jurisdiction in cyberspace is the visibility of numerous parties in different parts of the globe who have only virtual relationships. Then, suppose one party desires to take legal action against the other. In that case, the question is where litigants can sue each other. In this regard, traditional jurisdiction's demands typically include two issues: firstly, where the defendant's headquarters are, and secondly, where the reason for the activity occurs.
Nonetheless, in cyberspace, it is challenging to exert jurisdiction smoothly. The web is substantively multinational. Because the world wide web is limitless and non-centralised, a single country's jurisdiction over online practices always results in disputes and spillover effects of jurisdiction. The jurisdiction in one region may be an infraction of the sovereignty of one more nation. One online practice usually produces equivalent effects in several countries. Because of the standard jurisdiction regulations and the concept of influence, one situation might fall under the jurisdiction of many countries.[868]

Kettemann has diagnosed the problem of domain name jurisdiction in cyberspace. In this regard, he adds, jurisdictional scholars are especially critical of the "extraterritorial extension of national jurisdiction," which they see as—problematically—becoming the real politic of the internet[869]. However, it is helpful to consider the opportunity of utilising domain names in cyberspace to enforce international requirements, not just standards, versus infringement of worldwide trademarks. In this regard, among the obstacles to developing international legal systems is the lack of resources available to enforce decisions by international Courts, which is necessary for introducing global standards and norms. The issue is still primarily theoretical since no international civil tribunals exist for personal disagreements. The International Tribunal of Justice involves disputes between states. However, worldwide settlement inhabits a lot of this area effectively.

---

[867] *Peer Zumbansen, the Many Lives of Transnational Law: Critical Engagements with Jessup's Bold Proposal, ibid,p242.*
[868] *Matthias C. Kettemann, the Normative Order of the Internet: A Theory of Rule and Regulation Online, ibid, p217.*
[869] *ibid, p217.*

As total worldwide mechanisms are also designed for adjudication, the requirement for appropriate enforcement actions will certainly improve. Nonetheless, there will be several models in which national tribunal enforcement will exist. The standard principle is that the domain names would be revoked as a solution under an adjudicatory choice by an international agency. The domain name cancellation treatment is insufficient because it does not grant compensation for statutory damage to the main stakeholder (trademark holders, essentially). It does, nevertheless, have deterrent value. Utilising the domain names as a treatment for applying global adjudicatory decisions would surely contend at the very least three components, including rules for traditional territory, the regulations for adjudicatory jurisdiction, and also guidelines for ensuring compliance, at least, in the ability to bypass consequential jurisdiction, implementation, or remedies from national tribunals.

Furthermore, the adjudicatory and prescriptive jurisdiction policies have been exercised and are acknowledged in common global law. Such procedures are essential to decide which adjudicatory verdicts and substantive norms would be entitled to enforcement with the domain names system. When the substantive criteria and adjudicatory resolutions rise from global bodies and associations, their jurisdiction will be established based on the documentary sources of their power treaties for the immediate future. The countries' legal systems vary, so the Internet inevitably faces irregular jurisdiction.

7.2 Disadvantages of UDRP rules

One of the disadvantages of the UDRP rules is that they are limited to cases involving domain names registered in bad faith. Besides, this mechanism is still lacking in statutory damage compensation. Notwithstanding those practical issues , it is beneficial to consider utilising Internet domain names to implement international standards generally, not just norms against violation of well-known trademarks.

One of the problems in establishing global legal systems is the lack of resources to apply verdicts by tribunals and so establish global norms of behaviour. This issue is still theoretically under investigation because no international civil tribunals are devoted to this conflict-related conflict with contested domain names. However, international arbitration would effectively solve much of this conflict in cyberspace[870].

One of the problems in developing worldwide legal processes is the lack of the ability to impose judgements by international tribunals implementing global standards of norms. The issue is still mainly theoretical since there are no genuinely global civil tribunals for domain name conflicts, contrary to the International Court of Justice involving the matters of disputes between different countries[871] In both of these (potentially overlapping) instances, applying an international adjudicatory judgment against the domain names can be a reliable supplement to the efficiency of the worldwide legal regime. The fundamental idea is that the domain would be revoked as a solution under an adjudicatory judgment by a global body. As clarified above, the domain name cancellation solution is incomplete because it does not reimburse the complainant for damage. It does, nevertheless, have restrictions and deterrent

[870] *ibid, p7-237.*
[871] *ibid, p7-236.*

value. An intellectually comprehensive system for using domain retraction as a treatment for imposing international adjudicatory decisions would certainly contend at the very least three aspects, including policies for traditional territories: rules for the jurisdiction of adjudication and guidelines for ensuring conformity amidst the analog of the implementation process; the last order calls for a domain name to be cancelled. The authoritative and adjudicatory territory policies have previously been applied successfully and are acknowledged in popular global legislation. Such policies are essential to determine which substantive standards and adjudicatory judgments would be enforced via the domain name system.[872] As an example of the underlying problem, it is believed that due to the competitive pricing offered for *.1NFO* registrations, many were made for malicious purposes, such as promoting spam, malware, and phishing. As noted by John Levine, author of the Internet for Dummies and a former member of ICANN's at-large advisory committee, in the "Mapping the mal web revisited" report from antivirus vendor McAfee, “The very high numbers of bogus sites in *.cn* and *.info* makes sense because they are among the cheapest places to register, with the wholesale price for *.cn* now being about 15 cents"[873] .

In this regard, the author believes the best way to avoid jurisdiction challenges in cyberspace is to work on the UDRP rules’ mechanism of WIPO, not as an arbitration tool but as an international Court limited to domain name conflicts and trademark infringement rights related to the domain names. The advantage of this situation is that it will avoid all the jurisdiction's negatives and disadvantages. Besides, all the stakeholders and other litigants have already contracted with ICANN. In this regard, ICANN needs to develop a policy to deal with all cases related to domain names besides having the power to enforce and fulfil its verdicts.

7.3 UDRP rules as possible framework for the operation of an international Court

The author believes that the UDRP rules are the best alternative to solving jurisdiction issues in cyberspace if it was reshaped and developed from an arbitration tool to an international court with an enforcement tool to resolve domain name conflicts in cyberspace. Such an international court would not need jurisdiction power to practice its authority. Besides, the contract principles will be embedded for litigants because all stakeholders, particularly the trademark holders, have registered their domain names and agreed to use UDRP to solve their conflicts. In this context, it is noteworthy that the conflict laws issue will have vanished from this process.

Moreover, developing this international Court mechanism entails having enforcement tools. The author, in this regard, suggests that UDRP rules can borrow some legislation from the ACPA and work on it. For instance, it is suggested that the court might expand its core from targeting domain names' bad faith registration behaviour and take further actions related to comprehensive untrademarked personal names and providing an *in rem* right of action. For instance, it might take a quantum leap in protecting the trademark holder's right, expanding

[872] *ibid, p7-238.*
[873] *ibid, p7-240.*

its action from transferring or cancelling the domain name to offering statutory damages per domain name infringement.

The author suggests using a model similar to that of Interpol to achieve enforcement power related to compensation issues. Bearing in mind that the litigants might be foreigners and live in different regional areas, a UDP court could achieve more success as an international Court than traditional Courts dealing with thorny issues such as conflict laws and conflict jurisdiction.. In this regard, experts argue that the UDRP rules must have been provided an opportunity before such regulation of the ACPA was embraced[874]. The author agrees with this point of view. The UDRP rules carried the seed of success by forcing the parties to adopt its mechanism if a conflict happened. Furthermore, it is vague whether the UDRP rules would have sufficed to protect the legal rights of trademark holders, yet provided the schedule of the new ACPA, the full force of the UDRP rules may never be tested. Moreover, in light of the geopolitical polarisation in cyberspace and geographical regions, the worry arises that other countries will strike back by passing similar laws, subjecting domain name registrants to such rules in numerous jurisdictions[875.]

[874] *domain Names and Trademarks, March 5, 2000 https://cyber. harvard.edu/property00 /domain/ main. html#discussion*
[875] *Ibid.*

CONCLUSIONS

According to the hypothesis question related to the domain name's legal nature, the dissertation has answered the question of the hypothesis of whether domain names can be registered as a trademark; furthermore, the study has gone beyond that and justified that the legal nature of a domain name is a digital trademark. In this context, one of the best results that the study has concluded, as the author believes, is presented in the best understanding of the legal nature of the domain name.

The nature of domain names is a key issue in cyberspace. Knowing the legal nature of domain names helps us to deal with these phenomena in the best way as long as it can present a long-term guarantee to the cyberspace community and stakeholders' rights and give dynamic legal stability to the investment in the digital era. There is currently no consensus on the legal nature of a domain name. The dissertation tries to offer insights into the legal nature of domain names to protect further and recognise rights over contested rights of domain names. Determining the legal nature of domain names is the right way to provide comprehensive protection against the infringement of rights associated with domain names and trademark owners. The precise nature of the legal nature of domain names contributes to resolving the associated tendencies. It provides a more effective way to prevent such violations. In contrast, the frequent disputes and violations of domain names and trademarks associated with domain names were (we assume) because of the lack of clarity on the legal nature of domain names. The best conclusion we can reach is that the best legal adaptation of domain names, which provides comprehensive protection, is that domain names are considered a digital trademark as part of intellectual property, with the special characteristic that they are practiced only in cyberspace.

The dissertation has examined the search engine hypothesis. It has been proven that search engines have no huge impact on reducing the trademark vs. domain names conflict. Moreover, we found some clues about search engines' involvement in trademark infringement in cyberspace. Our findings indicated that the relationship between the main stakeholder is unstable. Besides that, the essence of the conflict is financial.

As for the hypotheses related to the resilience or immunity of the domain names industry, the question arises as to whether the domain names industry is immune enough against global crises, for instance, the COVID-19 crisis in the domain name industry. The dissertation shed light on how global crises could impact the domain name industry, particularly the health crises such as the COVID-19 pandemic. To this point, the dissertation analysed several reports and studies in this area. One of the researchers claimed no significant impact on the domain names industry. The author has refuted this argument and explained the logical reasons beyond this rejection. To the contrary, the dissertation proved the impact of COVID-19 on the domain industry on different levels as social behaviours (increasing internet users per increasing domain names registration, the illegal use of domain names related to COVID-19 during the pandemic in a different way as cybersquatting, misleading campaigns, using ransom viruses, and other malicious of materials, in particular, those that target health systems and care institutions, threatening the people who depend on

them, particularly the old and the sick.

Furthermore, the dissertation was able to prove the impact of COVID-19 on the domain names industry at different levels. One of the results of this study is to identify the shortfall of preventive measures developed by UDRP rules to fight cybersquatting and other trademark rights infringements, particularly the Clearinghouse mechanism. This study has explained the reason beyond the falling of this mechanism. One important result of this study is that governmental domain names' credibility was threatened during the COVID-19 pandemic. As the study mentioned above, governmental COVID-19 domain names became unsafe. In several cases, the right to ownership of these websites could not be effectively determined.

Furthermore, during the pandemic, several individuals seeking enrichment ignored ethics when they accepted registered domain names related to COVID-19. In this context, this dissertation investigated to what extent the ethical criteria must be included in domain names traded, in particular domain names related to the COVID-19 theme purchased with the intention of reselling for profit. In return, the importance of this study presented a rethink about free speech principles when it comes to sharing, posting, or forwarding misleading information or rumours that affect human health and society, for example, the campaigns to reject vaccines or other health protocols during the pandemic and consider that as a crime because there was a strong relationship between these campaigns and increased cases of COVID-19 infections. The dissertation indicated that death cases are higher among people who reject vaccinations under the influence of social media websites and other internet domain names connected to COVID-19 terms. On top of that, the authors believe the registry agencies played a large role in terms of the COVID-19 impact on this industry by allowing nonlegal rights holders to register COVID-19 domain names, including other individual rights, for instance, allowing them to have rights over domain names containing the Facebook trademark, without undertaking any further investigation to prevent these illegal registrations. Moreover, the dissertation established that registered agencies had registered some domain names in their favour, revealing the bias of these agencies and the conflict of interest.

The dissertation also shows that instability predominantly returns to registration agencies and the first-come, first-served principle. As for the question arising from the hypothesis of domain name's first-come, first-served registration system, based on the evaluation of domain name registration's priority according to the trademarks registration system, it turns out that the trademark registration system was more effective in preventing post conflicts in terms of the potential contested rights. On the contrary, domain name registration based on priority (first come, first served) makes the conflict between main stakeholders in cyberspace more likely due to the lack of examination.

On the other hand, failure to take advantage of the existing trademark examination system resulted in losing the opportunity to rely on the existing database that includes trademarks, which would have reduced the possibility of subsequent disputes over potential rights to the registration of domain names that include those trademarks. In addition, the advantage of non-duplication of identical domain names' registration in cyberspace has not been taken advantage of, which would be effective if a trademark examination system is

used. It would prevent and reduce potential conflicts between trademark holders and domain name owners by analysing the regulations related to domain names registrations, the presumption being that the authority is wary that the adaptation of the priority principle (first-come, first-served principle) alone without conducting the needed examination will lead to more conflicts in the future. It becomes a tangible and touchable reality that explicitly states liability exemption by trying to avoid taking responsibility for the stakeholders.

As for the hypothesis related to cybersquatting's legal character, the dissertation concluded that the legal character of cybersquatting could fit all possible claims that bring complete protection against cybersquatters, according to the national legal system. The main criteria that should be considered are the amount and effectiveness of protection against cybersquatting. The legal character of cybersquatting is connected to understanding the nature of domain names *per se*. In this context, one obstacle to understanding the legal personality of cybersquatting is the lack of clarity concerning the nature of domain names. The legal perspective considers it a trademark, part of it, or not. Most courts could not agree on whether domain names are property rights or contract services. In this context, the lack of clarity concerning the domain name's nature is reflected in understanding the legal nature of cybersquatting. In light of this, the legislation's absence made criminalising domain name cybersquatting very hard, at least at the early stage of the emergence of this phenomenon. Even when enacted, the ACPA could not clarify the nature of cybersquatting because this law did not have any punishment. Only monetary compensation equal to one hundred thousand dollars maximum per domain name, which is not enough to consider cybersquatting a crime. The absence of explicit discipline in the ACPA begs the critical question of whether cybersquatting is illegal. Compared to the principle *"Nullum crimen, Nulla poena sine lege,*" criminal offenses and penalties are determined only by the law.

Furthermore, it doubts whether civil compensation can be equivalent to punishment according to the principle no of crime, no punishment without law. This question is left for discussion: if there is a special law to fight cybersquatting, why do courts sue cybersquatting under different legal approaches, such as unfair competition, passing off, and dilution? The recognition of cybersquatting's legal nature accurately needs to consider the effectiveness of the protection given to trademark holders against the cybersquatters. The number of cybersquatting cases can measure this protection. Back to cybersquatting, it was noticed that the number of cybersquatting is getting high; the WIPO center reported a 20% increase in cases filed in 2004[876]. The rising cybersquatting cases, through the existence of the ACPA, indicate that the protection provided by the ACPA is minimal for one reason or another. It also concluded that the courts use of a different legal adaptation of cybersquatting suggests that all these attempts could not provide enough protection against cybersquatters because intellectual property rights are often treated as civil rather than criminal. The difficulty in pinpointing the legal nature of this phenomenon might partially be explained by the classic view of the conflict based on the illegal behaviour of cybersquatters. The conservative image considers individual strife between the two main stakeholders: trademark holders and domain name owners. The conflict in fact affects all cyberspace communities, even without

[876] *McGeorge School of Law, McGeorge School of Law, Symposium: I think I can, I think ICANN: regulating the Internet ... or not, McGeorge School of Law, University of the Pacific, 2008, p 33.*

considering the nature of borderless cyberspace with interlacing interests. A peek within a comprehensive vision: the cybersquatting threat acts on all cybercommunities.

Furthermore, the vital economic section would be a turning point to pave the way to reveal the best legal adaptation for the nature of cybersquatting. In line with that, it can provide complete protection against cybersquatters. It is worth discussing whether the ACPA or/and other alternative legal approaches used to be the legal adaptation of cybersquatting have given the expected result. In this regard, by analysing these approaches, we can conclude the following:

Trademark infringement does fit the violation under a legal system's trademark law[877]. Passing off does fit losses based on the harm resulting from the trademark holder's representation of commodities or services[878]. Unfair competition does fit business action losses that deceive or confuse consumers about a good or service source. Dilution of the famed trademark does fit for "Blurring" the distinctiveness or "Tarnishing" the reputation and position of a famous mark[879]. Ransom and Blackmail fit the nature of action and goal of cybersquatters that capture the domain name of the trademark holder to force him to pay the ransom. In terms of the ACPA, the law was designed to fight cybersquatting. Nevertheless, its ability to do so is not enough to eliminate the cybersquatting threat because this law does not impose penalties.

Moreover, based on that and according to these different approaches, we can assume that cybersquatting can jeopardise the financial interest of any economy as a serious crime. This dissertation has partially justified its hypothesis that the best legal adoption that can provide adequate protection is considering cybersquatting a financial crime with criminal penalties and monetary damages. The concept of cybersquatting should not be limited to registration. It must contain any way domain names could be controlled or taken. The ransom virus is the best example of the damages that affect virtual and non-virtual economies, with billions of dollars lost worldwide.

As for the question raised from the hypothesis of whether UDRP rules were formulated effectively to deal with reverse domain name hijacking, the study has concluded that at the early time of the conflict between main stakeholders in the digital community, the agency responsible for solving the conflicts between domain name owners and trademark holders was founded to protect trademark holders against cybersquatters. However, the principles used and applied were more active and suitable to protect trademark holders. They were less active and suitable for protecting domain name owners. On the other hand, reverse domain name hijacking's case approval depends on the factual circumstances surrounding each case, which makes it less protected. This study also concluded that neither the UDRP rules nor the ACPA provides much protection in reverse domain name hijacking cases, so civil actions remain crucial solutions in many cases. One of the main reasons behind that, as the study did show, is presented by UDRP's policy which was designated predominantly to deal with cybersquatters and not qualified enough to deal with RDNH; this study has fully proved, with reference to a number of reverse domain names hijacking cases shown in this study, that

---

877 JS Hatcher, The UDRP: A Guide for SMEs and Consumers on domain Names and domain Name Disputes, A Report for the International Intellectual Property Institute July,2007, p34.

878 ibid, p34.

879 ibid, p34.

UDRP rules have failed to provide enough protection to the legal domain names owner as they deserve. This study has investigated that UDRP rules must be developed on the legislative level to extend civil compensation. As for domain name dispute resolution procedures, the dissertation indicated the crucial case of BPOST as a turning point related to the domain name dispute resolution procedures, because the disappointing result for the BPOST trademark holder sounds the alarm over the leading standard: first-come-first-served, which is crucial for legitimising the originality of the contested domain names, mirrored the advantage given to one of the domain name conflict's parties. Furthermore, the dissertation has indicated no concept of territoriality relevant to domain names. Constantly shielding the one who registers the domain is a conscious decision to take care of contested domain names bearing in mind the complexity of the domain names dispute. The above case is an example where the domain owner's purpose in registering the domain was to unjustly maximize the complainant's unregistered mark to get trademark legal rights. This case also showed that the panel ignored some subjective clues that could have established bad faith intention against that party, for instance, a business merging shortly before or after the case; besides, the party was a previous staff member following the complainant's filing of a trademark request[880].

Another hypothesis was that the essence of the conflict is predominantly financial; the dissertation has proved that this conflict reflects the importance of the domain name economy; furthermore, the study has emphasised that it needs to be coded in the legal frame to be solved. In this context, the study indicated that real financial costs would contain the minimum and maximum cost fee, loss profit, and anticipated profits for the economy of domain names. To this point**,** UDRP rules are limited to returning or cancelling the domain name without any statutory damage. This study considers the conflict over domain name threats and the domain names industry. Besides that, the domain name industry plays a crucial role in e-commerce. Another fact the study found is that the economic effects of the domain name registration fees over the domain names industry will depend on total domain name numbers and the minimum or maximum fee rate offered by registers. One of the most important features of the economic effect of domain names is taxable income to the local economy, where some amounts of these shares will be turned into taxes.

Regarding the ICANN extra remedies hypothesis, can these extra remedies be effective separately? Or must they be combined? The study has concluded that many instruments created by ICANN to deal with new challenges could be more confusing and hinder this organisation's main mission. The study has concluded that ICANN's working group has finished considering six major and overarching topics; moreover, it has developed different work tracks to resolve some issues. To name a few: subjects associated with the total procedure, assistance, and outreach, besides the statutory and regulative subjects; and matters connected to domain names string, objections, and conflicts; furthermore, the group works hard on internationalised domain names, functional and other technical issues; in addition, it tried to solve the problems of the top-level domain that consist of geographical names[881].

Even though the ICANN group has revised all RPMs and other objection mechanisms mentioned above, they still need more revision. It would be more accurate if the ICANN

---

[880] *ibid, p3.*

[881] *Luc Seufer, the next round of gTLDs is around the corner, August 9, 2019, https://ebrandservices.com/the-next-round-of-gtlds-is-around-the-corner/.*

group combined all these mechanisms within the UDRP rules rather than designing them separately. In this connection, such separated frames could waste the time and efforts dedicated to finding a reliable resolution mechanism and make the essence of this mechanism empty and meaningless. For instance, if the complainant infringed trademarks by different domain strings, one under gTLD and the other under the second top-level domain name string, then it supposes he would submit two different complaints within two different mechanisms to settle the cases related to his infringed trademark rights. Besides, there will be two different panels that might make contractual decisions.

Furthermore, the separated mechanism could have different regulations that might hinder flexibility, accuracy, and centralisation of decisions resulting from different panels related to infringing trademark rights. Moreover, these mechanisms were turning points for the registry operator, bearing in mind that the registry agencies enjoyed immunity against other stakeholders at an early stage of cyberspace emerging and early conflicts between trademark holders and domain name owners. Furthermore, giving immunity to the registry operator was the main reason for igniting the conflict over domain names in the early stage of cyberspace and other rights related to trademarks in cyberspace. PDDRP has made the registry operator responsible for this connection and liable for his behaviour toward other stakeholders. On top of that, and in terms of PDDRP, the specialist committee might advise a range of vast enforcement tools if the registry provider is responsible under the Tm-PDDRP, including preventive measures against further infringing registration in the future[882]. Another suggested penalty is to freeze the acceptance of new domain enrolments in the gTLD until the offense(s) recognised in the determination are treated or a set amount of time is allocated to fix it.[883]

Moreover, in a very exceptional situation, the suggested remedy supported the termination of the registry contract if he acted in bad faith[884]. One of the most remarkable updates over this mechanism, especially the trademark PDDRP, is the introduction of the appeal stage. Though this step comes late, the author believes it gives conflicting parties more credibility, flexibility, and satisfaction. Another issue that deserves consideration is that some of these mechanisms keep the relationship hierarchy between ICANN policies and the judicial system by prioritising registration agreements to use ICANN policies to resolve the conflict before that person can approach a court. For instance, the main policy of ICANN related to using UDRP rules has declared that approaching UDRP rules as a way to resolve the conflict is mandatory to validate domain name registration. In contrast, another mechanism has given up this hierarchy by approaching the court concurrently with the case heard within trademark PDDRP. As an example, in this connection, article 22.2 declared that: "In those cases where a Party submits documented proof to the Provider that a Court action involving the same parties, facts, and circumstances as the trademark PDDRP was instituted before the complaint filing date in the trademark PDDRP, the Provider shall suspend or terminate the trademark PDDRP"[885].

[882] *article 18.3.1 Trademark PDDRP.*
[883] *ibid.*
[884] *ibid.*
[885] *Ibiud, Article 22.2.*

Moreover, in some mechanisms, ICANN kept the door open before the possible compensation to any possible infringing triggered by any stakeholder, including the registry operator. For instance, at TM PDDRP, ICANN indicated there "nothing prohibits ICANN from imposing remedies at any time and of any nature; it is otherwise entitled to impose for a registry operator's non-compliance with its registry agreement."[886] The author believes that if ICANN has embedded monetary penalties and compensation within its mechanism, it will make it very independent and flexible, meeting the requisites of the stakeholders in cyberspace. Furthermore, it gives these mechanisms huge momentum and makes them more practical than the court approach.

As for the confusion hypothesis, the dissertation has examined the basic grounds of the conflict based on the Lanham Act, trying to answer the question of whether registration and using a domain name identical to a trademark are enough to establish initial interest confusion especially true of a weak trademark or not.[887] In this respect, there are differences in the examined judicial practice. In the case Interstellar Starship Servs.Ltd. v. Epix, Inc[888], the United States Court of Appeal for the Ninth Circuit looks at the marks, the relation between the goods and services involved, and how both parties use the web as a marketing channel. This court will not find trademark infringement when products differ, and confusion among targeted consumers is unlikely.[889] The United States Court of Appeal for the Second Circuit and the United States Court of Appeal for the Sixth Circuit require trademark infringement plaintiffs to allege that the infringing mark has been used in commerce. However, the courts apply different definitions. The United States Court of Appeal for the Sixth Circuit defines use in commerce as a display to consumers in connection with a commercial transaction. It uses it as a trademark symbol to attract public attention[890]. This Court does not require the plaintiff to prove the defendant used the mark to satisfy the 'use-in-commerce' requirement as long as the mark is affixed to the goods.

In contrast, the United States Court of Appeal for the Sixth Circuit requires the plaintiff to allege the use of the mark as a trademark. (Brown v. Harpo)[891] The United States Court of Appeal for the Ninth Circuit ruled that purchasing a competitor's trademark as a keyword for search is using the mark in commerce for trademark purposes. *Network Automation, Inc. v. Advanced Sys. Concepts, Inc*[892], following *Rescuecom Corp. v. Google, Inc.*,[893]. Distributing software over the Internet is use-in-commerce sufficient to establish trademark rights in this case, in the term 'Coolmail,' given the public's association between the mark and the software. (Planetary Motion Inc. v. Techsplosion, Inc)[894] A trademark licensor can be held responsible as an 'apparent manufacturer' for defective products that are negligently placed in the stream of commerce and bear the licensor's logo because consumers expect licensors to oversee production. However, the licensor's liability is limited based on its

---

[886] *Article 21.5 of TM PDDRP Has*

[887] *Dana Shilling, Lawyer's Desk Book, 2nd Edition, Publisher Wolters Kluwer, 2018 ,p10-52-53 .*

[888] *304 F.3d 936 (9th Cir. 2002).]*

[889] *Ibid, p10-53*

[890] *Dana Shilling, Lawyer's Desk Book Ibid, p10-53.*

[891] *717 F.3d 295 (2d Cir. 2013).]*

[892] *., 638 F.3d 1137 (9th Cir. 2011)*

[893] *562 F.3d 123 (2d Cir. 2009):*

[894] *261 F.3d 1188 (11th Cir. 2001).]*

actual design, manufacturing, and distribution, as seen in the case of *Kennedy v. Guess, Inc.*[895]

As for the dilution mechanism, the dissertation established that the trademark dilution act modified the Lanham Act to shield popular marks from their different high-quality dilution. The term dilution implies the minimising of the capability of a well-known mark to determine as well as differentiate services or goods. In identifying whether a mark is well-known and unique, a court may consider elements such as the level of fundamental or obtained distinctiveness besides the grade of acknowledgment of the mark. Furthermore, the period and level of the use, promotion, and also publicity of the mark will be taken into consideration to decide the level of fame of the mark, in addition to the geographical degree of the trading area in which the mark is utilised; and the networks of trade for the goods or services with which the mark is utilised[896]. Once again, the disappointing result for the BPOST trademark holder rings the alarm over the leading standard: first-come-first-served, which is crucial for legitimising the originality of the contested domain. Moreover, as the study indicated, a dilution claim of the domain name does not require proof that consumers are likely to be confused by a connection between unauthorised use and the mark[897] .

Regarding the *in rem* jurisdiction dilemma, the dissertation tried to answer whether UDRP rules and judicial instruments could solve the conflict perfectly *in rem* jurisdiction. The study concluded that the dual system needs to be improved to satisfy the main stakeholders' interests. In this regard, the study justified this outcome because UDRP rules give the parties the right to go to Court. It cannot always have the power to enforce the decision outside the local territory if one of the parties is a foreigner or if it cannot approve the property of contested domain names. As for *in rem* jurisdiction, the study assumes that the Court can practice the *in rem* jurisdiction if the domain name is considered property.

Further analysis has supported the dissertation’s hypothesis in this context. It is based on the universal nature of domain names within borderless cyberspace. More often than not, any conflict over a contested domain name will contain a foreign party; as a result, the court must have the legal authority to practice its jurisdiction over such conflict. To this point, the Court can practice jurisdiction based on personal jurisdiction if there is a minimum connection between the state court and the party or based on *in rem* jurisdiction, and this entails, as the author believes, that domain names must be classified to be intellectual property for this practice. Otherwise, if domain names are not property, the court cannot practice *in rem* jurisdiction over the contested domain name. Furthermore, jurisdiction leaves many challenges in this area; for instance, if the court can make a judgment, it has adequate power to put it into force. It is almost to the point that the other litigant could take contra-legal action at his State Court to reject the other Court's decision.

Practicing this jurisdiction can sometimes encroach upon other states' sovereignty. The author suggests developing the UDRP rules mechanism to turn it from an arbitration tool into an International Court for domain name conflicts. Additionally, to achieve success, this

---

[895] *Dana Shilling, Lawyer's Desk Book Ibid, p10-53*

[896] *Richard A. Mann, Barry S. Roberts, Smith and Roberson's Business Lawibid,p864.*

[897] *Frank B. Cross, Roger LeRoy Miller ,The Legal Environment of Business: Text and Cases, ibid,,p 173.*

court must have appellate instances and the ability to decide on award damages rather than limit its judgements over the cancellation, transferring, or suspending of the domain names. Furthermore, the author suggests that this proposed court would extend its competence to include registered domain names based on confusion, dilution, or bad faith, such as cybersquatting or reverse domain hijacking, and all other violations stemming from using the domain name. What is more, the author believes that this alternative court must not separate domain names from websites or website content when hearing the claims; for instance, the registered domain name would have nothing to do with the other trademark holder, but the website that runs under this domain name could violate the trademarks holder's right in a way or another. For instance, the domain name *Amazone.com* hosts advertisements that offer fake products related to a fashion brand. In this case, this court must be able to judge against the domain name owner even if this domain name did not have a registered brand name on his registered domain name. In terms of the crucial rule of understanding the legal nature of domain names over *in rem* jurisdiction in cyberspace, this study has concluded that in some countries it is not always the scenario where the detailed courts' jurisdiction can exclude various other countries' courts from exerting its jurisdiction over the same instance. Considering that there are no unique arrangements for international jurisdiction on any issue worrying property, all the matters regarding IP are not subject to the individual jurisdiction of any solitary Court of a different nation, even though the credibility of signed-up copyright is subject to such special jurisdiction in some international legal systems such Brussels I Recast Regulation.

Moreover, mapping the normative and political structures in Europe, the United States, and Latin America in the territory and relevant law issues, and managing emerging private disputes of legal communications in cyberspace, is not easy. Non-extant or limited regulations and complex concepts prevail in the private international law of numerous countries. In such instances, the experimenter's task is to collect together all the web content in a solo work to help with the production of lawful experts - whether lawmakers, judges, trainees, teachers, or legal representatives[898].

Brussels I Recast Regulation is likely to provide more assurance to interactions of commercial and civil nature, specifically those that originated on the net. In the virtual atmosphere, in which modifications happen increasingly faster, the activity of legislative and judicial authorities is vital. Amongst typical legislation systems, the United States distinguishes itself poorly from Europe in how it fixes problems that stem from the Internet. There is no legislation targeted at solving digital disagreements. Also, these are addressed on a case-by-case basis, and based upon criteria that typically have no connection to the Internet. The elaboration of legislation much better suited for problems in the online world should be considered essential. It would make the work of American attorneys, in particular, much easier.

[898] *Laila Damascena Antunes,Matheus Rosa,Bruno de Oliveira Biazatti,Pedro Vilela,Odélio Porto, Jurisdiction and conflicts of law in the digital ageRegulatory frameworkof internet regulation, , Institute for Research onInternet and Society, 2018, https://hu1lib.org/ireader/5214415*

REFERENCES

Literature

- *Aaron Upcroft, "Trade Marks as Domain Names: An Australian Perspective," Macarthur Law Review 3 (1999): 43-60*
- *Andrew D. Murray, "Internet Domain Names: The Trade Mark Challenge," International Journal of Law and Information Technology 6, no. 3 (1998): 285-312*
- *Angus Stevenson, Maurice W.: Concise Oxford English Dictionary: Luxury Edition Publisher OUP. , Oxford (2011)*
- *Anselmo Reyes, Wilson Lui, Direct Jurisdiction: Asian Perspectives, Publisher Bloomsbury Publishing, 1st Edition,2021*
- *Antunes, L.D., Rosa, M., Biazatti, B. de O., Vilela, P., Porto, O.: Jurisdiction and conflicts of law in the digital age Regulatory framework of internet regulation. Institute for Research on Internet and Society (2018 &2021)*
- *Arriaga, P., Esteves, F., Pavlova, M.A., Piçarra, N.G.: Coronavirus Disease (COVID-19): The Impact and Role of Mass Media During the Pandemic. Frontiers Media, SA (2021)*
- *Asensio, P. de M.: Conflict of Laws and the Internet. Edward Elgar Publishing, Cheltenham and Camberley in the UK and Northampton, Massachusetts, in the USA.*
- *Au, Y., Howard, P.N., Anita, P.: Profiting from the Pandemic Moderating COVID-19 Lockdown Protest, Scam, and Health Disinformation Websites, COMPROP Data Memo 2020.7, Nov 2020, COVID-19 Series, publisher university of Oxford, p 2. university of Oxford, UK (2020)*
- *Baatz, Y., Velasco, A.C., Debattista, C., Gürses, Ö., Hjalmarsson, J., Lista, A., Lorenzon, F., Serdy, A., Tsimplis, M.: Maritime Law fifth edition. Taylor & Francis, Oxfordshire, England, UK (2021)*
- *Babcock, B.A., Massaro, T.M., Spaulding, N.W.: Civil Procedure: Cases and Problems. Wolters Kluwer, Netherlands (2021)*
- *Bagley, C.E.: Managers and the Legal Environment: Strategies for Business. USA: Cengage Learning, UK (2019)*
- *Bakaki, Zorzeta, Lockhart, \Sarah P., Money, Jeannette, Neill, Kate O', Stoeva, Preslava & Yao, Joanne, Europa Directory of International Organizations, Routledge, (2021).*
- *Baker, Loren, Search Engine Marketing and Trademarks, search engines journal, September 25, (2004).*
- *Bangia, R., Sing, Balvir: Operating Systems and Software Diagnostics. Firewall Media, Kolkata, India (2007)*
- *banks, Theodore l., banks, Frederick z.: Corporate Legal Compliance Handbook. Wolters Kluwer, new York (2022)*
- *Barkoff, R.M., Selden, Andrew C.: Fundamentals of Franchising. American Bar Association, USA (2004& 2008)*
- *Barrett, M.: Intellectual Property. Aspen Publishers Online, New York (2008)*

- *Barros, D.B., Hemingway, A.P., Cavalieri, S.: Property Law. Wolters Kluwer Law & Business, New York (2020)*
- *Batman, J.L.: Advising the Small Business: Forms and Advice for the Legal Practitioner. American Bar Association, USA (2007& 2018)*
- *Battersby, G.: Licensing Update 2020 Edition. Wolters Kluwer, the Nethrlands (2020)*
- *Battersby, G.J., Grimes, C.W.: Trademark & Copyright Disputes: Litigation Forms and Analysis. Wolters Kluwer, New York (2021)*
- *Belmas, G., Shepard, J.M.: Major Principles of Media Law, 2023 edition. Cengage Learning, Boston, MA (2022)*
- *Benedek, W., Kettemann, M.C.: Freedom of expression and the internet. Council of Europe (2020)*
- *Bernhard, M., Bracciali, A., Camp, L.J., Matsuo, S., Maurushat, A., Rønne, P.B., Sala, M.: Financial Cryptography and Data Security. Springer Nature, Switzerland (2020)*
- *Bernhardt, R., Palomar, J.D., Randolph, Patrick A.: Property: Cases and Statutes. Carolina Academic Press, CA, USA (2005)*
- *Bernstein, D.H.: Protecting your intellectual property assets. Practicing Law Institute, USA (2022)*
- *Bidgoli, H.: The Internet Encyclopedia. John Wiley & Sons*
- *Blackett, T.: Trademarks. Palgrave Macmillan, UK (1998)*
- *BNA's Banking Report. (2000)*
- *Bosworth, S., Kabay, M. E.: Computer Security Handbook. John Wiley & Sons, Hoboken, New Jersey, U.S. (2003)*
- *Bouchoux, D.E.: A Practical Introduction to Paralegal Studies: Strategies for Success. Wolters Kluwer Law & Business, New York (2021)*
- *Bouchoux, D.E.: Intellectual Property: The Law of Trademarks, Copyrights, Patents, and Trade Secrets. Cengage Learning, Boston, MA (2012)*
- *Bowker, D.W., Stewart, D.P.: Ristau's International Judicial Assistance A Practitioner's Guide to International Civil and Commercial Litigations. , publisher oxford press, UK (2021)*
- *BPP Learning Media: Business Essentials: Company and Commercial Law. BPP Learning Media, Uk (2010)*
- *Brilmayer, R.L., Goldsmith, J.L., O'Connor, E.O., Vázquez, C.: Conflict of Laws: Cases and Materials. Wolters Kluwer Law & Business, Alphen aan den Rijn, Netherlands (Global) and Philadelphia, United States (2019)*
- *Bryer, Lanning G., Lebson, S.J., Asbell, Matthew D.: Intellectual Property Strategies for the 21st Century Corporation: A Shift in Strategic and Financial Management. John Wiley & Sons, USA (2011)*
- *Busc, Ing.C., Wendler, T., Steinicke, M.: ECEL 2020 19th European Conference on e-Learning. Academic Conferences International Limited, UK (2020)*
- *Business Essentials: Company and Commercial Law. BPP Learning Media, Uk (2010)*
- *Byer, D.J., Lee, E.W.: u.s. The Supreme Court allows booking.com to register its domain name as a trademark. (2020)*

- *Bygrave, L.A., Bing, J.: Internet Governance: Infrastructure and Institutions. OUP Oxford, Oxford, England (2020)*
- *Cabell, D., Fellow, B.: Trademark, Domain Names, and Related up Issues on the Internet. Bar Association, Massachusetts: Massachusetts (1999)*
- *Calboli, I., de Werra, J.: The Law and Practice of Trademark Transactions: A Global and Local Outlook. Edward Elgar Publishing, UK & USA (2016)*
- *Campbell, D., Woodley, Susan: E-Commerce: Law and Jurisdiction: Comparative Law Yearbook of International Business Special Issue 2002. Kluwer Law International B.V., New York (2003)*
- *Campbell, J.T., Freund, S.M., Frydenberg, Mark, Cashman, S.: Series Discovering Computers & Microsoft Office 365 & Office 2016: A Fundamental Combined Approach. Cengage Learning (2016)*
- *Carl Oppedahl, "Remedies in Domain Name Lawsuits: How is a Domain Name Like a Cow," John Marshall Journal of Computer and Information Law 15, no. 3 (Spring 1997): 437-464*
- *Carroll, M.T., ABA's, A.: Practice Checklist Manual on Advising Business Clients III: Checklists, Forms, and Advice from The Practical Lawyer. , Publisher ALI-ABA (2004)*
- *Casenotes: Property: Casenote Legal Briefs. Aspen Publishers Online (2004)*
- *Cetinkaya, S.: The importance of domain name in an eCommerce business. (2014)*
- *Chadirjian, C.: The Business of Trademarks: A Practical Guide to Trademark Management for Attorneys and Paralegals. Universal-Publishers, Irvine, California, USA (2018)*
- *Chakrabarti, A.: Grid Computing Security. Springer Science & Business Media, Berlin/Heidelberg, Germany (2007)*
- *Chandramouli, R., Rose, S.: Secure Domain Name System (DNS) Deployment Guide Recommendations of the National Institute of Standards and Technology. National Institute of Standards and Technology, USA (2006)*
- *Christie, A.: Blackstone's Statutes on Intellectual Property. Publisher Oxford University Press, UK (2021)*
- *Cinelli, M., Quattrociocchi, W., Galeazzi, A., MicheleValensise, C., Brugnoli, E., Schmidt, A.L., Zola, P., Zollo, F., Scala, A.: The COVID-19 social media infodemic, Scientific Reports. Springer Nature (2020)*
- *Cinelli, M., Quattrociocchi, W., MicheleValensise, C., Galeazzi, A., Brug, E., Schmidt, A.L., Zola, P., Zollo, F., Scala, A.: The COVID 19 social media infodemic, (2020)*
- *Clarke, R.A., Knake, R.K.: The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats. Penguin, Newyork (2019)*
- *Clarkson, K.W., Miller, R.L.: Business Law: Text and Cases. , Publisher Cengage Learning, United Kingdom & United States (2016,2020,2021)*
- *Coffy, E., Decady, A.: The Value of Your Idea$: Make Intellectual Property Work for You. Trafford Publishing, USA & CANADA (2020)*
- *Cogburn, D.L.: Transnational Advocacy Networks in the Information Society. Springer (2017)*
- *Collins, B.: Vigilante treatments: Anti-vaccine groups push people to leave ICUs. , USA (2021)*
- *Comba, MC: The Law Applicable to Cross-border Contracts involving Weaker Parties in EU Private International Law. Springer Nature, swizrland (2021)*

- *committee on Commerce, Science, and Transportation. Subcommittee on Communications,: Internet Corporation for Assigned Names and Numbers (ICANN): Hearing Before the Subcommittee on Communications of the Committee on Commerce, Science, and Transportation, United States Senate, One Hundred Eighth Congress, First Session, July 31, 2003,. US Government Printing Office, USA (2014)*
- *Committee on Energy and Commerce, House of Representatives: ICANN internet governance: is it working? Hearing before the Subcommittee on Commerce, Trade, and Consumer Protection and Subcommittee on Telecommunications and the Internet of the Committee on Energy and Commerce, House of Representatives. Publisher US GPO, USA (2006)*
- *Computer Forensics: Investigating Network Intrusions and Cyber Crime. Cengage Learning, Boston, MA, USA (2009)*
- *Congress. House Commerce, Justice, Science, and Related Agencies Appropriations for 2014: Hearings Before a Subcommittee of the Committee on Appropriations, House of Representatives, One Hundred Thirteenth Congress. US Government Printing Office, USA (2014)*
- *congress: Anti-Cybersquatting Consumer Protection act. (1999)*
- *Congressional Record, V. 145, Pt. 21, November 17, 1999, to December 3, 1999, Publisher Government Printing Office. (1999)*
- *Connerty, A.: A Manual of International Dispute Resolution. Commonwealth Secretariat, London, the United Kingdom (2006)*
- *Cooley, John W. & Lubet, Steven, Arbitration Advocacy, Ntl Inst for Trial Advocacy, (2003).*
- *Correa, C.: Trade Related Aspects of Intellectual Property Rights: A Commentary on the TRIPS Agreement. Oxford University Press, UK (2020)*
- *Council of European National Top-Level Domain Registries (CENTR): The true effect of corona on the DNS, (2020)*
- *Crawford, S.P.: Representing the e-commerce company: a satellite program. Practicing Law Institute 2000, USA (2000.-1)*
- *Cross, F., Miller, R.: The Legal Environment of Business: Text and Cases - Ethical, Regulatory, Global, and E-Commerce Issues. Cengage Learning, Mason, OH (2009)*
- *Cross, F.B., Miller, R.L.: The Legal Environment of Business: Text and Cases. Cengage Learning, UK & UAS (2020)*
- *Cunningham-Hill, S., Elder, K.: Civil Litigation 2019-2020. Oxford University Press, UK (2020)*
- *Curtin, T.J.: The Name Game: Cybersquatting and Trademark Infringement on Social Media Websites. Journal of Law and Policy . 19, 46 (2010)*
- *Daller, MF: Business Torts. Aspen Publishers (2019)*
- *das, jatindra Kumar: law of copyright. Publisher PHI Learning Pvt. Ltd., Delhi (2021)*
- *Davidson, D.V., Forsythe, Lynn M.: Business in the Contemporary Legal Environment. Wolters Kluwer Law & Business, New York (2017, 2021)*
- *Davison, M.J., Monotti, A.L., Wiseman, L.: Australian Intellectual Property Law. Cambridge University Press (2020)*
- *Dent, S.: The Language Report. Oxford University Press, UK (2003)*

- *Dinwoodie, G.B., Janis, M.D.: Research Handbook on trademark Law Reform. Edward Elgar Publishing, UK & USA (2021)*
- *Dinwoodie, Graeme B. & Janis, Mark D., Trademark Law and Theory:A Handbook of Contemporary Research, Edward Elgar Publishing, (2009).*
- *Droit, A. de: Recueil Des Cours/Collected Courses (2000). Hachette, Netherland (2000)*
- *Dukeminier, J., Krier, J.E., Alexander, G.S., Schill, M., Strahilevitz, L.J.: Property: Concise Edition. Wolters Kluwer Law & Business, New York (2017,2020)*
- *Earnshaw, G.: China Economic Review's China Business Guide. SinoMedia(Holdings)Co.Ltd., New Shanghai, China (2005)*
- *Edwards, L., Waelde, C.: Law and the Internet Regulating Cyber Space. Oxford: Hart Publishing, UK (1997)*
- *Enright, C.: Federal Administrative Law. Federation Press, Alexandria, Australia (2001)*
- *Epstein, R.A.: Cases and Materials on Torts. Aspen Publishers, Boston, Massachusetts, United States (2004)*
- *Erichson, HM: Inside Civil Procedure: What Matters and Why? Publisher Wolters Kluwer, new York (2018)*
- *Ermert, M., Hughes, C.R.: What's in a name? China and the domain name system. Routledge, London, UK (2003).*
- *European law institute: unidroit, eli-unidroit model European, rules of civil procedure From Transnational Principles to European Rules of Civil Procedure. Oxford University Press, UK,2021.*
- *Fang, B.: cyberspace Sovereignty Reflections on Building a Community of Common Future in cyberspace. Science Press and Springer Nature Pte Ltd, Singapore (2018)*
- *Fasthoff, J.: Are you the master of your Domain? Enforcing Trademark Rights Online through the ICANN Domain Name Dispute Resolution. Policy & The Anti Cybersquatting Consumer Protection Attohenry. IV, 7 (2000)*
- *Fink, C., Helmers, C.: Trademarks Squatters: Evidence from Chile. World Intellectual Property Organization (2014)*
- *Fleishman, G.: Take Control of Your domain Names. Take Control Books, California, United States (2006)*
- *Floyd, A.V.: O'Connor's Federal Intellectual Property Codes Plus. Jones McClure Pub., Charlottesville, VA, United States (2007)*
- *Freeman, R.L.: A reference manual for telecommunications engineering. Wiley, Hoboken, New Jersey (2002)*
- *Freund, Steven M., Vermaat, M.E.: Discovering Computers © 2018: Digital Technology, Data, and Devices. Cengage Learning, , USA & UK ,(2017)*
- *Fulton, J., Fulton, S.: The Essential Guide to Flash Games: Building Interactive Entertainment with ActionScript. A press, USA (2010)*
- *G. Peter Albert Jr., "Right on the Mark: Defining the Nexus between Trademarks and Internet Domain Names," John Marshall Journal of Computer and Information Law 15, no. 2 (Winter 1997): 277-322*
- *Gader-Shafran, R.: the trademark law dictionary. iUniverse (2013)*

- *Garoupa, N., Ligüer, C.G.: Legal Origins and the Efficiency Dilemma. Taylor & Francis, Oxfordshire, United Kingdom (2016)*
- *Garzaniti, LJHF, O'Regan, M.: Telecommunications, Broadcasting and the Internet: EU Competition Law and regulation. Sweet & Maxwell, UK (2010)*
- *Gilbert, I., Tropin, HS: LexisNexis Practice Guide: Florida Business Torts. LexisNexis, USA (2021)*
- *Gillers, S.: Regulation of Lawyers: Problems of Law and Ethics. Wolters Kluwer, new York (2021)*
- *Gisele, R.: Digital Underworld. Lulu.com (2005)*
- *Glick, M.A., Reymann, Lara A., Hoffman, R.: Intellectual Property Damages: Guidelines and Analysis. John Wiley & Sons, Hoboken, New Jersey, U.S. (2002)*
- *Gompel, S. van: Formalities in Copyright Law: An Analysis of Their History, Rationales, and Possible Future. Kluwer Law International BV, Netherlands (2011)*
- *Gould, M.: an Island on the Net: domain Naming and English Law. John Marshal Journal Comp & Info. 15, 493. (1997)*
- *Govindarajulu, G., Ramaswami, S.S., Vasudevan, S.K.: It's Your Digital Life. CRC Press, New York (2021)*
- *Goyal, Dinesh, Balamurugan, S., Lung Peng, Sheng- & Verma, O. P., Design and Analysis of Security Protocol for Communication, John Wiley & Sons, (2020).*
- *Gurry, F., (WIPO) World Intellectual Property Organization, Intellectual property, innovation, access and COVID-19 WIPOWorld Intellectual Property Organization, WIPO Magazine, Issue 2/2020 (June), Volume 121 of WIPO Publication,p10., (2020)*
- *Halt, G.B., Donch, J.C., Stiles, A.R., Fesnak, R.: Intellectual Property in Consumer Electronics, Software and Technology Startups. Springer Science & Business Media, USA (2014)*
- *Handelman, J.: Guide to TTAB Practice. Aspen Publishers Online, Boston, Massachusetts, United States . (2007)*
- *Hargraves, O.: New Words. Oxford University Press, UK (2004)*
- *Harms, L.T.C., A Casebook on the Enforcement of Intellectual Property Rights, WIPO, (2018).*
- *Hart, J.D.: Internet Law, a Field Guide. BNA Books/ Associated Press,USA. (2008)*
- *Hart, J.D.: Web Law: A Field Guide to Internet Publishing. Bradford Publishing Compan,Bradford, PA (2004)*
- *Hartwig, H.: Research Handbook on Design Law. Edward Elgar Publishing, UK & USA (2021)*
- *Harvey, D.J.: Collisions in the Digital Paradigm: Law and Rule Making in the Internet Age. Bloomsbury Publishing (2017)*
- *Hatcher, J.: The UDRP rules: A Guide for SMEs and Consumers on domain name s and domain name Disputes, A Report for the International Intellectual Property Institute July. International Intellectual Property Institute (2007)*
- *Hay, D.C.: Enterprise Model Patterns: Describing the World. Technics Publications, New Jersey, United States (2011)*
- *Hedley, S., Aplin, T.F.: Blackstone's Statutes [on] IT & E-commerce. Oxford University Press, UK (2004)*

- *Helmke, M.: Ubuntu Unleashed. Sams Publishing, Carmel, Indiana, USA (2014)*
- *Hess, B., Bergström, M., Storskrubb, E.: EU Civil Justice: Current Issues and Future Outlook. Hart Publishing, UK (2016)*
- *Hewitt, J.R., Carlson, James B.: Securities Practice and Electronic Technology. Law Journal Press New York (2006 2019)*
- *Hickman, E.G., Dictionary of international trade. Librix.EU, Brno (2008)*
- *Hiduke, G., Ryan, J. D.: Small Business: An Entrepreneur's Business Plan. Cengage Learning (2013)*
- *Hoboken, Joris van, Search Engine Freedom on the Implications of the Right to Freedom of Expression for the Legal Governance of Web Search Engines, Wolters Kluwer, (2012).*
- *Hoeren, T., Stauder, J.: International Sources of Electronic Commerce regulation. Lit Publishing, Berlin, Vienna, Hamburg, London, Zurich, and New York City. (2001)*
- *Hohlfeld, O., Lutu, A., Levin, D.: Passive and active Measurement: 22nd International Conference, PAM 2021, Virtual Event, March 29 - April 1, 2021. In: 22nd International Conference, Proceedings, p. 40. Springer Nature (2021)*
- *Holtzhausen, D., Fullerton, J., Lewis, B.K., Shipka, D.: Principles of Strategic Communication. Routledge, New York (2021)*
- *Hong Xue, Caveats of intermediary liability in the domain Name System: a review of the ICANN new gTLD right protection measures, Intellectual Property Perspectives on the Regulation of New Technologies Edward Elgar Publishing, UK & USA (2018)*
- *Hörnle, Julia: Internet Jurisdiction Law and Practice. Oxford University Press, UK (2021)*
- *Hovenkamp, H., Janis, M.D., Lemley, M.A., Leslie, C.R., Carrier, A., M.: IP and Antitrust: An Analysis of Antitrust Principles Applied to Intellectual Property Law. Wolters Kluwer, New York (2022)*
- *Hurtt, E.: What's in a Name? The Rights to domain Names Under Various Principles. The University of Cincinnati Law Review. 840 (2017)*
- *Husovec, Martin, Injunctions Against Intermediaries in the European Union, Cambridge University Press, (2017).*
- *IBP, Inc.: China Business Law Handbook Volume 1 Strategic Information and Basic Laws. Publisher Lulu. com (2000)*
- *ICANN,gTLD Applicant Guidebook (v. 2012-06-04) Module 3. (2012)*
- *ICANN: Rules for Uniform Domain Name Dispute Resolution Policy. WIPO (2013)*
- *Inshakova, A.O., Bogoviz, A.V.: Alternative Methods of Judging Economic Conflicts in the National Positive and Soft Law. IAP, USA, Publisher (2020)*
- *Intellectual Property Office of Singapore: relative grounds for refusal of registration. Intellectual Property Office of Singapore, Singapore (2015)*
- *International Telecommunication Union: Challenges to the Network: Internet for Development. International Telecommunication Union Publishing, Pennsylvania, USA (1999)*
- *Jeftovic, M.E.: Managing Mission - Critical Domains and DNS: Demystifying name servers, DNS, and domain names. Packt Publishing Ltd, UK (2018)*

- *Jehoram, TC, Jozef, C.J., Nispen, Clemens van, Huydecoper, Tony, Huydecoper, JLRA: European Trademark Law: Community Trademark Law and Harmonized National Trademark Law. Kluwer Law International BV, Netherland (2010)*
- *Jentz, T.M. Case Printouts; Bus Law Today. Cengage South-Western, Mason. OH, USA (2005)*
- *Johnstone, I., Ratner, S.: Talking International Law: Legal Argumentation Outside the Courtroom. Oxford University Press, UK & USA (2021)*
- *Jolly, Adam, The Handbook of European Intellectual Property Management: Developing, Managing and Protecting Your Company's Intellectual Property, 3. Aufl., Kogan Page Publishers, (2012).*
- *Jr, J.L., Perumalla, K., Siraj, A.: ICCWS 2021 16th International Conference on Cyber Warfare and Security. Presented at the (2021)*
- *Karatzogianni, A.: The Politics of Cyberconflict. Routledge, Oxford shire, England, UK (2006)*
- *Keller, B.P., Harvey, D.P.: Strategies for litigating copyright, trademark and unfair competition cases. Practicing Law Institute, New York (2001)*
- *Kelly, M.D., Kumor, and K.: Trademark: Intellectual Property Protection on The Information Super High Way. European Intellectual property Review. 482. (1995)*
- *Kettemann, M.C.: The Normative Order of the Internet: A Theory of Rule and regulation Online Volumes 1-2020 of Normative orders working paper. Oxford University Press, UK (2020)*
- *Khuran, R., Aggarwal, R.: Interdisciplinary Perspectives on Business Convergence, Computing, and Legality. IGI Global, USA (2013)*
- *Kieninger, E.-M.: Security Rights in Intellectual Property. Springer Nature, Switzerland (2020)*
- *Kjaer, PF: Law of Political Economy: Transformation in the Function of Law. Cambridge University Press, UK (2020)*
- *Kohler, G.K., Schultz, T.: Online Dispute Resolution: Challenges for Contemporary Justice. Kluwer Law International B.V., Hague ,Netherland (2004)*
- *Komaitis, K.: The Current State of Domain Name Regulation: Domain Names as Second Class Citizens in a Mark-Dominated World. Routledge, London & New York (2010)*
- *Koonjoobeeharry, D.K.: Are Domain Names Contract of Services or Property Rights? (2017)*
- *Ku, R.S.R.: Cyberspace Law: Cases and Materials. Wolters Kluwer Law & Business, the Netherlands (2016)*
- *Kutylowski, M., Vaidya, J.: Computer Security - ESORICS 2014. Presented at the 19th European Symposium on Research in Computer Security, Wroclaw, Poland, September 7-11, 2014. Proceedings (2014)*
- *Lee, Kevin & Seda, Catherine, Search Engine Advertising: Buying Your Way to the Top to Increase Sales, New Riders, (2009).*
- *Lehman, B.A.: Intellectual Property in the Global Marketplace. Economic Perspectives An electronic journal of the U.S.information Agency. 3, (1998)*
- *Levine, G.M.: Garnishing Domain Names: Are They Contracts or Property? New York law journal. 1 (2015)*

- *Levine, G.M.: Understanding the legal options used to fight cybersquatting Cybersquatters jeopardize your exclusive trademark rights, and there are multiple ways to fight back. Network World. (2015)*
- *Levine, J.R., Young, M.L., Everett-Church, Ray: Fighting Spam for Dummies. John Wiley & Sons, Hoboken, New Jersey, U.S. (2007)*
- *Lindeberg, F.: Coordinating the Internet. Linköping University Electronic Press, Sweden (2019)*
- *Lindsay, D.: International Domain Name Law: ICANN and the UDRP. Bloomsbury Publishing, London, New York, New Delhi, Oxford & Sydney (2007)*
- *Lindsay, R.: Ad Law: The Essential Guide to Advertising Law and regulation. Kogan Page, London, United Kingdom (2016)*
- *Lipton, J.D.: Internet Domain Names, Trademarks and Free Speech. Edward Elgar Publishing, Cheltenham, UK (2010)*
- *Liska, A., Stowe, G.: DNS Security: Defending the Domain Name System. Syngress / Elsevier, Cambridge, USA (2016)*
- *Liu, J.K., Huang, X.: Network and System Security: 13th International Conference, NSS 2019, Sapporo, Japan, December 15–18, 2019, Proceedings. Springer Nature, Switzerland (2019)*
- *Liu, M.X.: Jurisdictional Limits of in rem Proceedings Against domain Names. Michigan Telecommunications and Technology Law Review. 20, 467,468. (2014)*
- *Lloyd, I.: Information Technology Law. Oxford University Press, UK (2020)*
- *Luther, P., Moran, A.: Technology in America. Macmillan International Higher Education, London, UK (2018)*
- *Manz, W.H.: Anticybersquatting Consumer Protection act: a legislative history of Public Law. William S. Hein (2002)*
- *Maras, M.-H.: Computer Forensics. Jones & Bartlett Publishers, Burlington, Massachusetts, USA (2014)*
- *Marda, V.: Internet Democratization: IANA Transition Leaves Much To Be Desired. Hindustan Times. (2016)*
- *Mather, T., Kumaraswamy, S., Latif, S.: Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. O'Reilly Media, Inc., Sebastopol, California, USA (2009)*
- *Mathiason, J.: Internet Governance: The New Frontier of Global Institutions. Routledge, LONDON & NEW YORK (2009)*
- *Matsuura, J.H.: Managing Intellectual Assets in the Digital Age. Artech House, Boston & London (2003)*
- *McCarthy, J.T., Schechter, Roger E., Franklyn, David J.: McCarthy's Desk Encyclopedia of Intellectual Property. Bureau of National Affairs, the University of Michigan, Michigan, USA (2004)*
- *McGeorge School of Law: Symposium: I think I can, I think ICANN: regulating the internet or not, McGeorge School of Law, the University of the Pacific, USA (2008)*
- *McJohn, S.M.: Examples & Explanations for Intellectual Property. Wolters Kluwer Law & Business, New York (2021)*
- *McKean, Erin, Pournelle, J.: 1001 Computer Words You Need to Know. Oxford University Press, UK (2004)*

- *Merges, R.P., Menell, Peter S., Lemley, M.A.: Intellectual property in the new technological age. Aspen Publishers/Wolters Kluwer Law & Business, New York (2007)*
- *Michaels, A., Norris, Andrew: A Practical Guide to Trade Mark Law. Sweet & Maxwell, United Kingdom (2002)*
- *Miller, R., Jentz, Gaylord: Cengage Advantage Books: Business Law Today: The Essentials. Cengage Learning, New York (2007)*
- *Miller, R.: Business Law Today, The Essentials: Text and Summarized Cases. Cengage Learning USA*
- *Miller, R.L., Clarkson, K., Jentz, G., Cross, F.: West's Business Law. Cengage Learning (2006).*
- *Miller, R.L., Hollowell, W.E.: Cengage Advantage Books: Business Law: Text and Exercises. Cengage Learning, Mason, Ohio, USA (2011)*
- *Miller, R.L., Hollowell, William E.: Business Law: Text & Exercises. Cengage Learning, New York (2019)*
- *Miller, R.L., Meinzinger, M.: Paralegal Today: The Legal Team at Work. Cengage Learning, Boston, MA (2021)*
- *Miller, R.L.: Business Law Today Essentials: Text and Summarized Cases. Cengage Learning, Boston, MA & San Francisco, CA. (2021)*
- *Miller, R.L.: Business Law Today, Comprehensive: comprehensive edition text and cases. Cengage Learning., Boston, MA (2021)*
- *Miller, R.L.: Cengage Advantage Books: Fundamentals of Business Law: Summarized Cases. Cengage Learning, USA (2012)*
- *Miller, Roger LeRoy & Cross, Frank B., The Legal Environment Today, Cengage Learning, (2021).*
- *Millstein, J.S., Neuburger, J.D., Weingart, Jeffrey P.: Doing Business on the Internet: Forms and Analysis. Law Journal Press, New York ,2003, 2020*
- *Mitchell, S.: Create Your Own Website. Sams Publishing, Indianapolis, Indiana, USA (2006)*
- *Moro-Visconti, R.: Startup Valuation: From Strategic Business Planning to Digital Networking. Springer Nature, swiszirland (2021)*
- *Mueller, M.: "Why ICANN can't [failings of Internet Corporation for Assigned Names and Numbers. IEEE Spectrum. 39, 15–16 (2002)*
- *Murray, A.: Information Technology Law:: The Law and Society. Oxford University Press, USA (2016&2019)*
- *N. M. Dawson, "Trade Mark Law and the Creation and Preservation of Well-Known Brands," Northern Ireland Legal Quarterly 49, no. 4 (Winter 1998): 343-362*
- *Nadarajan, R.: Proceedings of the National Conference on Mathematical and Computational Models. Allied Publishers, Delhi, India (2001)*
- *Nathenson, ira s.: showdown at the domain name corral: property rights and personal jurisdiction over squatters, poachers, and other parasites. Pittsburgh law review. 991, (1997)*
- *National center for Preventive Law (US): Preventive Law Reporter. Butterworth Legal Publishers, Salem, New Hampshire (1999)*

- *Navarro, G.B., Aguirre, M. de L.: Quick Guide to WIPO Domain Name Dispute Resolution Services for the.MX ccTLD. WIPO Arbitration and Mediation center , Geneva (2020)*
- *Nawaf, L.F., Hewage, C., Carroll, F., Yang, X., Sherratt, S., Dey, N., Joshi, A.: Minimization of Cyber Security Threats Caused by COVID-19 Pandemic Proceedings of Sixth International Congress on Information and Communication Technology: ICICT 2021, ICICT, London (2021)*
- *Ng, J.: The domain Name Registration System: Liberalization, Consumer Protection, and Growth. Routledge, Oxfordshire, England, UK (2013)*
- *Nguyen, N.H., 2018 Essential Cyber Security Handbook in English. Publisher am H Nguyen (2018)*
- *Nguyen, X.-T.N., Maine, J.A.: Taxing the New Intellectual Property Right. The Hastings Law Journal. 56, P41 (2005)*
- *NS, S.: Law Relating to Intellectual Property. Partridge Publishing, India (2013)*
- *OECD: Corporate Governance Flexibility and Proportionality in Corporate Governance. OECD Publishing, Paris (2018)*
- *O'Hair, H.D., O'Hair, M.J.: Communicating Science in Times of Crisis: COVID-19 Pandemic Communicating Science in Times of Crisis, John Wiley & Sons, New York (2021)*
- *Olsen, K., Petals, S.: Leprechaun Gold. Publisher Lulu.com (2011)*
- *Oosterveld, W.Th., de Jong, S., Spiegeleire, S.D., Polchar, J., Veenstra, A.-F. van: The Fission of Power: Flex and Flux in an Age of Fragmentation. The Hague Centre for Strategic Studies, Netherland (2015)*
- *Orji, UJ: International Telecommunications Law and Policy. Cambridge Scholars Publishing, UK (2018)*
- *Pakroo, P.: , The Small Business Start-Up Kit: A Step-by-Step Legal Guide. Nolo, USA (2018)*
- *Palladino, N., Santaniello, M.: Legitimacy, Power, and Inequalities in the Multistakeholder Internet Governance: Analyzing IANA Transition. Springer Nature, Switzerland (2021)*
- *Patent and Trademark Office: Trademark Manual of Examining Procedure. TMEP Patent and Trademark Office, United States. (1993)*
- *Pauwelyn, J., Véron, P., Treppoz, E., Bertholet, J., Killias, P.-A., Bettinger, T., Hanotiau, B.: Sarah Theurich, La résolution des litiges de propriété intellectuelle / Resolution of Intellectual Property Disputes. Publisher Université de Genève, Genève,2010*
- *Peermohamed, S.: Protecting Brands Online: Jurisdictional Comparisons. Sweet & Maxwell, London (2012)*
- *Perritt, H.H.: Digital Communications Law. Wolters Kluwer, New York , Wolters Kluwer , New York 2nd edition, 2021*
- *Piers, M., Aschauer, Christian: Arbitration in the Digital Age: The Brave New World of Arbitration. Cambridge University Press, UK (2018)*
- *Plotkin, M.E., Street, F. L.: Solving the legal issues affecting B2B transactions. Practicing Law Institute, USA (2001)*
- *Pollicino, O.: Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constitutionalism. Bloomsbury Publishing, London, New York, New Delhi, Oxford & Sydney (2021)*
- *Poni, C.; Berveglieri, R. (1982). Three Centuries of Venetian Patents: 1474–1796 Resumé.*

- *Pouryousef, S., Dar, M.D., Ahmad, S., Gill, P., Nithyanand, R.: Extortion or Expansion? An Investigation into the Costs and Consequences of ICANN's gTLD Experiments. Springer Nature, Switzerland (2020)*
- *Pozen, D.E Pozen Constitutional Bad Faith,", Harvard Law Review: Volume 129, Number 4 – February, Quid Pro Books, 2016, PP 885-955.*
- *Practising Law Institute: Understanding Basic Trademark Law. Practicing Law Institute, New York (2000)*
- *Press, E.: 55 Surefire Internet Businesses You Can Start for Under $5000. Entrepreneur Press, Canada (2009)*
- *Prud'homme, D., Zhang, T.: China's Intellectual Property Regime for Innovation: Risks to Business and National Development. Springer, Switzerland (2019)*
- *Qin, Z.: Introduction to E-commerce. Springer Science & Business Media, Berlin/Heidelberg, Germany (2010)*
- *Radin, M.J., Rothchild, John A., Silverman, G.M.: Intellectual Property and the Internet: Cases and Materials. Foundation Press, West Conshohocken, PA, USA (2004)*
- *Radu, R.: Negotiating Internet Governance. Oxford University Press, Oxford, UK (2019)*
- *Rains, T.: Cybersecurity Threats, Malware Trends, and Strategies: Learn to mitigate exploits, malware, phishing, and other social engineering attacks, Packt Publishing Ltd, UK (2020)*
- *Rasner, G.C., Cybersecurity and Third-Party Risk: Third-Party Threat Hunting. (2021)*
- *Raysman, R.: Emerging Technologies, and the Law: Forms and Analysis. Law Journal Press (2002)*
- *Records of the Diplomatic Conference for the adoption of a Revised Trademark Law Treaty. WIPO, Geneva (2006)*
- *Reed, C.: Internet Law: Text and Materials. Butterworths, Oxford, UK (2000)*
- *Reed, S.F.: Entrepreneurship Law: Cases and Materials. Wolters Kluwer Law & Business, New York (2021)*
- *Reilly, R.F., Shweihs, R.P.: Guide to Intangible Asset Valuation. John Wiley & Sons, New York (2016)*
- *Report of the Director General to the 2020 WIPO Assemblies: Retrospective 2008-2020. WIPO Publication Publisher, Switzerland, (2020)*
- *Rettew, D.A., Uffelman, J.: Maximising Success in UDRP Complaints. World Trademark Review. 62, 73–79 (2016)*
- *Rettew, D.A., Uffelman, J.: Maximising Success in UDRP Complaints. World Trademark Review. August/September, 73–79 (2016)*
- *Reyes, A., Lui, W.: Direct Jurisdiction: Asian Perspectives. Bloomsbury Publishing (2021)*
- *Ricketson, S.: Research Handbook on the World Intellectual Property Organization: The First 50 Years and Beyond. Edward Elgar Publishing, Cheltenham and Camberley, the UK and Northampton, Massachusetts, the USA. (2020)*
- *Riis, T.: User Generated Law: Re-Constructing Intellectual Property Law in a Knowledge Society. Edward Elgar Publishing, UK (2016)*
- *Rocci, L., Rachel, B.: Digital Media Integration for Participatory Democracy. IGI Global (2017)*

- *Rockman, H.B.: Intellectual Property Law for Engineers and Scientists. John Wiley & Sons, New Jersey (2004)*
- *Rockman, H.B.: Intellectual Property Law for Engineers and Scientists. John Wiley & Sons, New Jersey. USA (2020)*
- *Rockman, H.B.: Intellectual Property Law for Engineers, Scientists, and Entrepreneurs. John Wiley & Sons (2020)*
- *Roekel, J.V., Bell, M., Ezell, B.: Cybersins and Digital Good Deeds: A Book About Technology and Ethics. CRC Press, New York, London, and Oxford (2007)*
- *Roelofse, J.P.: From Innovation to Profit. Juta and Company Ltd, Cape town , South Africa (2006)*
- *Romaniuk, S.N., Manjikian, M.: Routledge Companion to Global Cyber-Security Strategy. Routledge, New York (2021)*
- *Romaniuk, S.N., Manjikian, M.: Routledge Companion to Global Cyber-Security Strategy. Routledge, New york (2020)*
- *Rony, E., Rony, PR: The domain Name Handbook; High Stakes and Strategies in cyberspace. Group West (1998)*
- *Roper, C.: Trade Secret Theft, Industrial Espionage, and the China Threat. CRC Press (2013)*
- *Rose, F.: Blackstone's Statutes on Contract, Tort & Restitution 2021-2022. Oxford University Press, UK (2021)*
- *Rosén, J.: Individualism and collectiveness in intellectual property law. Edward Elgar Publishing, Cheltenham, UK (2012)*
- *Ross, T.P.: Intellectual Property Law: Damages and Remedies. Law Journal Press, New York (2000)*
- *Ross, Terence P., Intellectual Property Law: Damages and Remedies, Law Journal Press, 2000.*
- *Rubalcaba, L., Kox, H.: the European internal market for business service : no open borders yet. Springer, New York (2007)*
- *Rubalcaba, L., Kox, H.: the European internal market for business service : no open borders yet. In: Business Services in European Economic Growth. p. 231. Springer, New York (2007)*
- *Rustad, M.L.: Punitive Damages in cyberspace: Where in the World is the Consumer? Chapman Law Review, the University of California. 7–9, 61. (2004)*
- *S., CBG: Chand's ISC Commerce For Class XI Publisher, S. Chand Publishing (2021)*
- *Saddhono, K., Ardianto, D.T., Hidayatullah, M.F., Cahyani, V.R.: Seward fressh 2019: Proceedings of the 1st Seminar and Workshop on Research Design, for Education, Social Science, Arts, and Humanities. Presented at the Seword fressh, Surakarta, Central Java, April 27 (2019)*
- *Samaha, J.: Criminal Law. Cengage Learning, Boston, MA (2007)*
- *Samet, J., Murray, J.W.: Workouts and Bankruptcies in the Ecommerce Economy. Practising Law Institute (2001)*
- *Sandberg, B.: Networking The Complete Reference. McGraw Hill Professional (2015)*
- *Sargent, M.: Retire-And Start Your Own Business. Nolo, Berkeley, California (2008)*
- *Saydé, A.: Abuse of EU Law and regulation of the Internal Market. Bloomsbury Publishing (2014)*

- *Scandizzo, S.: Intellectual Property Rights and International R&D Competition. International Monetary Fund, CA (2001)*
- *Scandizzo, S.: Intellectual Property Rights and International R&D Competition. International Monetary Fund (2001)*
- *Scassa, T., Deturbide, M.E.: Electronic Commerce and Internet Law in Canada. CCH Canadian Limited, Toronto, ON, Canada (2004)*
- *Schwabach, A.: Internet and the Law: Technology, Society, and Compromises. ABC-CLIO, Santa Barbra California, Oxford, England (2014)*
- *Schwabach, Aaron, Internet and the Law Technology, Society, and Compromises, Santa Barbara, Calif, ABC-CLIO, 2014.*
- *Scots, MD: Scott on Multimedia Law. Wolters Kluwer Law & Business, New York 2008,2021, 2022)*
- *Seyfarth, C.: International Distribution Law. brill, Leiden (NL), Boston (US), Paderborn (GER) Singapore (SG) and Beijing (CN), (2021)*
- *Shackelford, S.J., Raymond, A.H., Richards, E.L.: Legal and Ethical Aspects of International Business. Wolters Kluwer Law & Business, New york (2021)*
- *Sharma, V.: Information Technology Law and Practice. Universal Law Publishing, Delhi, India (2011)*
- *SHE, X.Z., Shang, Zhuan li yu, she, Biao Za Zhi: China patents & trademarks. Xianggang Zhongguo zhuan li yu shang biao za zhi she, china (2007)*
- *Shilling, D.: Lawyer's Desk Book. Wolters Kluwer, New York (2022)*
- *Shimonski, R.: Cyber Reconnaissance, Surveillance and Defense. Syngress, USA (2015)*
- *Singh, H.: Cybersquatting and the Role of Indian Courts: A Review. 2, 18–23 (2018)*
- *Singh, M.P.: The Practical Handbook of Internet Computing. CRC Press, Boca Raton, Florida (2004)*
- *Singla, RK: Business Studies - Class 11 by RK Singla (2020-21). VK Global Publications, Delhi (2021)*
- *Smith, G.J.H.: Internet Law and regulation. Sweet & Maxwell, United Kingdom (2007)*
- *Smith, M., Urbas, G.: Technology Law: Australian and International Perspectives. Cambridge University Press, UK (2021)*
- *Spinello, R.: Cybernetics: Morality and Law in Cyberspace. Jones & Bartlett Publishers, USA (2010)*
- *Spinello, R.A.: A Defense of Intellectual Property Right. Edward Elgar Publishing, Cheltenham and Camberley, UK & Northampton, Massachusetts, USA (2009)*
- *Sprankling, J.G.: International Property Law. OUP Oxford, UK (2014)*
- *Sprankling, J.G.: The International Law of Property. OUP Oxford, UK (2014)*
- *Standing Committee on the Law of Trademarks, Industrial Designs and Geographical Indications Thirty-Eighth Session Geneva, October 30 to November 2, 2017:update on trademark-related aspects of the domain name system. wipo, geneva (2017)*
- *Stephen Fishman: , Trademark: Legal Care for Your Business & Product Name. Nolo, USA (2016)*
- *Stephenson, G.: Core Statutes on Contract, Tort & Restitution 2021-22. red globe press, London, UK (2021)*

- *Stevenson, A.: Oxford Dictionary of English. OUP Oxford, UK (2010)*
- *Stim, R.: Patent, Copyright & Trademark: An Intellectual Property Desk Reference. Nolo, Berkeley, California (2017,2020)*
- *Stim, R.: Trademark law. West Legal Studies Thomson Learning (2000)*
- *Stokes, S.: Art and Copyright. Bloomsbury Publishing London, New York, New Delhi, Oxford and Sydney (2012 &2021)*
- *Street, F.L., Grant, M.P.: Law of the Internet. Wolters Kluwer, New York. (2009)*
- *Suryanto, T., Wahab, S., Hamzah, Chernysheva, Y., Juhary, A., Ferry, J.: Proceedings of The International Conference on Environmental and Technology of Law, Business and Education on Post Covid 19. European Alliance for Innovation, Bandar Lampung, Indonesia (2020)*
- *Taylor, R.W.: Digital Crime and Digital Terrorism. Pearson/Prentice Hall, Hoboken, New Jersey (2006)*
- *the Committee on the Judiciary, United States Senate: Cybersquatting and consumer protection: ensuring domain name integrity: hearing before the Committee on the Judiciary, United States Senate, One Hundred Sixth Congress. US GPO, USA (2000)*
- *The Computer Law Association Bulletin, Publisher the Association, Volume 13, 1998*
- *the European Parliament, & the council of the European Union. Regulation (EU) 2019/517 of the European Parliament and the council. In: EEA relevance)., L 91/25 Official Journal of the European Union § (2019)*
- *the European parliament, the council of the European Union: regulation (EU) 2019/517 of the European Parliament and the council of march 19, 2019, on the implementation and functioning of the .eu top-level domain name and amending and repealing regulation (EC) No 733/2002 and repealing Commission Regulation (EC) No 874/2004 (Text with EEA relevance). EU (2019)*
- *The Legal Nature of Domain Names. LawTeacher.net. (2013)*
- *The University of Arkansas: The Virtual Wild, Wild West (www): Intellectual Property Issues in cyberspace—trademarks, Service Marks, Copyrights, and domain name s. at Little Rock Law Review. 22, 64 (1999)*
- *Thronson, MJ, Roth, Gabrielle S., Grossman, Jon D.: Intellectual Property, Legal Opinions. Wolters Kluwer., Alphen aan den Rijn, Netherlands (global) Philadelphia, United States (corporate) (2020)*
- *Timmerman, P.: Legislating amidst public controversy: the services directive. Academia Press, Gent (2009)*
- *Tombs, N., Tombs, E.F, Ambiguity in the authenticity of top-level Coronavirus-related domains. Harvard Kennedy School (HKS) Misinformation Review. (2020)*
- *Tucker, P.M.: What You Should Know Before Starting a Business. Author House (2010)*
- *Twomey, D.P., Jennings, M.M., Greene, S.M.: Anderson's Business Law & The Legal Environment - Comprehensive Edition. Cengage Learning, USA & Uk (2022)*
- *United Nations: Information and Communication Technology Policy and Legal Issues for Central Asia: Guide for ICT Policymakers. United Nations Publications, New York (2007)*
- *University of Minnesota: Computer Buyer's Guide and Handbook. Computer Information Pub., Minnesota, USA (20011)*

- *Waelde, C.: Is the Dam about to Burst? An Analysis of Domain Name Disputes in the UK. Journal of Information Law & Technology. 3. (1997)*
- *Walden, I., Hörnle, Julia: E-commerce Law and Practice in Europe. Woodhead Publishing, England (2001)*
- *Walker, L.A.: ICANN's uniform domain name dispute resolution policy. Berkeley Technology Law Journal. 15, 310 Publisher University of California Press (2000)*
- *Wallace, M., Webber, L.: IT Governance: Policies and Procedures. Wolters Kluwer, New York. (2021)*
- *Waller, V., Waller, Glen: Internet Companion: The Easy Australian Guide. UNSW Press, Randwick, Australia (2000)*
- *Warf, B.: The Sage Encyclopedia of the Internet. SAGE (2018)*
- *Warren, E., Westbrook, J.L., Porter, K., Pottow, J.A.E.: The Law of Debtors and Creditors: Text, Cases, and Problems. Aspen Publishers, Boston, Massachusetts, United States. (2021)*
- *Wass, E.S.: Addressing the World: National Identity and Internet Country Code Domains. Rowman & Littlefield, Lanham, MD (2003)*
- *Wegenek, R., O'Neill, Ged, Moore, J.: E-commerce: a guide to the law of electronic business. Butterworth, Oxford, UK (2002)*
- *Wegner, H.C., Poplawski, E.G., Understanding the new patent law: how the changes affect your patent practice and portfolio. Practising Law Institute (2000)*
- *Weil, R.L., Frank, Peter B., Wagner, M.J.: Litigation Services Handbook: The Role of the Financial Expert. John Wiley & Sons, Hoboken, New Jersey, U.S. (2002))*
- *Weise, R.H.: Representing the Corporation: Strategies for Legal Counsel. Aspen Publishers Online. 151 (1996)*
- *Weltman, B., Lasser's, JK: Small Business Taxes 2021: Your Complete Guide to a Better Bottom Line. John Wiley & Sons, USA (2021)*
- *Wherry, T.L.: The Librarian's Guide to Intellectual Property in the Digital Age Copyrights, Patents, and Trademarks. American Library Association, Chicago and London (2002)*
- *Wild, C., Weinstein, S., MacEwan, N., Geach, N.: Electronic And Mobile Commerce Law An Analysis Of Trade Finance Media And Cybercrime In The Digital Age. Univ of Press, Hertfordshire, UK (2011))*
- *Wilson, L.S.: WordPress For Dummies. John Wiley & Sons, USA (2021)*
- *Winn, J.K., Wright, B.: The Law of Electronic Commerce. Wolters Kluwer, Alphen aan den Rijn, Netherlands & Philadelphia, United States (corporate) (2019)*
- *WIPO: Guide to WIPO's services for country code top-level domain registries Item. World Intellectual Property Organization, Geneva, Switzerland (2019)*
- *WIPO: Records of the Diplomatic Conference for the Adoption of a Revised Trademark Law Treaty. In: Diplomatic Conference for the Adoption of a Revised Trademark Law Treaty. p. 422. WIPO, Geneva (2010)*
- *Witte, E., Craeybeckx, Jan, Meynen, A.: Political History of Belgium: From 1830 Onwards. ASP /Academic and Scientific Publishers NV, Brussels (2009)*

- *Wolfe, JC, Chasser, AH: Domain Names Rewired: Strategies for Brand Protection in the Next Generation of the Internet. John Wiley & Sons, Hoboken, NJ, USA (2013)*
- *World Intellectual Property Organization. International Bureau: Protection Against Unfair Competition: Analysis of the Present World Situation. WIPO, Geneva, Switzerland (1994)*
- *World Intellectual Property Organization: Guide to WIPO Arbitration. WIPO (2020)*
- *Xue, H.: Caveats of intermediary liability in the Domain Name System: a review of the ICANN new gTLD right protection measures. Edward Elgar Publishing, UK & USA (2018)*
- *Yocom, N., Turner, J., Davis, Keir: The Definitive Guide to Linux Network Programming. Apress (2004)*
- *Yu, P.K.: Intellectual Property and Information Wealth: Issues and Practices in the Digital Age. Greenwood Publishing Group (2007)*
- *Zadroznys, B.: Who owns coronavirus.com? Behind the lucrative profiteering on website domains*
- *Zaichkowsky, J.L. The Psychology Behind Trademark Infringement and Counterfeiting. Psychology Press, Routledge, London & New York (2020)*
- *Zeid, I.: Mastering the Internet and HTML. Prentice Hall, Hoboken, New Jersey, U.S. (2000)*
- *Zemer, L.: The Idea of Authorship in Copyright. Ashgate Publishing, Ltd, Farnham,Surrey, United Kingdom (2007).*
- *Zheng, J.: Online Resolution of E-commerce Disputes: Perspectives from the European Union, the UK, and China. Springer Nature, Switzerland (2020)*
- *Zinzius, B.: Doing Business in the New China: A Handbook and Guide. Greenwood Publishing Group, USA (2004)*
- *Zumbansen, P.: The Many Lives of Transnational Law: Critical Engagements with Jessup's Bold Proposal. Cambridge University Press, UK (2020)*

Legislations

- *Act XI of 1997 on the protection of trademarks and geographical indications*
- *ADR Rules*
- *American dilution Act of 1995*
- *Brussels I 44/2001*
- *Brussels I Recast regulation 1215/2012*
- *China Business Law*
- *EEA Agreement*
- *Electronic Access SPAIN, ES080EN Marks, Law (Consolidation), 07/12/2001 (07/07/2003)*
- *ETA agreement*
- *Eu Council Directive 93/13/EEC 1993 on unreasonable terms in customer agreements*
- *EU Directive No. 89/104/EEC (The Trade Marks Directive)*
- *French Act No. 96-1106 of December 18, 1996, Art.*
- *Hungarian trademark law.*
- *intellectual-property CODE, Act No. 96-1106 of December 18, 1996, Art. 12 Official Journal of December 19, 1996)*
- *Jordanian Trademarks Law No. 33 of 1952, and Trademark Law No. 34 of 1999, article 2.*
- *Lanham act An amendment (15 USC § 1125(d) and The Trade Marks Act 1994*

- *Law No. 17/2001 of December 7, 2001, on Trademarks (Consolidated text including the Amendments made by Law No. 20/2003 of July 7, 2003, on Legal Protection of Industrial Designs)*
- *Post-Delegation Dispute Resolution Procedure (PDDRP*
- *Public Interest Commitments Dispute Resolution Procedure(PICDRP),*
- *Regulation (EC) No 874/2004.*
- *Rome 1 regulations no 593 for 2008 and Rome 2 Regulations no 864 for 2007.*
- *the Agreement Establishing the World Trade Organization GATT*
- *The Agreement on Trade-Related Aspects of Intellectual Property Rights TRIPS, (1995)*
- *The Anti-Cybersquatting Consumer Protection Act (ACPA) 1999*
- *the civil procedure of American Federal Rule*
- *the domain name and amending and repealing Regulation (EC) No 733/2002 and repealing Commission Regulation (EC) No 874/2004 (Text with EEA relevance). EU (2019).*
- *The European Directive on Electronic Commerce" (2000/31/ EC)*
- *The Indian Trade Mark Act,1999*
- *the registration restriction dispute resolution procedure Effective (RRDRP), February 1, 2020.*
- *trademark Clearinghouse (TCHM) regulations*
- *Trademark Law of the People's Republic of China (Adopted at the 24th Meeting of the Standing Committee of the Fifth National People's Congress on August 23, 1982, and promulgated by Order No.10 of the Standing Committee of the National People's Congress on August 23, 1982*
- *Trademarks and Other Signs (Trade Mark Act, as amended up to Act of July 16, 1998)*
- *Treaty on the Functioning of the European Union (TFEU), European Union. Volume 55 Official. Journal of the European Union. 70.*
- *U.S. Code › Title 15 › Chapter 22 › Subchapter III › § 112*
- *UDRP rules*
- *Uniform Information Transaction Act" (UCITA).*
- *Uniform rapid suspension system rules (URS)., 2013,*
- *the European parliament, & the council of the European Union. Regulation (EU) 2019/517 of the European Parliament and the council. In: EEA relevance)., L 91/25 Official Journal of the European Union § (2019)*
-

Conferences, reports, and other references

- *National Center for Preventive Law (US): Preventive Law Reporter. Butterworth Legal Publishers, Denver city (1999)*
- *The United States Congress House: Committee on the Judiciary, trademark Cyberpiracy Prevention Act: report(to accompany HR 3028). US GPO, ., USA (1999).*
- *The United States Congress. HouseAbate, F.R.: The Oxford Desk Dictionary of People and Places. Oxford University Press, UK (1999)*
- *United Nations Conference on Trade and Development, E-Commerce and Development Report. United Nations, New York and Geneva (2002)*
- *World Intellectual Property Organization: Report of the Director General to the 2019 WIPO Assemblies. WIPO (2019)*
- *Jaishankar, K., Ronel, N.: First International Conference of the South Asian Society of Criminology and Victimology (SASCV). Presented at the 15-17 January 2011, Jaipur, Rajasthan, India: SASCV 2011 Conference Proceedings, June 13 (2022)*

Online references

- *Adgully Bureau, PolicyBazaar Reprimanded By Delhi High Court In A Case Against Acko, unter: https://www.adgully.com/policybazaar-reprimanded-by-delhi-high-court-in-a-case-against-acko-*

86188.html, < https://www.adgully.com/policybazaar-reprimanded-by-delhi-high-court-in-a-case-against-acko-86188.html >, (28.3.2023).

- *Allemann, A.: Cybersquatting Cases At WIPO Trending Up In 2019 - Domain Name Wire | Domain Name News, https://domainnamewire.com/2019/10/24/cybersquatting-cases-at-wipo-trending-up-in-2019/ .*
- *Bennett, D.: Covid-19 and Counterfeiting: How the Pandemic is Reshaping Brand Protection – Part 2 What to Expect in the Short, Medium, and Long Term, https://corsearch.com/knowledge-base/news/covid-19-and-counterfeiting-how-the-pandemic-is-reshaping-brand-protection-part-2/ 09.04.2020, https://corsearch.com/knowledge-base/news/covid-19-and-counterfeiting-how-the-pandemic-is-reshaping-brand-protection-part-2/09.04.2020*
- *Byer, D.J., Lee, E.W.: u.s. Supreme Court allows booking.com to register its domain name as a trademark https://www.klgates.com/us-supreme-Court -allows-bookingcom-to-register-its-domain-name-as-a-trademark-07-07-2020.*
- *Cetinkaya, S.: The importance of domain name in eCommerce business, http://www.shopio.com/blog/the-importance-of-domain-name-in-ecommerce-business/.*
- *Chadha & Chadha Intellectual Property Law Firm, Search Engine Optimization And Trademarks, unter: Lexology, < https://www.lexology.com/library/detail.aspx?g=8c09f235-df7c-4187-8d02-07346f286ca4. >, (28.3.2023).*
- *Chew, J.: update & consultation on New gTLD Subsequent Procedures Consensus Building on Recommendations objections (v13), https://community.icann.org/download/attachments/111390697/13.SubProObjectionsasat25.08.2020forCPWG*
- *Council of European National Top-Level Domain Registries (CENTR): Measures taken by registries to help tackle COVID-19 related online abuse 2020-05-04, https://www.centr.org/statistics-centr/centrstats.html*
- *Đekić, M., Mester, G.: COVID-19 as a scam challenge. Tehnika. 76, 115–120 (2021). https://doi.org/10.5937/tehnika2101115D*
- *fasthosts: introduction to domain-names and DNs, https://help.fasthosts.co.uk/euf/assets/pdf-guides/Masterclass/domain-names.pdf*
- *Frequently Asked Questions. https://www.wipo.int/amc/en/domains/lro/faq/#3a.*
  Fridman, N.P.: A Remedy Against cybersquatting, http://www.asiaiplaw.com/article/39/3167/.
- *Galizia, N.: Trade mark litigation in Italy: overview, at:https://uk.practicallaw.thomsonreuters.com/w-010-0167?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1*
- *glover, Claudia: Coronavirus-Related Domain Registrations Rise 6,000 in a Week, Coronavirus Related Domain Registrations Rise 6,000 in a Week, (techmonitor.ai).*
- *GrahamHow, M.: a stay-at-home year accelerated three trends in the advertising industry*
- *Granneman, S.: Why You Should Never Use Network Solutions, https://www.granneman.com/webdev/domains/neveruseverisignnetworksol.*
- *harvard.edu: domain Names and Trademarks, https://cyber.harvard.edu/property00/domain/main.html#discussion, (2000)*
- *Hauser, C.: Supreme Court Ruling Protects Registered Domain Names, Preserving an Import Tool in the Fight Against Cybercrime, https://www.wiley.law/alert-Supreme Court Ruling Protects Registered Domain Names Preserving an Import Tool in the Fight_Against_Cybercrime#:~:text=On%20June%2030%2C%202020%20the,for%20combatting%20Internet%2Dbased%20fraud.&text=Such%20protection%20is%20critical%20to%20preventing%20domain%20name%20abuse.*
- *Hurewitz, B.J.: New Law Targets Cybersquatting, https://www.wilmerhale.com/en/insights/publications/new-law-targets-cybersquatting-december-7-1999*
- *Hutchers on law: What's in a Name: Reverse Domain Name Hijacking and Cybersquatting, https://hutchersonlaw.com/reverse-domain-name-hijacking-cybersquatting/.*

- *ICANN organization: Beginners guides to domain name, https://www.icann.org/en/system/files/files/domain-names-beginners-guide-06dec10-en.pdf..*
- *Italian Court solves a cybersquatting case over Altavista search engine, http://www.searchenginelaw.net/domain-names/100-italian-Court -solves-a-cybersquatting-case-over-altavista-search-engine*
- *Koonjoobeeharry, D.K.: Are Domain Names Contract of Services or Property Rights? ,http://www.circleid.com/posts/20170202_are_domain_names_contract_of_services_or_property_rights/*
- *Kurtzman, T.: The Continued Hijacking And Ransoming Of The Domain Name System By Modern-Day Corporate Privateers, https://www.americanbar.org/groups/business_law/publications/blt/2016/06/cyber_center_kurtzman/*
- *LawTeacher: The Legal Nature of Domain Names [Internet], https://www.lawteacher.net/free-law-essays/copyright-law/the-legal-nature-of-domain-names.php?vref=1.*
- *Levine, G.M.: Understanding the legal options used to fight cybersquatting Cybersquatters jeopardize your exclusive trademark rights, and there are multiple ways to fight back, https://www.networkworld.com/article/2868398/understanding-the-legal-options-used-to-fight-cybersquatting.html*
- *Marda, V.: Internet Democratization: IANA Transition Leaves Much To Be Desired, https://www.hindustantimes.com/analysis/internet-democratisation-iana-transition-leaves-much-to-be-desired/story-t94hojZjDXqS4LjNSepZlN.html.*
- *Measures taken by registries to help tackle COVID-19 related online abuse 2020-05-04. https://www.centr.org/statistics-centr/centrstats.html. (2020).*
- *MELENDEZ, S.: Microsoft is seizing control of domain names associated with COVID-19 phishing scams https://www.fastcompany.com/90525306/microsoft-is-seizing-control-of-domain-names-associated-with-covid-19-phishing-scams, https://www.fastcompany.com/90525306/microsoft-is-seizing-control-of-domain-names-associated-with-covid-19-phishing-scams*
- *MELKA, C.: COVID-19 domains: what's going on? https://clarivate.com/markmonitor/blog/covid-19-domains-whats-going-on/*
- *Mukherjee, R.: Domain of cheats: Cybersquatters using Covid to spread infodemic, https://timesofindia.indiatimes.com/india/domain-of-cheats-cybersquatters-using-covid-to-spread-infodemic/articleshowprint/81264726.cms1/5Domainofcheats:CybersquattersusingCovidtospreadinfodemic, (21-3-4)*
- *Riley, T.: The Cybersecurity 202: Internet domain names are ripe for scam during coronavirus crisis, https://www.washingtonpost.com/politics/2020/09/08/cybersecurity-202-internet-domain-names-are-ripe-scam-during-coronavirus-crisis/, (2020)*
- *Safenames organization: Cybersquatting and Opportunism: The Heightened Threat During Coronavirus - Part 1, https://www.safenames.net/about-safenames*
- *Seufer, L.: The Next Round Of gTLDs Is Around The Corner ebrand. 2019, https://ebrandservices.com/the-next-round-of-gtlds-is-around-the-corner/.*
- *Stewart, G.S., Weiler, M.S.: Emerging Issues In Statutory Damages, https://www.jonesday.com/en/insights/2011/07/emerging-issues-in-statutory-damages*
- *Todorova, Y., Arabistanov, M.: Can any word be my domain name? How about "COVID-19"?, www.kambourov.biz, (2020)*
- *U.S. Immigration and Customs Enforcement: HSI investigation results in seizure of 3 domain names purporting to be biotechnology company websites with COVID-19 treatments: At least one fraudulent website claimed to sell counterfeit vaccinations updated, https://www.ice.gov/news/releases/hsi-investigation-results-seizure-3-domain-names-purporting-be-biotechnology-company#. April 7, 2021., https://www.ice.gov/news/releases/hsi-investigation-results-seizure-3-domain-names-purporting-be-biotechnology-company#.*

- *Visscher, F. de, Dumont, C.: the importance of prior rights in domain name disputes, https://simontbraun.eu/wp-content/uploads/2021/02/News-domain-names-Importance-of-prior-rights-bpost-February-2021.pdf .*
- *Walfisz, J.: Verizon recovers infringing covid-19 domain names; Michael Jordan ends long-running dispute; Syria fee changes, verizon-recovers-infringing-covid-19-domain-names-michael-Jordan-ends-long, (2021)*
- *ward, K.: Ask the Expert: Social media's impact on vaccine hesitancy, ask-the-expert-social-medias-impact-on-vaccine-hesitancy*
- *WIPO (homepage): https://www.wipo.int/portal/en/index.html*
- *WIPO: Covid-19 Update on WIPO's UDRP and ccTLD Case Operations, https://www.wipo.int/amc/en/center/wipocenterupdate.html*
- *WIPO: Schedule of Fees under the UDRP (valid as of December 1, 2002), https://www.wipo.int/amc/en/domains/fees/*
- *WIPO: standing Committee on the law of trademarks, industrial designs and geographical indications, wipo/strad/inf/1rev.1,summaryofrepliestothequestionnaireontrademarklawandpractice(sct/11/6)*
- *WIPO: WIPO Guide To The Uniform Domain Name Dispute Resolution Policy (UDRP), https://www.wipo.int/amc/en/domains/guide/#i*
- *WIPO: WIPO's Anti-"Cybersquatting" Service Surpasses 50,000 Cases amid COVID-19 Surge, https://www.wipo.int/pressroom/en/articles/2020/article_0026.html*
- *World Intellectual Organization: Frequently Asked Questions, https://www.wipo.int/amc/en/domains/lro/faq/#3a.*
- *World intellectual property organization: All gTLDs (Ranking): 2019, https://www.wipo.int/amc/en/domains/statistics/gtlds_yr.jsp?year=2019*

Cases

- *8vs 1 ballot*
- *ADNDRC VS Taiwanese owner*
- *Al Jazeera Vs. John Williams's situation*
- *Audi AG and Volkswagen of America Inc. v. Bob D'Amato 469 F.3d 534, No. 05-2359 (6th Cir., November 27, 2006)*
- *belogic vs. Deniss Willard zewillis*
- *Booking.com vs. US Patent & trademark*
- *bpost vs. bpost.com*
- *Compaq vs. A.B.X*
- *Corp. v. a2z. Mobile Office Solutions, Inc., 326 F.3d 687 (6th Cir*
- *CRS. Recovery, Inc. v. Laxton 600 F.3d 1138 (9th Cir. 2010)*
- *Davies vs. Afilias Ltd*
- *Delta airlines" vs. "delta faucets*
- *digit limited liability company v. Privacy Administrator*
- *Dorer v Arel, 60 F. Supp. 2d. 558 (E.D. Va.1999)*
- *eBay. On December 7, 2016, the French Court*
- *Globalsantafe v. Globalsantafe.com*
- *Harrods BA vs. Harrods UK*
- *Harrods limited vs. United Kingdom network services*
- *Hasbro, Inc. v InternetEntertainment Group Ltd*
- *IKEA v Cinet*
- *Interactive Prods. Corp. v. a2z Mobile Office Solutions, Inc., 326 F.3d 687 (6th Cir.*
- *Intermatic, Inc v. Toeppen*
- *Interstellar Starship Servs. Ltd. v. Epix, Inc . 304 F.3d 936 (9th Cir. 2002*
- *Kremen v. Cohen, 337 F.3d 1024 (9th Cir. 2003),*
-

- *Limited v. Mat Feakins.*
- *Mattel, Inc. v. 3894207 Canada Inc.",*
- *Mishkoff vs. Tubman*
- *Network Solutions Inc. v. Umbro International Inc, 529 S.F. 2d 80 (Va. 2000)*
- *Panavision International v. Toeppen*
- *Patel v Allos Therapeutics*
- *Pitman training ltd and PTC Oxford HD against Nominet UK inc.*
- *Spirit Vs. MCI*
- *Tai-Kang-Tzu No 256 of 2019*
- *Tucows.Com Co. versus Lojas Renner S.A., 2011, ONCA 548*
- *Telecommunication vs. One in a million limited*
- *Umbro International v 3263581 Canada, 48 Va. Cir. 139 (1999US PTO v. Booking.com*
- *USPTO v. Booking.com B. V, 140 S. Ct. 2298 (2020); David Byer & Eric W. Lee, U.S*

Verein.n Verein .fiir Konsum