Doctoral Thesis Abstract

DOMAIN NAME VS. TRADEMARK AND PROBLEMATIC ISSUES IN CYBERSPACE

Supervisor A.P. Bartha Ildikó

Candidate: Fahed Wahdani

MARTON GÉZA DOCTORAL SCHOOL OF LEGAL STUDIES

DEBRECEN UNIVERSITY
2023

1. Aim and scope of the dissertation

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Meanwhile, the internet, as a means of storing, transferring, and disseminating information, has largely superceded traditional means, which have failed to keep pace.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.

2. 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; 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

[1] Poni, C.; Berveglieri, R. (1982). Three Centuries of Venetian Patents: 1474–1796 Resumé.
[2] https://www.wipo.int/portal/en/index.html

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.

3. 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.

4. The structure of the thesis

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.

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.

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.[3] 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.[4] 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 implement intellectual property policies on an international scale.[5] 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.[6] Besides providing specialized operations of vital Domain Name System (DNS) sources, ICANN specifies procedures for exactly how the "numbers and names" of the

[3] 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.

[4] ibid

[5] Aaron Upcroft, Trade marks as domain names: an australian perspective, 3 mac lr,p54.

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

internet need to run, and provides areas for Internet policy concerns[7]. DNS is the system of global navigation within the Internet.[8]

5.3 UDRP rules

Uniform dispute resolution policy (UDRP)[9] 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[10].

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.[11] 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 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

[7] ibid
[8] 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.
[9] ibid
[10] ICANN,Domain Name Dispute Resolution Policies, https://www.icann.org/resources/pages/dndr-2012-02-25-en
[11] https://www.wipo.int/amc/en/domains/guide/#a

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.[12] 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) 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

[12]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

(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.

6. Findings and 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[13]. 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 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

[13] 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.

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[14]. Passing off does fit losses based on the harm resulting from the trademark holder's representation of commodities or services[15]. 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[16]. 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 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

[14] 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.
[15] ibid, p34.
[16] ibid, p34.

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[17].

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[18].

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 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

[17] ibid, p3.

[18] 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/.

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[19]. 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.[20]

Moreover, in a very exceptional situation, the suggested remedy supported the termination of the registry contract if he acted in bad faith[21]. 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"[22.]

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."[23] 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.[24] In this respect, there are differences in the examined

[19] article 18.3.1 Trademark PDDRP.
[20] ibid.
[21] ibid.
[22]Ibiud, Article 22.2.
[23] Article 21.5 of TM PDDRP Has
[24]Dana Shilling, Lawyer's Desk Book, 2nd Edition, Publisher Wolters Kluwer, 2018 ,p10-52-53 .

judicial practice. In the case Interstellar Starship Servs.Ltd. v. Epix, Inc[25], 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.[26] 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[27]. 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)[28] 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*[29], following *Rescuecom Corp. v. Google, Inc.*,[30]. 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)[31] 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 actual design, manufacturing, and distribution, as seen in the case of *Kennedy v. Guess, Inc.*[32]

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[33]. 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[34].

[25] 304 F.3d 936 (9th Cir. 2002).]
[26] Ibid, p10-53
[27] Dana Shilling, Lawyer's Desk Book Ibid, p10-53.
[28] 717 F.3d 295 (2d Cir. 2013).]
[29] ., 638 F.3d 1137 (9th Cir. 2011)
[30] 562 F.3d 123 (2d Cir. 2009):
[31] 261 F.3d 1188 (11th Cir. 2001).]
[32] Dana Shilling, Lawyer's Desk Book Ibid, p10-53
[33] Richard A. Mann, Barry S. Roberts, Smith and Roberson's Business Lawibid,p864.
[34] Frank B. Cross, Roger LeRoy Miller ,The Legal Environment of Business: Text and Cases, ibid,,p 173.

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 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[35].

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.

[35] 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

UNIVERSITY AND NATIONAL LIBRARY
UNIVERSITY OF DEBRECEN
H-4002 Egyetem tér 1, Debrecen
Phone: +3652/410-443, email: publikaciok@lib.unideb.hu

Registry number: DEENK/249/2023.PL
Subject: PhD Publication List

Candidate: Fahed A. Fahed Wahdani
Doctoral School: Géza Marton Doctoral School of Legal Studies
MTMT ID: 10068780

List of publications related to the dissertation

Articles, studies (6)

1. **Wahdani, F.**, Alfaouri, M., Mashaqbeh, A.: Case Study: The Impact Of Brexit On Domain Names Right.
   Curentul Juridic. 25 (3), 13-27, 2022. ISSN: 1224-9173.

   Level of HAS Committee on Legal and Political Sciences: D

2. **Wahdani, F.**: ICANN mechanisms: Extra remedies evaluation.
   Zbornik radova Pravnog fakulteta, Novi Sad. 56 (1), 317-336, 2022. ISSN: 0550-2179.
   DOI: http://dx.doi.org/10.5937/zrpfns56-33016

3. **Wahdani, F.**: The legal character of domain names' cybersquatting.
   Law, Society & Organisations. 6 (10), 23-41, 2021. EISSN: 2537-477X.

4. Alfaouri, M., **Wahdani, F.**: The Theoretical Grounds For The Provision Of Trademark'S Protection.
   SEA: Practical Application of Science. 8 (22), 75-83, 2020. EISSN: 2360-2554.

5. **Wahdani, F.**: Reverse domain names hijacking.
   Journal of Advance Research in Social science and Humanties. 5 (4), 1-10, 2019. ISSN: 2208-2387.

DEBRECENI EGYETEM * Egyetemi és Nemzeti Könyvtár *

UNIVERSITY of DEBRECEN

UNIVERSITY AND NATIONAL LIBRARY
UNIVERSITY OF DEBRECEN
H-4002 Egyetem tér 1, Debrecen
Phone: +3652/410-443, email: publikaciok@lib.unideb.hu

6. **Wahdani, F.**: Does intellectual property support clean energy?
Public Goods & Governance. 3 (2), 16-24, 2018. EISSN: 2498-6453.
DOI: http://dx.doi.org/10.21868/PGnG.2018.2.3.

Level of HAS Committee on Legal and Political Sciences: C

By the directives of HAS Committee on Legal and Political Sciences:

Publications in periodicals level „C": 1, related to the dissertation: 1.

Publications in periodicals level „D": 1, related to the dissertation: 1.

The Candidate's publication data submitted to the iDEa Tudóstér have been validated by DEENK on the basis of the Journal Citation Report (Impact Factor) database.

14 June, 2023

DEBRECENI EGYETEM * Egyetemi és Nemzeti Könyvtár *