MYKOLAS ROMERIS UNIVERSITY

FACULTY OF LAW

PRIVATE LAW INSTITUTE

IVANNA HORAICHUK

European and International Business Law

PROBLEMATIC ASPECTS OF LEGAL REGULATION OF DOMAIN NAME DISPUTES

Master thesis

Supervisor:

Doc. dr. Goda Ambrasaitė-Balynienė

Vilnius

2022

TABLE OF CONTENTS

ABBREVIATIONS

IANA - Internet Assigned Numbers Authority

ICANN - the Internet Corporation for Assigned Names and Numbers

IETF - the Internet Engineering Task Force

EUIPO - the European Union Intellectual Property Office

IPR - Intellectual Property Rights

DND - Domain Name Disputes

DNS - Domain Name System

DOC - the United States Department of Commerce

SLD – Second-Level Domain

TLD – Top-Level Domain

RDNH - Reverse domain name hijacking

gTLD – generic Top Level Domain

ccTLD – country code Top Level Domain

UDRP - Uniform Domain Name Dispute Resolution Policy

US, USA - the United States of America

EU - European Union

WIPO - World Organisation for Intellectual Property

INTRODUCTION

> A domain name is your address, your address on the Internet. We all have a physical address; we're all going to need an address in cyberspace. They're becoming increasingly important. I believe we'll get to the point where when you're born, you'll be issued a domain name.
>
> *Bob Parsons*

Nowadays, most of us can not imagine our life without the Internet. On January 01, 2023, the world will celebrate the 40th official anniversary of the Internet. Before this, the various computer networks did not have a standard way to communicate with each other. Connecting billions of people worldwide, now the Internet has become a core pillar of the modern information society, the most popular communication and entertainment tool. The growth and impact of the Internet influence a lot of economic, political, and business processes. The International Telecommunication Union (ITU) estimated that approximately 5.3 billion people – or 66 percent of the world's population – are using the Internet in 2022. This represents an increase of 24 percent since 2019, with 1.1 billion people estimated to have come online during that period.[1]

Despite the positive aspects, during less than half of a century of Internet evolution, its governance became a tricky task for the international community. While the usage of the World Wide Web is highly increasing each year, new legal challenges arise in the field of Internet users' protection.

The recent COVID pandemic accelerated the transition of all spheres of life to the Internet. Lockdown forced the people and businesses to find an alternative way of communicating and conducting activities in order to survive. One of the best possible ways become to cease or act online. Accordingly, over a short period of time, there has been a significant increase in the number of Internet disputes. One of the most challenging though became domain name disputes.

Problem of research.

Nowadays, in order to provide free and safe activities on the Internet legal regulation needs to keep up with the rapid pace of its development. The protection of intellectual property rights in relation to Internet domain names has become one of the most important and complicated issues. As domain name regulation falls primarily outside the purview of state

[1] International Telecommunication Union Statistics, "Individuals using the Internet," 29 July 2022, accessed 05 September 2022, https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

policy, problematic aspects of domain name dispute resolution policy have sparked extensive debate in a number of countries and international organisations.

Together with the dynamic development of e-commerce and the rapid transition of business activities online, domain names have rightly taken an important place among the intangible assets of many companies. As more businesses move to post information and represent their products on the Internet, the clashes and "grey zones" in Internet domain name regulation become more common over the years, giving rise to many conflicts, while the practice of solving them is currently not unified.

We need to consider that the legal policy of domain names has its specifics. Such regulation is quite limited due to certain objective factors, in particular, the supranational nature of the Internet, and technical characteristics of the Internet (data exchange speed, changes in the content of websites, etc., which can create problems with the evidence base) as well as the peculiarity of the administration of the domain name system, which has historically developed.[2]

Nowadays, in most countries, domain name disputes are covered under trademark law. The friction between trademark law and domain names is an inevitable outgrowth of Internet growth. In the absence of better legal alternatives, trademark owners initially attempted to combat abusive attacks by asserting trademark rights in the domain name. Traditional trademark law, however, did not foresee trademark disputes occurring in a global, electronic medium. Specifically, domain names' uniqueness and global scope complicate the application of traditional trademark concepts.

These clashes are challenging the existing law and the Internet community to develop new procedures and legal rules that adequately address the equities involved.[3]

Accordingly, the question arises: "*Whether the existing dispute resolution proceedings are able to effectively deal with all the challenges arising in domain name disputes*"?

Relevance of the final thesis.

Unlike the trademark field, where rights, obligations, and liability related to the registered trademark are covered by certain regulations in many states, domain name disputes regulation is full of inconsistencies, unclarity, and confusion. That is why effective coordination within the

---

[2] Тетяна Кудрицька, "Доменні спори в Україні: останні тенденції та перспективи застосування альтернативних способів вирішення," *Журнал "Інтелектуальна власність України"* №10, (21.11.2012), https://vkp.ua/publication/domain_disputes_in_ukraine_latest_trends_and_perspectives_of_alternative_dispute_resolution

[3] "Domain name disputes," BITLAW, accessed 03 October 2022, https://www.bitlaw.com/internet/domain.html

Internet worldwide is crucial for many other objectives and aspirations in the broader context of Internet-related policies, especially in the domain name sphere.

Existing academic research on domain name disputes is fragmentary, one-sided or incomplete. Most of them only outline the existing domain name disputes without proper analysis of their problematic aspects or solutions.

From the scientific relevance of this thesis, the entire analysis intends to show the defects of the current legal system while dealing with domain name disputes in particular.

With regard to the supranational nature of the Internet domain name disputes can occur in a country different from where it is registered. As for today, there is no consistency concerning the legal regulation of domain names all around the world, though having a harmonised, unambiguous, universal regulation could prevent potential conflicts and give more clarity to the parties of the dispute.

Fairly, it must be stated that attempts have been made to standardise the dispute resolution procedure and during the Internet evolution the legal regulation of domain names became more clear. Though, still, certain amendments are required in order to keep up with a rapid Internet development pace and respond effectively to problematic challenges governing new types of domain name disputes in a modern and consistent manner. Some amendments to the existing legal regulation will be suggested further in this master thesis.

Scientific novelty and overview of the research on the selected topic.

Different scholars, as well as international and regional organisations, in their articles, looked into prospects and challenges related to domain name dispute regulation. All researchers in their works refer to domain name history and the evolution of the domain name dispute resolution mechanism.

In particular, the domain names were explored by Sara María Ballester Climent, Begoña Payá Todolí, who discovered the legal problematic of the domain name[4]. Snehlata Singh[5] and Zohar Efroni[6] in their works covered the issue of conflicts between trademarks and domain names. The contributing discussion was made by Ángel García Vidal, an author of numerous

[4]Sara María Ballester Climent and Begoña Payá Todolí, "Domain names," https://www.uaipit.com/uploads/publicaciones/files/0000002011_dn.pdf

[5] Singh, Snehlata, "Conflicts between Trademarks and Domain Names: A Critical Analysis," 14 September 2011, https://ssrn.com/abstract=2045222

[6] Efroni, Zohar, "Names as Domains, Names as Marks: Issues Concerning the Interface between Internet Domain Names and Trademark Rights," INTELLECTUAL PROPERTY AND INFORMATION WEALTH: ISSUES AND PRACTICES IN THE DIGITAL AGE, Peter K. Yu, ed., Praeger Publishers, (2007), https://ssrn.com/abstract=957750

publications on domain names, including the books “El derecho español de los nombres de dominio” (Spanish domain name Law) and “Derecho de marcas e Internet” (Trademark law and Internet). Marius Kalinauskas and Mantas Barčys researched the legal challenges related to the regulation of the domain name system.

Authors such as Jonathan Agmon, Staey Halper, and David Pauker have established a typology of disputes around domain names, outlining general types of problems encountered by companies that have a “famous” name, etc. Eric Perrott, Sophie Edbrooke as well as Warren B. Chik covered the effectiveness of the UDRP Procedure in resolving domain name disputes. Elisa Cooper in her “How to win UDRP domain name disputes research” [7] outlines important aspects of the procedure the parties should definitely take into account. The problematic issues of the domain name dispute regulation in Ukrainian legislation and case law were discovered by Taras Kyslyy, Kateryna Oliinyk, Tetiana Kudrytska, Victoria Sopilnyak and Anastasia Kazankina, Ilarion Tomarov, Kostiantyn Zerov, Baadzhi Natalia etc.

However, I have not found any relevant research that deeply examines and emphasises the problematic aspects of existing regulation of domain name disputes.

Significance of research.

The deep analysis presented in the research defines the status of domain names in intellectual property. It covers the existing domain name legal system and domain name dispute policy within the USA, the EU countries and Ukraine.

While discovering that the current legal system is incapable of handling domain name issues effectively, this master thesis concludes with the same remark and suggestions that might help in this situation.

The research discusses in detail the causes and kinds of domain name disputes and what the current legal system offers to this situation. Conflicts such as cybersquatting, typosquatting, and reverse domain name hijacking are discussed in length with the help of relevant case laws. This thesis covers new types of infringements in the domain name sphere such as soundsquatting or levelsquatting and the challenging questions they bring to the current regulatory system.

The existing UDRP, UA-UDRP Policies and the problematic aspects for the parties during the dispute resolution process have been analysed in detail. A deep comparative analysis

[7]Elisa Cooper, How to win UDRP domain name disputes, 26 July 2022, https://www.worldipreview.com/contributed-article/how-to-win-udrp-domain-name-disputes

is made in order to describe the advantages and disadvantages of the UDRP procedure and traditional litigation.

The aim of the research.

Considering that problematic aspects of legal regulation of domain name disputes have not been sufficiently investigated, the main goal of this master thesis is to explore the current domain name dispute resolution Policy within the USA, the EU, and Ukraine and identify the problematic issues in domain name dispute regulation.

The objectives of the research.

In order to achieve this aim the following objectives were formulated:

1. To analyse the existing domain name legal system and domain name disputes resolution policy within the USA, the EU countries and Ukraine;
2. To identify the most problematic types of domain name disputes and analyse their causes;
3. To discover the existing resolution mechanisms while disclosing specific measures and rules in the Uniform Domain Name Dispute Resolution Policy and applicable case law;
4. To answer the controversial and sore question: what are the most problematic aspects of legal regulation of domain name dispute and determine possible solutions;
5. To evaluate the tendencies related to domain name disputes policy.

Research methodology.

- Analysis of scientific literature on domain name disputes regulation;
- Data collection and descriptive data analysis towards legal regulations of domain names and dispute procedures within the USA, the EU and Ukraine in order to find common patterns among policymakers' approaches in different countries;
- Analysis of statistic data regarding domain names to determine variables that cause a rise in the number of specific types of domain names dispute;
- Structural and functional methods in determining domain name nature;
- A comparative synthesis of domain name disputes regulation within the USA, the EU and Ukrainian to determine and compare the dispute resolution procedure;
- Comparative data analysis of the USA, the EU and Ukrainian court practice and UDRP case practice in the field of domain name dispute relations aiming to identify future tendencies in the domain name disputes regulation;

The practical significance of the master thesis.

From a practical point of view, this research could be useful for academics, lawyers, students, and legal authorities who are involved in the scope of discussion about a domain name legislative framework and domain name dispute policy, which is currently taking place. Also, Internet users such as businesses and physical persons could find out from the thesis clarification of the existing procedure and relevant case law regarding the topic in order to be aware of possible ways to protect their rights and legitimate interest in this sphere.

Besides, the thesis not only provides an analysis of the effectiveness of a domain name disputes policy in the USA, the EU and Ukrainian law but also gives examples of possible solutions to the problematic accepts that are still arising. Analysis of possible amendments may help lawmakers to reduce the number of domain name disputes improving the legal regulation in this field.

Structure of the research.

This master thesis consists of a list of abbreviations and an introduction part, 3 chapters, conclusions and a list of applicable sources. The first chapter introduces the notion of domain names and Domain Name System (DNS), reveals their main functions and explains why they are so commercially valuable. This chapter also describes the evolution of the management of the DNS and specifies in detail the ICANN's role in DNS administration. The current legal and regulatory framework (the USA, EU and Ukraine) is also outlined in this chapter while determining the ambiguity, non-uniformity, and other drawbacks of the existing legislation.

The next chapter identifies the most problematic types of disputes that may occur in the domain name field (such as Cybersquatting, Typosquatting, Passing off domain names, Cyber twin and Reverse domain name hijacking, etc.) and analyses their causes.

The last chapter covers the existing Domain name disputes Policies and describes the problematic aspects arising in their application. It describes in detail the UDRP and UA-UDRP resolution procedures, determining their advantages and disadvantages compared to the traditional court litigation procedure. UA-UDRP policy was described in comparison to the general UDRP procedure. The pros and cons of UA-UDRP implementation in Ukraine were discussed below in this research.

The thesis also includes an analysis of tendencies related to domain name dispute regulation and comes to an end with conclusions and suggestions.

Defence statements.

1. Domain names should not be regulated under trademark law and special law shall be adopted to single out a separate object of intellectual property rights - a domain, establish its legal regime, the status of the domain name owner, and ensure effective protection of their rights and interests;
2. UDRP procedure, though having its drawbacks, is more effective than traditional litigation in domain name dispute resolution;
3. UDRP procedure shall be amended is the following way: UDRP decisions must be consistent not only with the provisions of the applicable policy, but also with the relevant previous decisions under the procedure, and with the relevant summaries, which are set out in the WIPO Overviews (where appropriate); appeal procedure under UDRP shall be established.

III. THE NOTION OF DOMAIN NAME

In order to discuss domain name disputes and possible problematic aspects in its regulation, it is necessary to have a clear understanding of what domain names and their main functions are, and how they are currently treated in different jurisdictions.

1. Nature, definition and functions of the domain name

Nowadays, unfortunately, there is no consensus in doctrine and case law on the *legal* nature of domain names. While analysing the approaches of different scholars to what the domain name is, most of them (whether lawyers or IT specialists), usually provide the same definition, describing the domain name mostly from the *technical* point of view. However, it is fair to agree with the Bulgarian researcher G. Dimitrov who, while admitting that domain name definition is clear from the technical point of view, outlined that "up to now there is no serious doctrinarian research giving a clear answer on what the domain name is from the legal point of view."[8]

The Norwegian researcher T. R. Gulliksen outlines that: "Domain names are the plain word references to the IP addresses".[9] At the same time, Elen Rony and Peter Rony have defined a domain name as "[a] unique alpha-numeric designation to facilitate reference to the sets of numbers that actually locate a particular computer connected to the global information network"[10], etc.

All these definitions corresponded to domain names when the Internet was used mainly for research purposes and was not so important for economic success. However, nowadays we all experience drastic changes in the domain name functioning as its usage rapidly increases over the years. While the importance of domain names is still rising, from a legal point of view, it is very important for the legislators to take into account the social and economic aspects.[11]

---

[8] Dimitrov George, "INTELLECTUAL PROPERTY THE INTERNET AND ELECTRONIC COMMERCE LEGAL PROTECTION OF DOMAIN NAMES," paper presented at International Conference on Intellectual Property, the Internet, Electronic Commerce and Traditional Knowledge, May 2001. https://www.wipo.int/edocs/mdocs/ip-conf-bg/en/wipo_ectk_sof_01/wipo_ectk_sof_01_1_6.pdf

[9] Gulliksen T. R., "Internet Domain Names and Trademarks," COMPLEX, 2/01. – Oslo: Institut for rettsinformatikk, 2001, quoted in Darius Sauliūnas, "Problems of legal nature of internet domain names," (Law University of Lithuania),33. https://repository.mruni.eu/bitstream/handle/007/13436/3330-6980-1-SM.pdf?sequence=1&isAllowed=y

[10] Ellen Rony and Peter. R. Rony, *The Domain Name Handbook: High Stakes and Strategies in Cyberspace* (Lawrence, Kan.: R&D Books, 1998).

[11] Darius Sauliūnas, "Problems of legal nature of internet domain names," *Jurisprudencija*, 2003, t. 47(39), 15 December 2003: 33, https://repository.mruni.eu/bitstream/handle/007/13436/3330-6980-1-SM.pdf?sequence=1&isAllowed=y

Unfortunately, the current legal regulation in the domain name field worldwide still does not reflect all these issues entirely causing uncertainty for its administration. In most jurisdictions, there is no specific law covering domain names, accordingly, the general provisions of domain names are separated within different laws (mostly trademark laws). Domain name legal definition may vary in different legislations despite the worldwide usage of the Internet without any territorial boundaries.

Here are a few legal approaches to domain names within the USA, EU and Ukrainian legislations analysed further in this master thesis:

The USA

As the Internet originated in the USA, it is important to understand how the concept of a domain name was reflected in US law in the first place. The applicable statute containing a domain name definition in the USA is the Lanham (Trademark) Act of 1946, in accordance with which the term "domain name" means any "alphanumeric designation which is registered with or assigned by any domain name registrar, domain name registry, or other domain name registration authority as part of an electronic address on the Internet".[12]

The EU

The EU legislation approach to domain names, as a general principle, is outlined in the Communication from the Commission to the Council and European Parliament on the issue of organisation and management of the Internet, issued in Brussels in 2000. Following the document, domain names were considered as "means of addressing which are used to route data from one host computer to another" while importantly endowing the domain names with the identification function, specifying that the very names "serve for easy identification of the Internet hosts".[13]

Ukraine

In Ukraine, there is also no specific law regulating the domain name issue. There are a few related legal acts which, however, define the domain names in different ways. The Law of Ukraine "On Telecommunications" dated November 18, 2003, contains the following definition of "domain": "part of the Internet hierarchal address space having a unique identifying name and served by a group of domain names servers and administered in a centralized manner".[14] At the

[12] "Lanham (Trademark) Act," 1946, accessed 17 October 2022. https://www.bitlaw.com/source/15usc/index.html

[13] Communication from the Commission to the Council and the European Parliament, "The Organisation and Management of the Internet International and European Policy Issues 1998 – 2000." Brussels, COM(2000) 202 final, 11 April 2000, accessed 15 October 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52000DC0202&from=EN

[14] Law of Ukraine "On Telecommunications", November 18, 2003, accessed 17 October 2022, https://www.wto.org/english/thewto_e/acc_e/ukr_e/wtaccukr98a13_leg_1.pdf

same time, the Law of Ukraine "On Protection of Rights to Marks for Goods and Services" outlines that "domain name shall mean a name used for addressing computers and resources on the Internet".[15]

While having some differences in defining domain names, we can highlight important similarities in their regulation as some functions performed by domain names are indirectly described in the existing legal definitions.

Darius Sauliūnas fairly defines the main functions performed by domain names as follows:

1. Firstly, a domain name identifies the origin (the source) of the domain;
2. Secondly, domain names distinguish the domains of one person from those of another;
3. Thirdly, a domain name may serve as a symbol of quality;
4. Fourthly, a domain name is the means of advertisement.

The researcher also considers that all those functions of a domain name correspond to some extent to those of the trademark, the main function of which is a distinguishment from other goods. Moreover, according to WIPO research, it is concluded that trademarks are also capable of functioning as the identifier of the origin (the source), a symbol of quality, and the means of advertisement.[16]

To sum up, we can see that both trademarks and domain names have a lot of common features, they are closely linked in that they both indicate origin, and both acquire substantial value. This provides the initial justification for their parallel interaction and liaison. Though a domain name cannot be protected as a trademark because it is merely an address on the Internet, however, in addition to using the name in commerce, it must be used in a way that distinguishes the websites of different businesses/persons.

It is also important to keep in mind that domain names, compare to the trademark, are effectively international in scope. Accordingly, if there is no difference in whether you physically register the name, you will hold the domain name for the Internet in general. Unlike trademarks, which can co-exist in different jurisdictions and in different product and service markets simultaneously, there is only one "domain.com" version of the name and only one person can register it at a time.

---

[15]Law of Ukraine "On Protection of Rights to Marks for Goods and Services", December 15, 1993, accessed 17 October 2022, https://ukrpatent.org/atachs/tm-law-of-ukraine.pdf

[16] Sauliūnas, *supra note*, 11: 34.

As we can see, identifying and distinguishing functions of the domain names are already indirectly reflected in some legislations. Accordingly, in order to better understand the domain names' legal nature it is necessary to have a generally consistent approach considering not only "technical" but also the legal and economic aspects of certain domains in all the legislations taking into account worldwide Internet usage.

2. Domain name system (DNS)

Having an understanding of the legal definition of the domain name it is important to indicate what types of domain names are and how they are treated in cyberspace.

One of the cornerstones of how the Internet operates is the existing Domain name system (DNS) which ensures smooth and fast Internet work, without being stuck while memorizing long lists of numbers (IP addresses) to access the content we want.

A domain name system is a naming database in which Internet domain names are located and translated into Internet Protocol (IP) addresses. An IP address is a numeric address that indicates the location of a computer on the Internet. It is represented as strings of digits divided into parts or fields. Every IP address is linked with a unique domain name, which is a part of the domain name system (DNS). When a domain name is typed into a computer, the Internet software automatically converts the domain name to its numbered address.[17]

In simple words, the domain name system maps the name people use to locate a website to the IP address that a computer uses to locate that website. Web browsing and most other Internet activities rely on DNS to quickly provide the information necessary to connect users to remote hosts.

Users are usually seeking fairly concrete information amongst the endless supply available online, and domain names may direct them to the right destination where information is located and may indicate the origin and authenticity of the content. The Internet without its alphabetic addressing system somewhat resembles a giant metropolis where no street names exist and no residents' nameplates hang in front of its countless buildings, houses, and apartments.[18]

DNS mapping is distributed throughout the Internet in a hierarchy of authority. The hierarchical structure is relevant for the functioning of the DNS and the iterative way of looking up domain names.[19]

---

[17] Sauliūnas, *supra note*, 11: 32.
[18] Snehlata, *supra note 5.*
[19] "The Domain Name System (DNS)," The Council of European National Top-Level Domain Registries (CENTR), accessed 18 October 2022. https://www.centr.org/about-the-industry/item/the-dns.html

Access providers and enterprises, as well as universities, governments, or other organisations, typically have their own assigned ranges of IP addresses and assigned domain names. They also typically run DNS servers to manage the mapping of those names to those addresses. Most Uniform Resource Locators (URLs) are built around the domain name of the web server that takes client requests.[20]

Let's look a little bit closer at the DNS framework.

DNS is based on the so-called concept of an upside-down tree of named domains, where the domain is a named branch (or a sub-tree) in a tree of DNS names. At the core of the domain name system, hierarchy is the concept of delegation and authority. The DNS tree consists of nodes and each node has a “label” separated by [.].

The Internet Engineering Task Force (IETF) has specified Rules about implementing domain names in Request for Comments (RFC) 1035.[21] Under these Rules, the maximum length of each label is 63 characters, and a full domain name can have a maximum of 253 characters.

Labels can only consist of letters of the alphabet, numbers, and symbols "-" (hyphen), but under Rules, a domain name must not start or end with a hyphen and not have a fully numeric TLD name.[22]

It is also important to outline that uppercase and lowercase letters are treated as equivalent, which means that domain names are case-insensitive. Accordingly, the sequence of characters "Com", "COM", "cOm", "com", etc. mean the same name.[23]

As we can see from *Figure 1* below, like the IP numeric addresses, the domain names are divided into fields separated by dots, which separate them into levels:

1) Root domain

2) Top-level domain

3) Second-level domain

4) Sub-domains

5) Name of the host

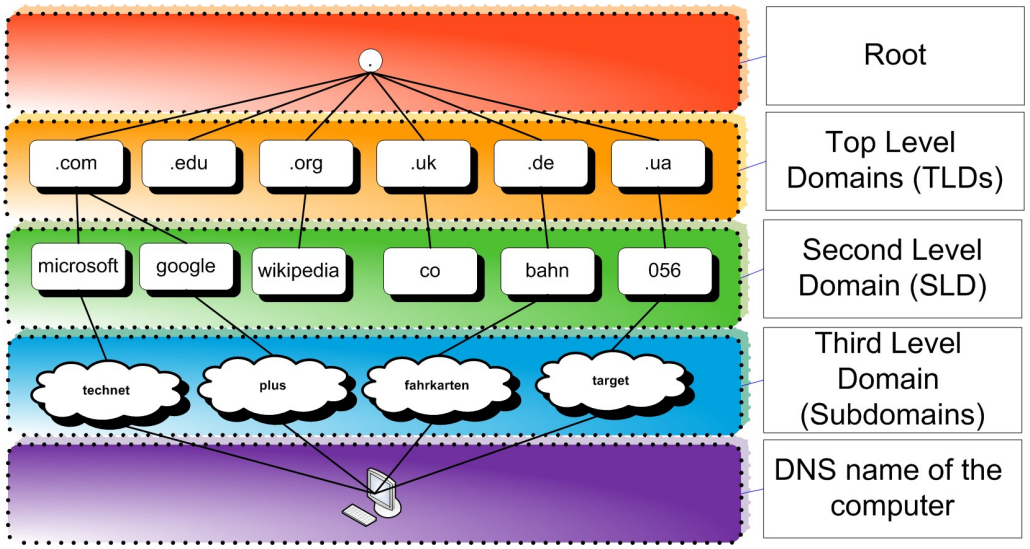
---

[20] Ben Lutkevich and John Burke, “Domain name system (DNS),” last updated in August 2021, accessed 20 October 2022, https://www.techtarget.com/searchnetworking/definition/domain-name-system

[21]“DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION,” The Internet Engineering Task Force (IETF), November 1987, accessed 22 October 2022, https://datatracker.ietf.org/doc/html/rfc1035

[22] “History of Internet Resources Management in Japan Focusing on Domain Name and IP Address,” April 2015, accessed 12 October 2022. https://www.nic.ad.jp/timeline/en/20th/appendix1.html

[23]Jane Kruch, “DNS: what is it and how it works,” accessed 15 October 2022, https://en.wikiversity.org/wiki/User:Jane_Kruch/DNS:_what_is_it_and_how_it_works



(Figure 1) [24]

1. **Root domains -** the totality of Internet hosts. The root domain is signed as "." and is conditional since it is not administrated. It is the highest hierarchical level of a site and represents the delegation details of top-level domains. [25]
2. **Top-level domains (TLDs) -** domain extensions used to categorise websites by type, location or business model. Administration starts from the top-level domains distinguished in the 1980th.[26]

The top-level of the hierarchy appears after the last dot ('.') in a domain name. For example, in "www.mruni.eu", the top-level domain name is **.EU**. The .EU domain name is a way for organisations and citizens to show their European identity online. It contributes to greater online visibility and evolving consumer needs, increasing user choice of domain names and promoting e-commerce.[27]

Out of the thousands of domain extensions available on the web, the most useful ones are[28]:

- ☐ .COM is the most common top-level domain name which is used to indicate that the domain name is owned by a commercial enterprise;

[24]Photo by Jane Kruch "The structure of DNS," December 01, 2013, accessed 15 October 2022, https://uk.wikipedia.org/wiki/%D0%A4%D0%B0%D0%B9%D0%BB:Structure_DNS.jpg

[25] "What is a root domain?" Online Marketing Glossary, 10 January 2019, accessed 19 October 2022, https://raventools.com/marketing-glossary/root-domain/

[26] J. R. Ricart, ".ORG vs .COM vs .NET: What Do They Mean and Which Is Better?" Wix Blog, accessed 20 October 2022, https://www.wix.com/blog/2020/06/org-vs-com-vs-net-domain-extensions/

[27]".EU domain name: Questions and answers. | Shaping Europe's digital future," European Commission, last update 22 February 2022, accessed 19 October 2022, https://digital-strategy.ec.europa.eu/en/faqs/eu-domain-name-questions-and-answers

[28] Bitlaw, *supra note, 3.*

- ☐ .NET is the second most popular extension. The .net domain name extension stands for "network" and Internet-related organisations and was originally meant to be used by umbrella websites acting as a portal for smaller sites;
- ☐ .ORG stands for non-profit organisations and is primarily used for nonprofit websites such as charities, NGOs, open-source projects, and educational platforms;
- ☐ .EDU generally describes the entity owning the domain name as a four-year college or similar educational institution;
- ☐ .GOV was established to make it easy to identify US-based government organisations on the Internet. The US Government, all 50 states, and many local governments use .GOV for their domains.

All of them are generic top-level domains (**gTLD**).

According to the Domain names Discussion Paper issued by the EUIPO, the global market had grown to an estimated '375 million domains under management with a split of 66 % to gTLDs and 34 % to ccTLDs'.[29]

Suddenly, everyone needed a website, which led to a new problem: the .com and .net domain spaces of the world were becoming saturated. To combat this overcrowding of the Internet namespace, over 1,300 new generic TLDs have been launched in the past years. While .com remained the most popular choice for a long time, these new extensions helped make domain registration more accessible.[30]

After completing the New gTLD Program launched by ICANN, a new gTLD becomes part of the Internet when it is delegated. This means it is introduced into the Internet's authoritative database, known as the Root Zone. As for now, the expansion of generic Top-Level Domains in the Domain Name System is still underway. [31]

In addition to gTLD, each country has been given a unique top-level domain name - **ccTLD** (country code Top Level Domain). For instance, .UA domain indicates domains in Ukraine and .LT indicates a Lithuanian domain, etc. The high importance of the ccTLDs is that it is the single strongest way to show search engines and users that site content is specifically

[29]Domain names Discussion Paper "Challenges and good practices from registrars and registries to prevent the misuse of domain names for IP infringement activities," European Union Intellectual Property Office, March 2021, accessed 19 October 2022, https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2021_Discussion_Paper_on_Domain_Names/2021_Discussion_Paper_on_Domain_Names_FullR_en.pdf

[30]Rebecca Scott, "The evolution of Domains. Crazy Domains Learn," 4 October 2022, accessed 25 October 2022, https://www.crazydomains.com.au/learn/evolution-of-domains/

[31]"New gTLDs,"ICANN, accessed 26 October 2022, https://newgtlds.icann.org/en/program-status/delegated-strings

targeted to a certain country or region — but, importantly, not specifically a certain language. When a site uses a ccTLD, Google assumes that the site (and all the content on it) is specifically relevant to the geographic area targeted by the ccTLD and should appear on SERPs in that area.[32]

3. While TLD extensions are very important to categorise websites by type, location or business model, **"second-level"** domain names (SLD) play the biggest role in determining the credibility of the site and how it aligns with someone's brand. All the disputes that arise over domain names involve SLD.

The second-level name is the name directly to the left of the top-level domain name in an Internet address.[33] For instance, in the address "www.mruni.eu", the second-level domain name is "**mruni"**.

While top-level domains are restricted to a finite number of options, the possibilities for second-level domains are nearly endless. The SLD is a great space for somebodies brand name, product name, or personal name.[34] Accordingly, the disputes arising over SLD are always challenging and debatable as domain name protection is of high importance for all people, businesses and organisations involved in the dispute resolution process.

It is important to keep in mind that two identical second-level domain names *cannot coexist* under the same top-level domain.

For example, even though both i.e. "Ivanka IT Company" and "Ivanka Airlines" would like the "ivanka.com" domain name, only one Ivanka company can have ivanka.com. For both "Ivanka IT Company" and "Ivanka Airlines", the parent company is "Ivanka Financial Inc", Delaware. Accordingly, instead of using "ivanka.com", "Ivanka Airlines" can use "ivankaairlines.com", while "Ivanka ITech Company" - "ivankaIT.com" (P.S. all company names are fictitious).

4. **Third level domain** is related to the main or root domain and is the portion to the left of the second-level domain.

They are called **subdomains** as sometimes they refer to specific sections or pages of a website. The third-level domain name refers to different servers within different departments of a

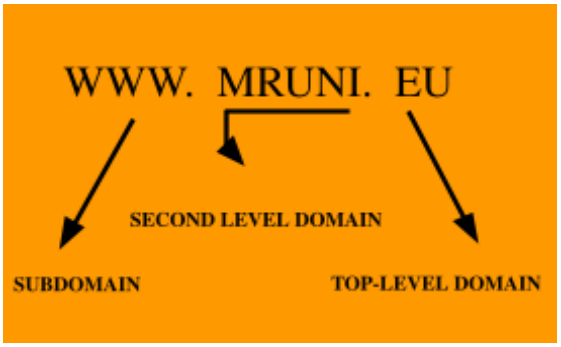
[32] "What are ccTLDs? Why do they matter?" Moz, accessed 25 October 2022, https://moz.com/learn/seo/cctlds
[33]"Second-level domain - MDN web docs Glossary: definitions of web-related terms: MDN," last modified: 21 September 2022, accessed 27 October 2022, https://developer.mozilla.org/en-US/docs/Glossary/Second-level_Domain
[34]"What's in a Domain Name: Sub, Second-Level, Top-Level and Country Code Domains Insight," Hover Blog, 24 December 2020, accessed 27 October 2022, https://hover.blog/whats-a-domain-name-subdomain-top-level-domain/

company. In larger organisations, each division or department might have its own third level domain, which can serve as an effective means for identifying it. The third level domains are not mandatory unless the user has a specific requirement.[35]

For example, if the person or the organisation want to have its own domain (if it is still free till that moment), such as “ivanka.org” and decides to operate a blog on a subdomain, the domain would be - “blog.ivanka.org”. As we can see, the third-level domain names provide the growth of the DNS name tree.

WWW is the default third-level domain name and the most commonly used, as in the address "www.mruni.eu".

To sum up, let's have a look at the domain name www.mruni.eu as an example. The DNS of www.mruni.eu is the following:



(*Figure 2)*

Accordingly, as was mentioned before, a) the TLD is - .EU; b) the second-level domain is .mruni and c) the third level domain is www.

3. Management evolution of domain names, ICANN

As we already know, each address has to be unique for computers to know where to find each other. Nowadays, to reach another person via the Internet you have simply to type an address into your device - a number or a name. However, it was not that easy at the very beginning. In the years after Internet's creation, its evolution and management became a challenging task for the international community. Accordingly, it is important to understand how we get there and who deals with DNS management as the power and impact of the Internet have drastically changed during the past decades.

As the Internet originated in the USA, up to 1998, its technical infrastructure had been run by the United States Government agencies, such as DARPA and the National Science

[35]“What are third level domain names?” Softlink Options Limited, 14 September 2022, accessed 28 October 2022, https://softlinkoptions.co.ke/third-level-domain-names/

Foundation, having most of the legal control over the domain name system (DNS). However, in the late 80's, and early 90's, the Internet began to grow into a worldwide resource and become very commercialised.[36] Accordingly, the US Government needed to take some actions concerning DNS regulation and began to look for ways to transfer its administrative functions to the private sector.

To achieve this goal, significant changes were made in 1998:

June 05, 1998, the National Telecommunications and Information Administration (NTIA) of the DOC issued a policy statement, the "White Paper," calling on private sector Internet stakeholders to form a non-profit corporation to take over the administration of the DNS and the Internet numbering system. This action meant that the White House de facto handed over DNS control to the Internet Corporation for Assigned Names and Numbers (ICANN) - a US-based not-for-profit public-benefit corporation - while keeping some less visible powers.

The legal basis of the newly created ICANN – DOC relationship was based on three agreements[37]:

1. Memorandum of Understanding (MOU,1998), later replaced by a Joint Project Agreement (JPA) (2006);
2. ICANN's Cooperative Research and Development Agreement (CRADA) with the U.S. Government (1999);
3. The contract between ICANN and the U.S. Government for the performance of the so-called IANA (Internet Assigned Names and Numbers) function relating to the operational management of the root zone file, and the assignment of Internet Protocol (IP) numbers and protocol numbers (2003).

Up to date, the ICANN manages the domain name system and allocation of IP addresses across the world. Without such coordination, we wouldn't have one global Internet as we got used to now.

ICANN describes their goal as being to "preserve the central coordinating functions of the global Internet for the public good." The ICANN has responsibility for the assignment of

[36] Marius Kalinauskas and Mantas Barčys, "Legal Challenges Related to the Regulation of a Domain Name System," *Social Technologies*, ISSN 2029-7564 (2012): 368, https://www3.mruni.eu/ojs/social-technologies/article/view/203/194

[37] *Ibid.*

Internet protocol parameters, oversight of the domain name system, allocation of IP addresses, and management of the root server system.[38]

According to ICANN Fact Sheet: "as a technical coordinating body, ICANN's mandate is not to "run the Internet". Rather, it is to oversee the management of only those specific technical managerial and policy development tasks that require central coordination: the assignment of the Internet's unique name and number identifiers." [39]

On March 10, 2016, ICANN and the DOC signed a historic, culminating agreement to finally remove ICANN and IANA from the control and oversight of the DOC.[40] On October 1, 2016, ICANN was freed from U.S. government oversight. It means that since October ICANN was granted complete independence and ownership over the Internet directory which led to a significant change in Internet policy, ending the era of the multilateral Internet governance system.

Registration

Though ICANN coordinates the domain name system by overseeing the distribution of unique IP addresses and domain names, the rights to register and administer top-level domains were delegated to registrars accredited by ICANN. Registrars are entities providing domain name registration services to the public on the basis of an accreditation agreement with the relevant registry (as indicated in the Article 2 of Regulation 2019/517 [41]).

Prior to December 1999, a company called Network Solutions Inc. ("NSI") was almost solely responsible for the registration of second-level domain names for the most popular top-level domains, including .COM, .NET, and .ORG. Since the vast majority of domain names are under one of these top-level domains, Network Solutions had a great deal of control over how domain names were registered, and how disputes would be resolved. To avoid having to be the arbitrator between two parties who both desire the same domain name, NSI decided to simply adopt a first come, first serve arrangement with respect to domain names. Under this scheme, NSI would not question an applicant's right to have a particular domain name. If the domain name was available, the applicant was given the name.[42]

---

[38] "ICANN, Internet corporation for assigned names and numbers," accessed 28 October 2022, https://www.livinginternet.com/i/iw_mgmt_icann.htm

[39] "International Telecommunication Union - ICANN and the Global Internet," Workshop on Member States' experiences with ccTLD Geneva, 3-4 March 2003, accessed 28 October 2022, https://archive.icann.org/en/cctlds/icann-and-the-global-internet-25feb03.pdf

[40]Maria Farrell, "Quietly, symbolically, US control of the internet was just ended," *The Guardian*. ISSN 0261-3077 (March 14, 2016). https://www.theguardian.com/technology/2016/mar/14/icann-internet-control-domain-names-iana

[41]Regulation 2019/517, 19 March 2019, accessed 29 October 2022, https://eur-lex.europa.eu/eli/reg/2019/517/oj

[42] Bitlaw, *supra note, 3.*

Following 1999, the ability to TLDs was spread out among many registrars. However, following NSI's precedence, all of these registrars continue to assign names on a so-called first-come, first-served basis and do not do any checking before assigning a new domain name.[43]

It is important to keep in mind that when assigning a domain name, NSI exercises veto power over requested names that are not identical to names already assigned domain names. This policy always creates a problem as NSI does not conduct a search to determine whether a third party is registering a trademark as a domain name.[44]

The lack of prior examination of the applications for a new domain name against the existing rights of third parties covers not only trademarks but also company names or personal names. Consequently, businesses bear the responsibility of policing their trademarks to ensure that their trademarks are not infringed or diluted which always leads to problems in the Domain name Vs. Trademark relationship.

As for today, the registrars maintain a database that contains all the information about their zone, they keep track of who owns a domain, where its name servers are located, and so on. Then they communicate the necessary technical information to the appropriate registries for inclusion on the top-level domain name servers.[45] The most popular registrars include GoDaddy, Tucows, Register.com, and Dotster.

Before registration, the registrar will check if the domain name is available for registration and create a WHOIS record with the domain name registrant's information. It is also possible to register domain names through a registrar's resellers.[46]

In Ukraine, for example, the "Hostmaster" LLC provides services for the administration and corresponding support of the .UA domain and public domains in it. National registrars grant domain registration rights under the terms of a domain administration agreement.[47]

Ownership

---

[43] *Ibid.*

[44] Michael Tanner, "Trademarks, Internet Domain Names, and the NSI: How Do We Fix a System That Is Already Broken," *Journal of Technology Law & Policy:* Vol. 3: Iss. 2, Article 3 (1998). https://scholarship.law.ufl.edu/jtlp/vol3/iss2/3

[45]"Domain name registration process," ICANN, last update July 2017, accessed 29 October 2022, https://whois.icann.org/en/domain-name-registration-process

[46] *Ibid.*

[47]Бааджи Н.П. "Доменне ім'я як об'єкт права інтелектуальної власності", p. 670, http://dspace.onua.edu.ua/bitstream/handle/11300/7281/%D0%91%D0%B0%D0%B0%D0%B4%D0%B6%D0%B8%D0%BD%20%D0%94%D0%BE%D0%BC.%20%D1%96%D0%BC%E2%80%99%D1%8F.pdf?sequence=1&isAllowed=y

While ICANN is responsible for the management of the Domain Name System and registrars are dealing with the registration and administration issues, the important question arises - *"Who is the actual domain owner?"*.

Domain names are owned by whoever first registered the web address with an accredited registrar (first-come, first-serve basis). In order for the person to maintain ownership, they have to pay registration fees and ensure that all of their contact details are up to date. Once a person has legally registered for a domain name and has given all of the relevant personal information to an accredited registrar, that individual owns the rights to that web address. They are in sole possession of that web address and have the right to sell it at any time. The owner can transfer domain name ownership to a new user if they care to do so.[48]

Possibility to determine the domain name holder is very important when a dispute over the existing domain name arises. There are a few ways to define the owner if you know only a website's domain name.

In most cases, the easiest way to find a domain name owner is by searching WHOIS databases, coordinated through ICANN.

WHOIS is a query and response protocol that is widely used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block or an autonomous system, etc.[49] These are free, publicly available search tools that contain almost every single website and domain name. WHOIS services work in conjunction with registrars like Domain.com, collecting all of the information related to the purchase, sale, and transfer of domain names.[50]

Since the establishment of the Internet, it went through quick cycles of evolution in terms of power and accessibility. As we can see, the administration of domain names becomes a really important though complicated challenge for the international community. Nowadays, domain name management is mostly coordinated by ICANN and accredited by ICANN institutions. We can observe that the number of domain names keeps growing these years as well as new challenges in their regulation.

---

[48]"How to find a domain name owner," 12 March 2021, accessed 30 October 2022, https://www.domain.com/blog/find-a-domain-name-owner/

[49] RFC 3912, WHOIS Protocol Specification, L. Daigle, September 2004, last update 02 March 2013, accessed 30 October 2022, https://datatracker.ietf.org/doc/rfc3912/

[50] "How to find a domain name owner," *op. cit.*

4. Current legal and regulatory framework (the USA, EU and Ukraine)

Domain Name Law become a complex area of the law due to the challenging issues in its regulation.

Since its creation, the domain name system mostly illustrates a fundamental dichotomy between trademark law and the complexities of Internet technology: while trademark law is territorial, the Internet is universal.[51]

As for now, there is no specific legal regulation covering domain names in different jurisdictions. Accordingly, the governance of the Domain name system is one such area where unilateral efforts to address the problem of domain name disputes and trademark infringement have resulted in a skewed and inconsistent system of governance.

Trademark law & domain name

Due to that, courts while recognising the commercial importance of domain names, thus apply traditional principles of trademark law to domain name disputes. However, traditional principles of trademark law usually are not capable to resolve the problem created when two parties have a valid claim to a specific domain name. This situation arises either because both parties own the trademark in different geographic areas or because they use the trademark in connection with different goods or services.

The trademark law was also not necessarily well suited to all types of domain name disputes, including situations where the domain name was not, strictly speaking, a trademark. Cases involving personal names and culturally/geographically significant terms were obvious examples.[52]

The lack of clear legal identification of domain names has led to the so-called cybersquatting (described in detail in the next Chapter of this thesis) and other problematic situations. As a result, while analysing a case law in this sphere, courts consistently favour trademark owners when one party, commonly known as a cybersquatter, registers a well-known trademark as a domain name for the sole purpose of collecting money from the trademark's owner.

---

[51] Alice A. Wang, "Diversifying the Domain Name Governance Framework," *Berkeley Technology Law Journal* 32, no. 1 (2017), https://www.jstor.org/stable/26488663

[52] Natalia Ramirez, "Will the Anticybersquatting Consumer Protection Act Create More Problems Than It Solves?" *Washington University Journal of Law & Policy,* Vol. 8 (2002): 412–13. https://docplayer.net/230894928-Will-the-anticybersquatting-consumer-protection-act-create-more-problems-than-it-solves-natalia-ramirez.html

All these issues become very challenging to the lawmakers. Accordingly, in order to adapt existing principles of trademark law to the cyberspace realities and to protect the goodwill of trademark owners, a bill that addressed cybersquatting was adopted in the USA on November 29, 1999 - the Anticybersquatting Consumer Protection Act (ACPA). The ACPA, as enacted, uses traditional trademark infringement and dilution principles to determine whether a person has infringed or diluted the mark in bad faith.[53]

Natalia Ramirez in her research fairly outlined that the ACPA's effect, however, merely codifies existing cybersquatting case law, which scarcely addresses the difficult issue created when both parties have a valid claim to the same domain name.[54]

Another problematic aspect is that as the Internet is borderless, due to the global presence of most businesses in the World Wide Web, domain name disputes also can occur in a country different from where it is registered.

Alice A. Wang outlines that legally, the existing ACPA ignores the fact that trademark law is governed nationally, failing to account for the possibility that there might be legitimate foreign trademarks that would conflict with U.S. trademarks. By giving U.S. trademark holders a right of action in U.S. courts where the foreign interested party may be absent, the ACPA favours U.S. trademarks without attempting to reconcile them with other legitimate trademark claims. Accordingly, the extraterritorial application of in rem actions to domain names registered abroad by a foreigner violates due process because the minimum contacts requirement established by the Supreme Court in Shaffer v. Heitner case[55] is not met.[56]

The EU

Within the EU there is no specific legislation in the domain name sphere. The country code top-level domains (ccTLDs) of the various Member States' national legislation have not been harmonised by the EU. All countries regulate domain name issues in accordance with their national laws (mostly trademark laws).

This indicates that the national laws of each Member State and the specific rules or terms of use, that the administrator of each ccTLD has established, serve as the legal foundation for the specific legislative measures, namely the *suspension*, *transfer*, or *deletion* of domain name

---

[53] Anticybersquatting Consumer Protection Act, Pub. L. No. 106-113, 113 Stat. 1536, 1501A-545 (1999), accessed 30 October 2022, https://www.govinfo.gov/content/pkg/PLAW-106publ113/html/PLAW-106publ113.htm

[54] *Ibid.*

[55] Shaffer v. Heitner, 433 U.S. 186 (1977), accessed 30 October 2022. https://supreme.justia.com/cases/federal/us/433/186/

[56] Wang, *supra note,* 51.

registrations that are suspected of violating the IPR of a third party. Although the three analysed legislative measures are available in most Member States, but none of them is available in all Member States. [57]

As an illustration, in some Member States it might be conceivable to get a court order that transfers infringing domain names from their owner to the proprietor of the rights. Even if the parties involved are the same, this will not be possible in other Member States which caused uncertainty in the legal regulation of domain name disputes within the EU.

Let's have a closer look at the legal framework in the domain name sphere in one of the EU Member states.

For example, in Lithuania, the main acts which could be used indirectly to protect against unauthorised use of domain names are considered to be the Civil Code, the Law on Competition and the Law on Trademarks.[58]

In the case, UAB "Baldų centras" v. UAB "Neiseris" the Supreme Court of Lithuania emphasized that having regard to the fact that there is no law regulating the legal protection against unauthorized and fraudulent use of a legal person's name as a domain name, the court uses the analogy of law. [59]

Ukraine

In Ukraine, there is only one ruling in the legislation covering domain name disputes. Article 20 (1) of the Law of Ukraine "On Protection of Rights to Marks for Goods and Services" outlines that: "The use of trademarks and signs specified in Article 16(5) of this Law in domain names without the certificate holder consent is also considered to be the infringement of the rights." [60]

As we can see, this law also covers only a violation related to the illegal use of a trademark in a domain name and accordingly does not take into account the interests of the owner of the legitimate owner of the domain name.

To sum up, we can see a lot of loopholes in the legislation of different counties with regard to domain names. Due to this legal uncertainty, there might be cases when there are no direct legal rules that define domain names' legal status, their possible violations, disputes over

[57]Sebastian Schwemer, et al., "Study on legislative measures related to online IPR infringements," European Union Intellectual Property Office, 2018, https://data.europa.eu/doi/10.2814/819909
[58] Vilnius Regional Court, Civil Division, Case No. 2-1061-623/2008. 1 October 2008.
[59] Lithuanian Supreme Court's Civil Division, Case No. 3K-3-272/2009, 22 June 2009.
[60] Law of Ukraine "On Protection of Rights to Marks for Goods and Services", *supra note,* 15.

domain names, and most importantly the legal protection against unauthorised use of domain names and possible means of protection.

In order to reduce the number of such cases, it is fair to agree with the opinion of A. O. Hordeyuk about the expediency of adopting a special law, to single out a separate object of intellectual property rights - a domain, establish its legal regime, the status of the domain name owner, and ensure effective protection of their rights and interests.[61]

Moreover, the legislation all around the world shall be consistent as clashes between domain names may arise in different jurisdictions. That is why having a harmonised, unambiguous, universal regulation can prevent potential conflicts and provide more clarity to the parties of the dispute. Changes will help to reflect domain name specifics as a separate object of intellectual property rights as well as cover new types of domain name disputes so that such activities do not go unpunished.

Nowadays, in order to cover domain name disputes internationally, if such a trans-border infringement occurs, the person can use the Uniform Domain Name Dispute Resolution Policy (UDRP) adopted in 1999 by ICANN. In Ukraine UA-UDRP (based on UDRP) policy establishes the legal framework for the disputes arising out of .UA domain. UDRP is not a Law by nature, however, it is used as s a standard and uniform Policy across the world, unlike domestic laws that can vary across jurisdictions. The UDRP procedure will be addressed in detail in Chapter V of this thesis.

[61]Гордеюк А. О. “Проблема вдосконалення правового регулювання веб-сайтів і доменних імен в умовах інформатизації суспільства.” *Гуманітарний часопис* - № 2 (2019): 79. http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=gumc_2019_2_10

II. THE NATURE OF DOMAIN NAME DISPUTES

We all define ourselves by our names, nationalities, and addresses to be recognisable in the world. The name of the person is a very important identification tool as well as the domain name is very significant for its owner in order to stand out in the Internet space.

Taking into account the fact that each domain name is unique and two same domain names can not coexist on the Internet, the value of each increases separately, especially domain names that are simple, popular or denote a specific company, product, or service.

1. Causes of domain name disputes

Due to the growing popularity of the Internet, businesses have realised that having a domain name that matches their company name or the name of one of their products can be a valuable aspect of establishing an online presence. In order to do so, a company wishing to acquire a domain name must file an application with the appropriate agency, while doing an advanced search to see if their desired domain name is already taken.

In case the domain name corresponding to their corporate name or product trademark is owned by someone else, the company can either choose a different name or fight to get the domain name back from its current owners.[62]

It is important to mention that according to WIPO, the recent increase in the number of domain name dispute cases was caused due to fact that "the greater number of people spending more time online, especially during the COVID-19 pandemic, with trademark owners reinforcing their online presence to offer authentic content and trusted sales to Internet users". As much of the world has been working from home, businesses and consumers are relying heavily on the Internet and related IT resources – whether to engage in their "day jobs", to shop online, or to inform themselves on staying safe in the current pandemic. [63]

At the same time, the number of domain name registrations highly increased. WIPO comments that "these may be used for news/information sites, or even to provide new business offerings, but much like social media platforms, new domain names were also being used to spread misinformation and to engage in illegal and fraudulent activities".[64]

Accordingly, as websites have become very important communication and commerce tools, and the domain name itself has become a valuable intellectual property asset the number

---

[62] Bitlaw, *supra note,* 3.
[63] WIPO "WIPO cybersquatting case filing surges during COVID-19 crisis," 3 June 2020, accessed 01 November 2022, https://www.wipo.int/amc/en/news/2020/cybersquatting_covid19.html
[64] *Ibid.*

of disputes has dramatically increased over the years hence the need for brand owners to take action against villainous domain registrants through the various dispute procedures that are available.

Nowadays, in order to successfully establish a domain names dispute, the Complainant is required to satisfy the criteria laid down in the various dispute resolution policies outlined in detail in the next Chapter of this thesis.

However, it is important to answer the following question first: *when do disputes concerning domain names tend to arise?*

The domain name holder bears full legal responsibility for how the domain is used. The holder is free to decide whether the domain will be offering services, and, if so, which services the domain will offer.[65]

Mainly, domain name disputes may arise when there is infringing, conflicting and/or unauthorised use of a domain name on part of an individual.[66]

Conflicts between domain names and trademarks typically involve the use of the goodwill of a trademark by an infringer in a domain name to divert the potential customers of the owner of the trademark to a website unaffiliated with the trademark, the use of meta-tags to dilute the trademark, or the unauthorised registration of the trademark as a domain name to extort money or prevent the owner from using the trademark.

Registered trademarks, as we can understand from the previous Chapter of this thesis, are also protected online, i.e. also in the domain name sphere. Therefore, even where a trademark owner has not registered a related domain, the trademark is still protected.[67]

Domain names typically become involved in two types of conflicts:

1. conflicts where the domain name itself is at the crux of the dispute, and
2. conflicts where the domain name is involved because it leads to disputed content, such as attempted fraud.

The last types of conflicts tend to end up as criminal cases, where the prosecuting authority is looking to shut down a certain type of content or service. Sometimes other parties – public or private – want to shut down the disputed content of a website.[68] However, these types of activities won't be covered in detail in this master thesis.

---

[65] "Domain conflicts in the legal system," Norid AS. 28 October 2020, last update 21 March 2022, accessed 01 November 2022, https://www.norid.no/en/om-domenenavn/veiledere/domenekonflikter-i-rettssystemet/

[66] Singh, *supra note*, 5.

[67] EU policy. CENTR. https://www.centr.org/policy/eu-policy.html

[68] "Domain conflicts in the legal system," *op. cit.*

It should be noted that the resolution of conflicts arising from the use of a domain name is one of the most problematic in the system of Internet legal relations. This is due to objective factors, in particular:

- the supranational nature of the Internet (in the procedural aspect, this circumstance may affect the jurisdiction of a domain dispute);
- technical features of the Internet (speed of data exchange, changes in the information content of websites, which creates risks of loss of the evidence base);
- the special nature of its regulation ("self-regulation")[69].

2. Types of domain name dispute

Domain names also play a central role in a number of IP-infringing online business models that were identified in research by the EUIPO Domain name Discussion paper.[70]

According to the research, these business models can be divided into two main categories:

I. Business models where IP is misused in the domain name:

IPR-infringing business models differ from the non-infringing business models in the way that they are often deceptive to the customers and it can be observed that certain specific online IPR-infringing business models have been developed to benefit from IPR-infringing activities. Examples of that are misuse of the domain name system through cybersquatting and other related activities described below.

A. Cybersquatting

Cybersquatting also referred to as domain "squatting" is one of the most common scenarios in domain disputes. [71]

Cybersquatting is a practice in which a person registers a domain name that resembles a well-known brand without authorisation to gain some profit. Domain registrants buy the domain name with a mala fide (a bad or wrong) intention that harms the goodwill and reputation of the company. A common motive for cybersquatting is the intention to sell the domain name back to the trademark owner or to attract web traffic to unrelated commercial offers. Sometimes a

[69] Кудрицька, *supra note, 2.*
[70] Domain names Discussion Paper, *supra note*, 29.
[71] Medha Mehta, "10 interesting cybersquatting examples to learn from," InfoSec Insights. 19 February 2021. https://sectigostore.com/blog/cybersquatting-examples/

person registers the name and expects that he will sell the domain name in the future to the highest bid.[72]

Cybersquatting primarily refers to the registration and use of a domain name that is identical or confusingly similar to a third party's trademark, in bad faith and with the intention to benefit from the registration and usage.

While doing that cybersquatters exploit the first-come, first-served nature of the domain name registration system to register as domain names, third parties' trademarks or business names or names of famous people, as well as variations thereof. This practice of cybersquatting creates disputes between trademark owners and domain name registrants, which present features stretching the capacity of the ordinary judicial system.[73]

As for now, Facebook, Apple, Google, TikTok, Walmart, Bank of America, PayPal, and other huge brands have become victims of cybersquatting.

Let's have a look at one of the typical cybersquatting cases.

TikTok Case

In Case № D2020-2439 Bytedance Ltd. v. Registration Private, Domains By Proxy, LLC/Fotios Tsiouklas, Kickspan all five domains in question <growtiktok.com>, <tiktokcharts.com>, <tiktokexposure.com>, <tiktokplanet.com>, and <tiktoks.com> were transferred to the Complainant.[74]

The Respondent presumed that the TikTok app would become a very popular brand, so just after TikTok's launch, they decided to buy a domain <tiktoks.com> for only 2000 USD. TikTok's owner, Bytedance, offered 145,000 USD to buy that domain. However, they rejected the offer and kept the domain while starting to grow a business, offering a "follow-for-follow" service and helping people to increase their followers by charging a fee in order to gain profit from the registration and use of disputed domains. Following this illegal activity, Bytedance filed a winning cybersquatting case against abusive registration and the disputed domain names were transferred to the Complainant.

---

[72]Sharad Yadav, "Domain name disputes in Cyberspace," iPleaders, 14 July 2021. https://blog.ipleaders.in/domain-name-disputes-cyberspace/

[73] Guide to WIPO Domain Name Dispute Resolution. WIPO Publication No. 892(E), ISBN: 92-805-1426-1, https://www.wipo.int/export/sites/www/amc/en/docs/guide-en-web.pdf

[74] Bytedance Ltd. v. Registration Private, Domains By Proxy, LLC / Fotios Tsiouklas, Kickspan Case № D2020-2439. WIPO Arbitration and Mediation Center, 13 January 2021, https://www.wipo.int/amc/en/domains/decisions/text/2020/d2020-2439.html

a) Typosquatting

Have you ever typed Facebok.com, Facbook.com or Faceboo.com instead of Facebook.com? If you are not an eagle-eyed person, you most likely made such a mistake. While typing a domain name wrongly, you probably will be redirected back to the site you wanted to reach in the first place. However, it might be the case, that you will discover a "fake" website behind big brands' backs while their domain names are used in a confusingly similar manner.

This kind of infringement is a variation of cybersquatting named typosquatting where a registrant acquires misspellings of other's domain names with the intention of catching and exploiting the traffic that was intended for the genuine websites. A typosquatter refers to a person who registers a domain name with common typos of the company's primary domain name to shift the traffic from the main website to its website. This practice is also known as "URL hijacking" or sometimes "web address hacking." A person takes advantage of common typing mistakes which people make while entering any URL.[75]

Let's use the domain www.mruni.eu as an example.

Some common types of typosquatting include:[76]

- The omission of the "." in the domain name: wwwmruni.eu;
- A common misspelling of the intended site: www.mryni.eu;
- Adding letters to the domain name, either for a typo or an errant keystroke: www.mruuni.eu
- Inserting numbers or symbols instead of letters: www.mrun1.eu;
- A different top-level domain: www.mruni.edu
- Adding a generic or descriptive term to a registered trademark: www.mruniuni.eu

The relevant cases of typosquatting where the domain name was transferred to the Complainant are:

- SIEMENS AG v. Omur Topkan, WIPO Case №D2013-1318[77] - where the "sıemens" (in Turkish) was found as a confusingly similar to the Complainant's trademark "Siemens"

[75] Schwemer, *supra note*, 57.

[76] Pratibha Ahirwar, "Domain name disputes and cybersquatting in India," 22 February 2019, https://www.mondaq.com/india/trademark/783958/domain-name-disputes-and-cybersquatting-in-india-part-i

[77] SIEMENS AG v. Omur Topkan, Case №D2013-1318, WIPO Arbitration and Mediation Center 30 September 2013, https://www.wipo.int/amc/en/domains/search/text.jsp?case=D2013-1318

as it is phonetically and visually almost identical (See an identical case is Twitter, Inc. v. Ahmet Ozkan, WIPO Case №D2014-0469[78]);

- LinkedIn Corporation v. Daphne Reynolds, WIPO Case №D2015-1679, “linkedlnjobs.com” - adding a generic or descriptive term to a registered trademark does not prevent the domain name from being confusingly similar to that registered trademark[79];
- Humana Inc. v. Cayman Trademark Trust, WIPO Case №D2006-0073[80], “humanna.com” compare to trademark “Humana” - repeated consonant does not significantly affect the appearance or pronunciation of the domain name;
- PartyGaming Plc., PartyGaming IA Limited v. Harry Thomas, WIPO Case №D2008-1275 (disputed domain name <gamebukers.com> confusingly similar to “GAMEBOOKERS” mark for phonetic reasons (transfer denied on other grounds).[81]
- At the same time, in the Chanel, Inc. v. Sandy Goldman Case № D2000-1837 the Chanel's “ishopchannel.com” and “ishopchannel.net” domain name redelegation claims were denied on the grounds that Respondent had the right and legitimate interest to use those domain names. Though the domain names were found confusingly similar to the Complainant's mark, the use of the word "channel" (as compared to the CHANEL trademark) was not considered as typosquatting, since the Respondent used the site for its lawful activities, and the typo was made intentionally - the Respondent's marketing ploy.[82]

b) Soundsquatting

Soundsquatting - a new unexplored area in domain name disputes. Soundsquatting takes advantage of the sound similarity of words and the user’s confusion about which word represents the desired concept.

---

[78]Twitter, Inc. v. Ahmet Ozkan, Case №D2014-0469Humana Inc. v. Cayman Trademark Trust Case No. D2006-0073, WIPO Arbitration and Mediation Center 15 June 2014, https://www.wipo.int/amc/en/domains/search/text.jsp?case=D2014-0469

[79]LinkedIn Corporation v. Daphne Reynolds, Case №D2015-1679, WIPO Arbitration and Mediation Center 16 November 2015, https://www.wipo.int/amc/en/domains/search/text.jsp?case=D2015-1679

[80]Humana Inc. v. Cayman Trademark Trust, Case №D2006-0073, WIPO Arbitration and Mediation Center 7 March 2006, https://www.wipo.int/amc/en/domains/decisions/html/2006/d2006-0073.html

[81]PartyGaming Plc., PartyGaming IA Limited v. Harry Thomas, Case №D2008-1275, WIPO Arbitration and Mediation Center 14 November 2008, https://www.wipo.int/amc/en/domains/decisions/html/2008/d2008-1275.html

[82]Chanel, Inc. v. Sandy Goldman Case № D2000-1837, WIPO Arbitration and Mediation Center 13 February 2001, https://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-1837.html

The first grounded research in this sphere was done by Nick Nikiforakis, Marco Balduzzi, Lieven Desmet, Frank Piessens and Wouter Joosen Soundsquatting who discovered that Soundsquatting is different from Typosquatting as it does not rely on typing mistakes and in that not all domains contain homophones and thus, not all domains can be soundsquatted.[83]

The attack is based on homophones, i.e., sets of words pronounced the same but spelled differently, e.g., {ate, eight} or {weather and whether}. Attackers can register homophone variants of popular domains, such as 4ever21[.]com for forever21[.]com.

As text-to-speech software like Siri and Google Assistant becomes prevalent, more and more users will become vulnerable to the abuse of soundsquatting domains.[84]

c) Levelsquatting

a challenging issue for the international community became the use of subdomains to 'hide' infringing content, which is an emerging trend for websites selling counterfeits according to the Domain name Discussion paper.[85]

If the domain itself (e.g. ivanka.com) does not have any content and appears to be offline, counterfeits are sold through pages appearing on a subdomain (e.g. subdomain.ivanka.com). These subdomains are promoted and communicated directly to users through multiple channels, including social media. This makes it more difficult to check and establish if a specific domain is used for IP-infringing activities. Several researchers discovered the phenomenon of levelsquatting and how it exploits the visual vulnerabilities of browsers to defraud web users.[86]

"Infringing subdomain" takes advantage of a brand and is used in an abusive way, or one that does not itself take advantage of the brand, eg, a generic subdomain, but which is used in a brand-abusive way. Legal remedies available to address infringing subdomains are limited relative to those available at the parent level (second-level domain).

---

[83]Nikiforakis, N., Balduzzi, M., Desmet, L., Piessens, F., and Joosen, W.,"Soundsquatting: Uncovering the Use of Homophones in Domain Squatting." In: Chow, S.S.M., Camenisch, J., Hui, L.C.K., Yiu, S.M. (eds) Information Security. Part of the Lecture Notes in Computer Science, vol 8783. Springer, Cham, 2014, https://doi.org/10.1007/978-3-319-13257-0_17

[84]Zhanhao Chen and Janos Szurdi, "Cybersquatting: Attackers Mimicking Domains of Major Brands Including Facebook, Apple, Amazon and Netflix to Scam Consumers," 1 September 2020, https://unit42.paloaltonetworks.com/cybersquatting/

[85] Domain names Discussion Paper, *supra note,* 29: 10.

[86]Kun Du, Hao Yang, Zhou Li, Haixin Duan, Shuang Hao, Baojun Liu, Yuxiao Ye, Mingxuan Liu, Xiaodong Su, Guang Liu, Zhifeng Geng, Zaifeng Zhang, and Jinjin Liang - DR Hazard, "A Comprehensive Study of Levelsquatting Scams," 2019, https://cpb-us-e2.wpmucdn.com/faculty.sites.uci.edu/dist/5/764/files/2019/07/securecomm19.pdf

Unfortunately, policies like the UDRP do not apply to subdomains, given the policy's references to the domain being registered with a registrar, thus it will not assist where the parent is not confusingly similar to the trade mark.[87]

For example, in the EFG Bank European Financial Group SA v. Domain Consults Case №D2011-1907 [88] only one disputed domain "uk-efgc.com" was transferred to the Complainant. It was outlined that since there is no evidence of record that other disputed subdomains "de.uk-efgc.com" and "es.uk-efgc.com" are as such registered with a registrar, via an applicable registration agreement which inter alia incorporates the Policy as an appropriate administrative dispute resolution mechanism, the Panel is not able to order that a subdomain be transferred.

Unfortunately, this approach opens doors for the unlimited abusive use of subdomains and only court litigation can be applied in these situations.

B. Passing Off Domain Name

Cases of passing off are distinct from cybersquatting. It occurs when a business registers a domain name that resembles the trade name or product name of a competitor. By doing so, the attackers are willing to unfairly benefit from a competitor's branding or marketing activities without intending to sell the domain name back to the trademark owner (as in the case of cybersquatting).

Registered under abusive domain name websites can be considered competitor's one and users might think that illegally registered site has the same owner. Accordingly, attackers build such websites on someone else's good reputation. Another similar form of dispute may arise where a company uses metatags or pays for sponsored ads which incorporate the competitor's branding.[89]

In the leading case - BT v One in a Million (1999)[90] - the court decided that defendant's registration of domain names constituted passing off and trade mark infringement. In this case, the defendants registered a number of domains incorporating the brand names of well-known

---

[87] Jeremy Speres, "Subdomains and online brand protection: What you need to know. World Trademark Review," 01 October 2020, https://www.worldtrademarkreview.com/article/subdomains-and-online-brand-protection-what-you-need-know-long-read

[88] EFG Bank European Financial Group SA v. Domain Consults Case № D2011-1907, WIPO Arbitration and Mediation Center 23 December 2011, https://www.wipo.int/amc/en/domains/search/text.jsp?case=D2015-1679

[89] Simon Halberstam, "Key Issues in Domain Name Law," Weblaw, 29 January 2019, accessed 17 November 2022, https://www.weblaw.co.uk/domain-name-disputes/domain-name-key-issues/

[90] British Telecommunications Plc v One in A Million Ltd, 1 WLR 903 - English Court of Appeal, 1999. https://app.justis.com/case/british-telecommunications-plc-v-one-in-a-million-ltd/overview/c4yZmXqdm5Wca

companies (such as Marks & Spencer, BT, Virgin). For example, anybody who sees or hears Marks & Spencer name connects it with the business of Marks & Spencer plc.

The judge concluded that if a person searches for "marksandspencer.co.uk", and sees the name One in a Million Ltd, could clearly create a false representation constituting the "instruments of fraud".

C. Reverse domain name hijacking (RDNH)

In contrast to cybersquatting, reverse domain name hijacking is an attempt by a trademark owner in bad faith to take control of a domain name from a third party with a legitimate interest in the name.

RDNH is mostly enacted by large corporations and individuals, in defence of their rightful trademark or for preventing libel or slander.[91]

According to Rule 15 (e) of the Uniform Domain-Name Disputes Resolution Policy, "when the complaint was brought in bad primarily to harass the domain-name holder, then the Panel shall declare in its decision that the complaint was brought in bad faith and constitutes an abuse of the administrative proceeding."[92]

The first decision under the UDRP where RDNH was declared was Qtrade Canada Inc. vs. Bank of Hydrov, Case №AF-0169 on June 19, 2000. The disputed domain name was <Qtrade.com>. The Panelist concluded that RDNH existed because the Complainant initiated proceedings "after unsuccessfully initiating attempts, directly and/or indirectly, to encourage the Respondent to sell the domain name for almost one year" and because of the Complainant's "over-statement" of the status of its trademark rights when it only had a pending application for a trademark. The Panelist remarked that "if this case does not rise to the level of bad faith and reverse domain name hijacking, it is difficult to imagine a set of facts and circumstances that would".[93]

The problematic aspects of RDNH are that in some of the cases bad faith might be clear, such as where the complainant's behaviour is plainly malicious and the claim is brought without

---

[91]Warren B. Chik, "Lord of Your Domain, But Master of None: The Need to Harmonize and Recalibrate the Domain Name Regime of Ownership and Control," *International Journal of Law and Information Technology*, Volume 16, Issue 1, 8–72, (Spring 2008), https://doi.org/10.1093/ijlit/eam005

[92]Rules for Uniform Domain Name Dispute Resolution Policy approved by ICANN on 24 October 1999, accessed 02 November 2022, https://www.icann.org/resources/pages/udrp-rules-2015-03-11-en

[93]Qtrade Canada Inc. vs. Bank of Hydrov, Case №AF-0169, WIPO Arbitration and Mediation Center, 19 June 2000, http://www.disputes.org/decisions/0169.htm

any basis as was outlined in Smart Design LLC v Carolyn Hughes, (2000) WIPO Case №D2000-0993.[94]

However, while the UDRP lists factors illustrative of bad faith on the part of a registrant to assist in identifying bad faith on their part, no such factors are listed as indicating bad faith on the part of the complainant in the RDNH context.[95]

In order to overcome this issue, WIPO concluded the circumstances cited by panels as justification for reverse domain name hijacking:

- To establish Reverse Domain Name Hijacking, there must be evidence of knowledge on the part of the complainant of the respondent's right or legitimate interest in the disputed domain name and evidence of harassment or similar conduct by the complainant in the face of such knowledge (see Sydney Opera House Trust v. Trilynx Pty. Limited, WIPO Case №D2000-1224[96]);
- bad faith in this context is bringing a claim despite actual knowledge of a legitimate right or lack of bad faith on the part of the registrant, or where it should have been obvious that the complaint had no real prospect of success (see Smart Design LLC v Carolyn Hughes, (2000) WIPO Case №D2000-0993);
- RDNH was also more commonly meted out against Complainant's whose trademark rights clearly post-date the disputed domain name registration, such as in Canon City Property Management, LLC v. David Borden, NAF Claim Number: FA2203001987569 as of May 4, 2022 [97]

However, still there are a lot of cases involving RDNH arrises. Nonetheless, each RDNH determination also serves as a reminder that the UDRP has its drawbacks and in its present form encourages attempted hijackings and that an RDNH determination is an entirely insufficient deterrent to attackers. Each attempted hijacking is an attack on a legitimate domain name registrant, who is forced to face an expensive, time-consuming, and stressful defence of the domain name though being to claim damages caused by such harm under the UDRP.

---

[94]Smart Design LLC v Carolyn Hughes Case №D2000-0993, WIPO Arbitration and Mediation Center, 18 October 2000, https://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0993.html

[95]Sourabh Ghosh, "Domain Name Disputes and Evaluation of The ICANN's Uniform Domain Name Dispute Resolution Policy", *Journal of Intellectual Property Rights* Vol 9, September 2004. http://nopr.niscpr.res.in/bitstream/123456789/4883/1/JIPR%209%285%29%20424-439.pdf

[96]Sydney Opera House Trust v. Trilynx Pty. Limited, Case №D2000-1224, WIPO Arbitration and Mediation Center 31 October 2000, https://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-1224.html

[97]Canon City Property Management, LLC v. David Borden, NAF Claim Number: FA2203001987569. 4 May 2022, https://www.adrforum.com/domaindecisions/1987569.htm

D. Cyber twin

Cyber twin disputes occur when both the domain name holder and the person contesting the domain have a legitimate claim to the domain.

While analysing domain name infringement cases, the cyber twin cases can be considered the most problematic for courts to decide because, in the absence of a domain name dispute, both parties would otherwise likely be able to enjoy concurrent use of the name under traditional trademark law.[98]

In the Indian Farmers Fertiliser Cooperation Ltd v. International Foodstuffs Co, Case № D2001-1110[99], the issue was related to the domain name "iffco.com". In this particular case, it was stated that the defendant was using the domain name in good faith. The complainant had a legitimate interest in the domain, which was related to iffco.com. Although the complainant stated that the defendant was diverting users to its own website, the Arbitration Centre dismissed the case because the complainant failed to prove that the defendant was using the domain name in bad faith, despite the fact that both parties had a legitimate interest in the domain name.

II. Business models where the domain name leads to a website supporting IP-infringing activities:

Nowadays, more and more situations arise where the domain name itself does not contain any trademark, company name, logo, copyright, or other protected name owned by the third party. However, the website's content itself may be considered intellectual property infringement. These cases are usually outside the scope of the alternative dispute resolution policy such as UDRP. The complainants are typically directed to (civil or even criminal) courts, where the content of the website is examined for infringements of the intellectual property rights of third parties.

The aforementioned kinds of infringements of IPRs frequently reach a scale where the infringements also constitute criminal offences, meaning that the penal provisions in the concerned national IPR legislation or in the penal code may apply.[100]

Examples of such abusive activities

---

[98] Brian W. Borchert, "Imminent Domain Name: The Technological Land-Grab and ICANN's Lifting of Domain Name Restrictions," *Valparaiso University Law Review*, Volume 45, Number 2, (2011), https://scholar.valpo.edu/cgi/viewcontent.cgi?article=1437&context=vulr

[99] Indian Farmers Fertiliser Cooperation Ltd v. International Foodstuffs Co, Case № D2001-1110, WIPO Arbitration and Mediation Center 4 January 2002, https://www.wipo.int/amc/en/domains/decisions/html/2001/d2001-1110.html

[100] Schwemer, *supra note*, 57*: 20.*

These kinds of IP-infringing business activities, including website marketing and/or providing links to counterfeit goods or pirated content, are 'operated through an Internet site that is controlled by the infringer which means that the infringing entity (or its proxy) is the registrant of the domain name and the content of the website is made available by the infringer. However, attackers behind the IPR-infringing activities often either conceal their identities by using privacy shield services for the registration of their domain names or provide inadequate, false or otherwise misleading contact details on the website thus hampering or even precluding enforcement actions.[101]

Another example is when an attacker establishes a new business under a different domain name but with the exact same design and content as before, immediately after the previous domain name was transferred or deleted as a result of legal action.[102]

The registration of several domains for the same site to dodge enforcement measures intended at a single domain, or the registration of the name of a prominent IP infringing website with a different domain by a new 'operator,' are also examples of abusive behaviour. These two business models can also coexist, for example, the registration of a domain name using a registered trademark to sell counterfeit products under this trademark.[103]

E. Phishing

Phishing describes malicious attempts to collect money or sensitive information or install malware by establishing contact with victims via email, social media platforms, blogs, or text messages. The inquiry will immediately appear to be sent in good faith and for a legitimate purpose: it will thus often appear to be sent by an established company since the sender address makes use of a domain name that resembles the genuine domain name of that company.[104]

An attacker will often have established a *spoofing website*, a website that is a close imitation of the official website of the impersonated company or person, which is why a visit to the website does not create any suspicion about the malicious circumstances.[105] The phishing email will typically contain a link to the attacker's website, although the site can also be accessed independently.

---

[101] "Research on Online Business Models Infringing Intellectual Property Rights," EUIPO, Phase 1, (July 2016): 10, https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/resources/Research_on_Online_Business_Models_IBM/Research_on_Online_Business_Models_IBM_ex_sum_en.pdf

[102] *Ibid.*

[103] Domain names Discussion Paper, *supra note*, 29.

[104] Schwemer, *supra note*, 57: *21.*

[105] 'Research on Online Business Models Infringing Intellectual Property Rights', *op. cit.*, 101.

As we can see IPR-infringing activities under this business model may be limited to one or include various abusive actions. Though they may be carried out on other digital platforms, but ultimately lead Internet users to the target website, either through phishing e-mails, social media websites, etc.

In such cases, the right holder may institute civil court actions against the alleged infringer and in some cases, the infringing activities may also be subject to criminal proceedings and sanctions[106] which are, though, beyond the scope of this research.

However, in most cases, the aforementioned fraudulent activities also make use of domain names that include the trademark or company name of the imitated legitimate brand owner. Accordingly, if the domain name that is used for the Internet site is itself infringing on a third-party trademark, the trademark owner may, instead of filing a court action, use the extra-judicial enforcement tools that apply to most abusive domain name registrations, either through the UDRP-procedure or through similar alternative dispute resolution procedures.

Let's take a Google Inc. UDRP decision with the disputed domain name <web-account-google.com> as an example. In this case, Google complained that Respondent engages in a phishing scheme to obtain personal information for users, as well as that the login information contained on the resolving webpage (associated with the domain name <web-account-google.com>) does not actually function, but rather Respondent uses it to obtain personal information from users.[107]

The Panel established all the criteria under the policy to consider the registration as abusive and the domain name was transferred to Google.

However, we need to take into account, that dispute resolution mechanisms such as UDRP might be limited and inappropriate to take down a website when it is impossible to prove that the domain name itself is used as an infringement tool.

For example in Zimmermann Wear Pty Ltd v. Sam Dumond Case[108], the Respondent was conducting obvious infringing activities on the website under the disputed domain name. The website was made to look like the clothing company and is allegedly shipping counterfeit goods when someone orders. However, Zimmermann and Zim were not considered by the Panel

---

[106] 'Research on Online Business Models Infringing Intellectual Property Rights', *op. cit.,* 101.

[107] Google Inc. v. 1&1 Internet Limited, Claim Number: FA1708001742725, FORUM, 31 August 2017, https://www.adrforum.com/domaindecisions/1742725.htm

[108] Zimmermann Wear Pty Ltd v. Sam Dumond, FORUM, 17 September 2018, https://www.adrforum.com/domaindecisions/1802176.htm

in this case as confusingly similar. Accordingly, the Panel declines to reach other criteria such as rights or legitimate interests and registration and use in bad faith.

Unfortunately, it is impossible to deal with such cases using UDRP only which should always be considered part of a broader dispute resolution process to address all the problematic aspects. This process may involve sending a cease and desist letter to the website, contacting the hosting company and the domain name registrar, reporting the fraud to the police or adding warning notices to the business' legitimate website, asking search engines to de-index the website and, if all else fails, seeking a blocking injunction against the website.[109]

To sum up, it is evident that domain name disputes of all types continue to occur in large numbers. As a result of the pandemic a lot of businesses "migrated" online, and the number of disputes significantly increased during the last few years. This may also be partially explained by the introduction of numerous new generic top-level domains and the ongoing development of the IT industry.

Numerous IP infringing activities, including the sale of counterfeit goods under the contested domain name and phishing, are regarded as typical cybercriminal activities, and alternate domain name dispute resolution procedures are not viable tools to deal with such situations. There are also a lot of new types of infringements such as soundsquatting and levelsquatting, etc. which arise and become a "grey zone" for legislators as there are no rules or case laws covering these issues properly. That's why it is important for the ICANN to initiate an academic discussion in order to develop a mechanism and sort of guideline for the Panelists on how to face such cases effectively and fairly in the future.

As we can see, potential attackers are constantly exploiting the weakness of the domain name regulation and inventing new attack vectors. That is why there is a need to continue further research concerning domain name abuse in order to improve the legal regulation of domain name disputes by focusing on the latest trends.

[109] "Domain names, online fraud and UDRP proceedings," 11 December 2020, accessed 02 November 2022, https://www.allenovery.com/en-gb/global/blogs/digital-hub/domain-names-online-fraud-and-udrp-proceedings

III. DOMAIN NAME DISPUTES POLICIES

In order to prevent a domain name dispute in the first place, proactive measures, such as registering some of the most common typos or the .com and .org of your domain name, are a good start to policing your domain name. However, it is impossible for businesses to register each and every possible infringing domain. Infringement can still take place due to the high speed of Internet development and the invention of new attack vectors as described in the previous Chapter.

Due to that, the affected party needs to know the applicable Policies to deal with problematic aspects arising in the domain name field.

As was mentioned before, in the early days of the Internet domain name system, there was little to no regulation specifically to address disputes that rapidly arose in the domain name sphere, especially between trademark holders and domain name registrants. Accordingly, the trademark law was used as the main legislative framework for resolving these issues due to the lack of clear regulatory principles to deal with possible infringement scenarios.

In case a person became involved in one of the types of domain name disputes, there is a need to know how to protect legitimate interests and resolve the disputed situation in the most efficient way.

So what are the possible domain name dispute resolution mechanisms?

Nowadays, you can resolve this issue in the following ways:

- complaint under the Uniform Domain Name Dispute Resolution Policy (UDRP) and related to its policies (e.g. such as UA-UDRP in Ukraine);
- court action, or
- agreement/mediation process (which is rarely used).

1. UDRP

A. General overview

The Uniform Domain Name Dispute Resolution Policy (UDRP) is a method of resolving domain name disputes out of court. The disagreement will be settled outside any judicial body and involves an administrative procedure.[110]

[110] Sara María Ballester Climent and Begoña Payá Todolí, *supra note, 4: 13.*

Since 1999 and as of today, the UDRP procedure is the most efficient regulation instrument for resolving domain name disputes, under which the WIPO Center has processed over 57,000 cases.[111]

Adopted by the ICANN in 1999 the UDRP sets the legal framework for the resolution of disputes between a domain name registrant and a third party (i.e., a party other than the registrar) regarding the abusive registration and use of an Internet domain name in the generic top-level domains or gTLDs (e.g., .biz, .com, .info, .mobi, .name, .net, .org), and those country code top-level domains or ccTLDs that have adopted the UDRP Policy on a voluntary basis.[112] Regarding domain name disputes, the UDRP policy provides arbitration as opposed to litigation.

ICANN also adopted the UDRP Rules[113] which outline the procedures and other requirements for each phase of the administrative and dispute resolution procedure.

The dispute resolution procedure is administered by service providers accredited by ICANN. Currently, there are six approved dispute resolution providers to which complaints can be addressed under the UDRP: World Intellectual Property Organization (WIPO), Asian Domain Name Dispute Resolution Centre (ADNCRC), National Arbitration Forum (NAF), Canadian International Internet Dispute Resolution Centre (CIIDRC), Arab Center for Dispute Resolution (ACDR) and Czech Arbitration Court (CAC). Among them, WIPO has been the most popular domain name dispute resolution platform.[114]

Mainly, the adoption of UDRP had three main objectives:

- to eliminate the jurisdiction and conflict of law problems related to all internet disputes;
- to reduce the cost of bringing suits against the attackers;
- to provide a time-effective mechanism applied instead of traditional litigation.

A UDRP Proceeding is a private, binding arbitration proceeding. The arbitration is overseen by either one arbitrator or a panel of three impartial arbitrators and differs from a lawsuit because it involves less evidentiary processes and is a much quicker process. Also, arbitration is typically not appealable, however, UDRP Proceedings can be appealed via a lawsuit only.[115]

---

[111] "Domain Name Dispute Resolution," WIPO - ADR, https://www.wipo.int/amc/en/domains/

[112]"WIPO Guide to the Uniform Domain Name Dispute Resolution Policy (UDRP)" WIPO, https://www.wipo.int/amc/en/domains/guide/#a3

[113] Rules, *supra note*, 92.

[114]List of Approved Dispute Resolution Service Providers, ICANN, https://www.icann.org/resources/pages/providers-6d-2012-02-25-en

[115] Eric Perrott and Sophie Edbrooke, "Domain Name and UDRP Disputes – a Definitive Guide," *Gerben Intellectual Property* 7 November 2022, https://www.gerbenlaw.com/blog/the-definitive-guide-to-udrp-proceedings-and-domain-disputes/

So what are the main *advantages* of UDRP Vs traditional court dispute resolution?

Time-efficiency

A UDRP Proceeding is much faster than a federal court case, which may take years. Depending on the forum you file in and the number of filings by each party, a proceeding can be completed as quickly as six weeks to two months from filing to transfer. As a rule, no more than 60 days pass from the moment the application is submitted to the arbitration centre until the decision is made and the domain is transferred to the rightful owner.[116]

Cost-efficiency

Due to the private nature of a UDRP proceeding, the trademark owner is responsible for paying the arbitration fees. These fees could seem expensive depending on how many arbitrators will review the case (by the Complainant's choice), the forum in which will arbitrate the case, and how many domain names are claimed. For example, for a case filed with the WIPO Center involving between 1 and 5 domain names that are to be decided by a single Panelist, the fee is 1500 USD. For a case that is to be decided by 3 Panelists, the fee is 4000 USD, etc.[117]

To compare, this amount is much lower than a court proceeding, which includes the costs of a court and lawyer fee, etc.

Internationality

UDRP provides a single mechanism for resolving domain name disputes, independent of the location of the registrar, domain name holder, or complainant. Even if you possess the rights to a trademark in Ukraine and the infringer is, for instance, in Lithuania, you can apply to the relevant centre and acquire a ruling that is pertinent to your case. It facilitates the resolution of challenging circumstances involving the participation of parties in a foreign court and the execution of its decision.

Automatic execution

The UDRP system provides automatic execution of a remedy for successful complainants by ensuring that every contract between ICANN and an accredited domain name registrar contains a provision under which the registrar agrees to transfer to a successful complainant the domain name which is the subject of the arbitration under the UDRP. [118]

---

[116] Perrott and Edbrooke, *supra note*, 115.

[117] Schedule of Fees under the UDRP, WIPO (valid as of 1 December 2002), https://www.wipo.int/amc/en/domains/fees/index.html

[118] Registrar Transfer Dispute Resolution Policy. ICANN. https://www.icann.org/resources/pages/tdrp-2016-06-01-en

Online hearing

Paragraph 13 of the UDRP Rules[119] outlines that there shall be no in-person hearings (including hearings by teleconference, videoconference, and web conference), unless the Administrative Panel determines, only as an exceptional matter, that a hearing is necessary in order for it to make its decision.

A complaint can include more than one domain name

Under Paragraph 3(c) of the UDRP Rules, the Complaint may relate to more than one domain name, so long as the person or entity that is the registrant of the domain names specified in the Complaint is the same.[120]

B. UDRP: Procedural aspects

At the time of filing, the Complainant may choose between the *transfer* of the domain name from the Respondent to the Complainant and the *cancellation* of the domain registration (in case the Complainant has no interest in the domain). However, the disadvantage of the latest is that the Complainant must monitor the domain name when it becomes available to any other party trying to register it, which could result in recurrent infringement.

According to Paragraph 4(a) of the UDRP Policy[121], the UDRP Administrative Procedure is only applicable for disputes involving the alleged abusive registration of a domain name if the following criteria are met:

1. **First criteria -** the domain name registered by the domain name registrant is identical or confusingly similar to a trademark (either registered or unregistered) or service mark in which the complainant (the person or entity bringing the complaint) has rights;
2. **Second criteria** - the domain name registrant has no rights or legitimate interests in respect of the domain name in question;
3. **Third criteria -** the domain name has been registered and is being used in bad faith.

The Complainant must prove *all three requirements* in the administrative procedure; otherwise, the administrative panel will neither cancel nor transfer the domain name.

That is why it is important to describe in detail all three criteria as the panel may face different challenges in their establishment in each case, which causes uncertainty for the parties and Panellists while resolving such disputes.

---

[119] Rules, *supra note*, 92.
[120] *Ibid.*
[121] Uniform Domain Name Dispute Resolution Policy, Approved by ICANN on 24 October 1999, http://icann.org/udrp/udrp-policy-24oct99.htm

First criteria

The First criteria that the registered domain name is identical or confusingly similar to a trademark or service mark is considered the easiest one to establish during the dispute resolution procedure.

It is generally accepted that the first part serves primarily as a standing requirement. The standing test for confusing similarity involves a reasoned but relatively straightforward comparison of the complainant's trademark and the disputed domain name. The Complainant basically must demonstrate that it has rights in a trademark, and, if so, to show that the registered domain name contains all or part of its registered mark so is identical or confusingly similar.[122]

In accordance with the WIPO Overview, Panels consider the first element as a threshold test concerning a trademark owner's standing to file a UDRP complaint, i.e., to determine if there is a sufficient linkage to evaluate the concepts embodied in the second and third parts.

Let's consider the LEGO Juris A/S v. Legoverhuur.nl, Frank Schuermans Case No. D2011-155[123] as an easy example, where the Respondent registered a disputed domain name <legoverhuur.com>.

The Panel considered the word LEGO as the most distinctive element of the disputed domain name while determining that this is also an extremely well-known and renowned trademark. It was outlined in this case that the addition of the descriptive word "ver huur" (which means from Dutch "for hire") does not eliminate the possibility of confusion with the LEGO trademark. In fact, the Panel concluded that it strengthened the association.

As we can see, in general, Panels have determined that the UDRP's threshold test for confusing similarity involves a direct comparison of the trademark and the alphanumeric string of the disputed domain name to determine the likelihood of Internet user confusion.

Though it looks easy, however, in some cases the establishment of the first criteria also might be challenging and ambiguous.

We may note that there is no consistent approach among UDRP decisions about the requirement to consider the domain name's meaning or its component in order to show confusing similarity.

---

[122]WIPO Overview of WIPO Panel Views on Selected UDRP Questions, 2017. https://www.wipo.int/amc/en/domains/search/overview3.0/

[123]LEGO Juris A/S v. Legoverhuur.nl, Frank Schuermans, Case No. D2011-1559, WIPO Arbitration and Mediation Center, 13 December 2011, https://www.wipo.int/amc/en/domains/decisions/text/2011/d2011-1559.html

Christine Haight Farley in his research outlines that the determination of meaning in a UDRP case is necessarily flawed because domain names often do not have a context that may be considered.

He raises the questions, such as for example, is <ferrari.red> an easy case to establish the confusing similarity? Since the iconic Ferrari is red, perhaps as with e.g. <canyon.bike>[124] (as outlined by the Panel "especially since the word "canyon" could otherwise be understood as a generic term") a panel would find that the meaning of the gTLD enhances the confusing similarity. But this creates confusion about how meaning should be determined. In Spanish, "red" means network. Thus, it is certainly possible that Spanish speakers might assume that the domain name was associated with a site for the Ferrari enthusiast community. To reach such a conclusion, a panel would have to take into account the context of the domain name.[125]

It is also important to note that typically, the similarity test is applied without regard to website content or the applicable gTLD (though new gTLDs may impact on this) as was addressed in detail in the previous Chapter.

However, the degree of distinctiveness of the mark at issue and the extent to which the domain name at issue may contain alpha-numeric elements in addition to those of the mark may be considered. In this context, panels have also found that the overall facts and circumstances of a case (including relevant website content) may support a finding of confusing similarity, particularly where it appears that the respondent registered the domain name precisely because it believed that the domain name was confusingly similar to a mark held by the complainant.[126]

"Spanning the dots"

An unresolved question in domain name disputes is whether the UDRP would assist where the offending domain has the brand or the confusingly similar term "spanning the dots" across the parent and subdomain levels.

It is well-established under the UDRP practice that spanning the dot between the TLD and the parent can satisfy the first element.

For example, in Mr Green Ltd. v. Alfred Zeiselberger, Mediapool Communications Limited Case № D2017-1944 trademark the disputed domain name <mr.green> was considered

---

[124]Canyon Bicycles GmbH v. Domains by Proxy, WIPO Case No. D2014-0206, WIPO Arbitration and Mediation Center, 14 March 2014, https://www.wipo.int/amc/en/domains/decisions/text/2014/d2014-0206.html

[125]Christine Haight Farley, "Confusing the Similarity of Trademarks Law in Domain Name Disputes," *Akron Law Review*: Vol. 52: Iss. 3, Article 1. July 2019, https://ideaexchange.uakron.edu/cgi/viewcontent.cgi?article=2473&context=akronlawreview

[126] UDRP, *supra note, 121.*

as confusingly similar to the Complainant's MR GREEN trademark. The Panel finds that the Complainant's mark is readily identifiable in the disputed domain name, taken as a whole. It should be noted that the disputed domain name is alphanumerically identical to the trademark with the exception of the addition of the dot which does nothing in the Panel's view to distinguish the mark from the disputed domain name. In the Panel's view, this leads to a finding of confusing similarity.[127]

This has likewise been the approach of panels under the Policy in both country code top-level domain cases and gTLD cases where the complainant's trademark "spans the dot" in the domain name concerned, see for example Tesco Stores Limited v. Mat Feakins, WIPO Case No. DCO2013-0017[128] (<tes.co> compared to TESCO trademark); Bayerische Motoren Werke AG v. Masakazu/Living By Blue Co., Ltd., WIPO Case No. DMW2015-0001 (<b.mw> compared to BMW trademark)[129]; Swarovski Aktiengesellschaft v. Aprensa UG haftungsbeschraenkt, Mike Koefer, WIPO Case No. D2016-2036 (<swarov.ski> compared to SWAROVSKI trademark[130]); and WeWork Companies, Inc. v. Michael Chiriac, Various Concepts Inc., WIPO Case No. D2016-1817 (<joinwe.work>, <nycwe.work>, and <rentmywe.work> compared to WE WORK trademark[131]).

It might seem that the problem of "spanning the dot" is successfully addressed in the UDRP practice, however, *what about spanning the next dot*?

There might be cases, such as e.g. "face.book.tld", in which not only the parent, "book", but the combination of parent and subdomain is confusingly similar to the brand and used in bad faith. Unfortunately, there are no UDRP decisions considering this issue as of now, and the question remains unanswered, remaining a legal loophole for the potential attackers.

---

[127] Mr Green Ltd. v. Alfred Zeiselberger, Mediapool Communications Limited Case No. D2017-1944, WIPO Arbitration and Mediation Center, 30 November 2017, https://www.wipo.int/amc/en/domains/search/text.jsp?case=D2017-1944

[128]Tesco Stores Limited v. Mat Feakins, WIPO Case No. DCO2013-0017, WIPO Arbitration and Mediation Center, 04 October 2013, https://www.wipo.int/amc/en/domains/decisions/text/2013/dco2013-0017.html

[129]Bayerische Motoren Werke AG v. Masakazu/Living By Blue Co., Ltd., WIPO Case No. DMW2015-000, WIPO Arbitration and Mediation Center, 22 September 2015, https://www.wipo.int/amc/en/domains/searach/text.jsp?case=DMW2015-0001

[130] Swarovski Aktiengesellschaft v. Aprensa UG haftungsbeschraenkt, Mike Koefer, WIPO Case No. D2016-2036, WIPO Arbitration and Mediation Center, 2 December 2016, https://www.wipo.int/amc/en/domains/search/text.jsp?case=D2016-2036

[131] WeWork Companies, Inc. v. Michael Chiriac, Various Concepts Inc., WIPO Case No. D2016-1817, WIPO Arbitration and Mediation Center, 17 October 2016, https://www.wipo.int/amc/en/domains/search/text.jsp?case=D2016-1817

Personal names

In accordance with WIPO Overview, personal names as well as descriptive terms and geographical identifiers (though not actionable as such) may be actionable to the extent that they have acquired secondary meaning (through appropriately evidenced use) as a mark.

Can a complainant show UDRP-relevant rights in a personal name?

Well-known examples under UDRP proceedings initiated by Madonna[132] (relying on a US trademark registered for entertainment services and related goods), Paris Hilton[133], Victoria and David Beckham[134], all relying on registered trademarks, to name just a few.

In all these cases the Panels outline that the UDRP does not explicitly provide standing for personal names which are not registered or otherwise protected as trademarks. However, it is a positive aspect of the UDRP that in situations, where a personal name is being used as a trademark-like identifier in trade or commerce, the complainant may be able to establish *unregistered or common law rights* in that name for purposes of standing to file a UDRP case where the name in question is used in commerce as a distinctive identifier of the complainant's goods or services.

In Case №D2022-0036[135], Emmanuel Macron filed a complaint to wrest control of the <emmanuel-macron.com> domain name, which was used to redirect to the website of a politique opponent. The panel concluded that the complainant has established an *unregistered trademark rights* in his name for the purposes of the UDRP. It was discovered that the use of the name "Emmanuel Macron" by the complainant is not limited to his political activities. For example, the complainant has published a certain number of books under his name and offered these for sale which means the name "Emmanuel Macron" for commercial purposes.

At the same time, in Jim Carrey Case[136] *common law trade mark rights* were established in his personal name for the purposes of the Policy. The Panel stated that by virtue of the success

---

[132] Madonna Ciccone, p/k/a Madonna v. Dan Parisi and "Madonna.com" Case No. D2000-0847, WIPO Arbitration and Mediation Center, 12 October 2000, https://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0847.html

[133] Paris Hilton v. Turvill Consultants, Case No. D2012-0965, WIPO Arbitration and Mediation Center, 10 July 2012, https://www.wipo.int/amc/en/domains/search/text.jsp?case=D2012-0965

[134] Victoria Beckham, David Beckham v. Contact Privacy Inc. Customer 1247653581/ Cynthia Panford, Case No. D2021-1841, WIPO Arbitration and Mediation Center, 26 August 2021, https://www.wipo.int/amc/en/domains/search/text.jsp?case=D2021-1841

[135] Monsieur le Président de la République française, Emmanuel Macron contre Samy Thellier, Litige No. D2022-0036, WIPO Arbitration and Mediation Center, 18 May 2022, https://www.wipo.int/amc/en/domains/decisions/pdf/2022/d2022-0036.pdf

[136]Jim Carrey v. BWI Domains, Case No. D2009-0563, WIPO Arbitration and Mediation Center, 16 June 2009, https://www.wipo.int/amc/en/domains/decisions/html/2009/d2009-0563.html

of his numerous films the Complainant has achieved renown as one of the world's most famous actors and comedians. The Panel considers that the disputed domain name is made up of the common law trade mark JIM CARREY to which the generic top-level domain ".com" has been added which does not serve to distinguish the disputed domain name from the Complainant's common law trade mark. The Panel is therefore satisfied that the disputed domain name is virtually identical and confusingly similar to the Complainant's trade mark.

However, the WIPO position is that merely having a famous name (such as a businessperson or cultural leader who has not demonstrated the use of their personal name in a trademark/source-identifying sense), or making broad unsupported assertions regarding the use of such name in trade or commerce, would not likely demonstrate unregistered or common law rights for purposes of standing to file a UDRP complaint (as described in WIPO Overview). Relevant decisions in this sphere are e.g., Israel Harold Asper v Communication X Inc, WIPO Case No. D2001-0540[137], and Chinmoy Kumar Ghose v ICDSoft.com and Maria Sliwa, WIPO Case No. D2003-0248[138]).

Quite separate from the requirement that a complainant asserting unregistered trademark rights in his or her own name establishes that the name has been used in trade or commerce, it would be desirable for such a complainant to indicate the jurisdiction in which such rights are claimed to exist (see, for example, Sibyl Avery Jackson v Jan Teluch, WIPO Case No. D2002-1180[139]). This is complicated by the fact that trademark rights are territorial: they exist only to the extent that they are acknowledged in a particular jurisdiction. In this case, the Complainant has failed to identify the jurisdiction in which the common law rights asserted to exist in her personal name.

As we can see, even in the "easiest" for the establishment criteria there might be a lot of debatable questions, which cause uncertainty and different Panels` approaches to resolving different cases.

Second criteria

The second requirement that the Complainant must prove is that the Respondent has no rights or legitimate interests in the disputed domain name.

---

[137]Israel Harold Asper v Communication X Inc, WIPO Case No. D2001-0540, WIPO Arbitration and Mediation Center, 11 June 2001, https://www.wipo.int/amc/en/domains/decisions/html/2001/d2001-0540.html

[138]Chinmoy Kumar Ghose v ICDSoft.com and Maria Sliwa, WIPO Case No. D2003-0248, WIPO Arbitration and Mediation Center, 22 May 2003, https://www.wipo.int/amc/en/domains/decisions/html/2003/d2003-0248.html

[139]Sibyl Avery Jackson v Jan Teluch, WIPO Case No. D2002-1180, WIPO Arbitration and Mediation Center, 4 March 2003, https://www.wipo.int/amc/en/domains/decisions/html/2002/d2002-1180.html

Among the ways that a domain name owner can prove a legitimate right or interest in a domain name is by showing (in accordance with paragraph 4(c) of the Policy):

- use or preparations to use the domain name in connection with a bona fide offering of goods or services prior to any notice of the dispute;
- that the second-level domain name has commonly known the domain name owner; or
- that the domain name owner is making legitimate noncommercial or fair use of the domain name, without the intent of (i) commercial gain, (ii) misleadingly diverting consumers, or (iii) tarnishing the trademark at issue.

However, the circumstances listed in section 4(c) of the Policy are not an exhaustive list of ways to demonstrate rights or legitimate interests.

Notably, although the Complainant bears the overall burden of proof under the UDRP, Panels have acknowledged that proving a Respondent's lacks rights or legitimate interests in a domain name is often an impossible task, requiring information that is frequently primarily within the knowledge and control of the Respondent (as outlined in WIPO Overview).

Consequently, when a Complainant makes an initial prima facie case (establishment of a legally required rebuttable presumption) that a Respondent lacks rights or legitimate interests in a disputed domain name, the Respondent generally bears the burden of proof on this element. In the absence of such relevant evidence from the respondent, the complainant is presumed to have satisfied the second requirement.

The well-known “Oki Data Test”, though decided in 2001, has been cited in numerous UDRP decisions over the years.

The UDRP case involved a dispute over the domain name <okidataparts.com>. The Respondent stated that it was engaging in fair use of the domain name and, in fact, as an authorised dealer of the Complainant`s products, it said that it must be able to tell consumers that it sells and repairs those products. But Oki Data asserted that its agreement with ASD did not give ASD any rights to the OKI DATA trademark, including in a domain name.[140]

In the Oki Case, the panel provided a concise and important analysis under the second element, focusing mainly on paragraph 4(c)(i) of the UDRP, which says that a registrant has such rights if it has used the disputed domain name “in connection with a bona fide offering of goods

[140]Oki Data Americas, Inc. v. ASD, Inc. Case No. D2001-0903, WIPO Arbitration and Mediation Center, 6 November 2001, https://www.wipo.int/amc/en/domains/decisions/html/2001/d2001-0903.html

or services." To establish a bona fide usage, a registrant must satisfy at least four conditions, according to the panel:

1. "Respondent must actually be offering the goods or services at issue."
2. "Respondent must use the site to sell only the trademarked goods; otherwise, it could be using the trademark to bait Internet users and then switch them to other goods."
3. "The site must accurately disclose the registrant's relationship with the trademark owner; it may not, for example, falsely suggest that it is the trademark owner, or that the website is the official site, if, in fact, it is only one of many sales agents."
4. "The Respondent must not try to corner the market in all domain names, thus depriving the trademark owner of reflecting its own mark in a domain name."

While analysing UDRP cases, we can see that Panels have recognised additional reasons that, despite not being codified in the UDRP, might establish respondent rights or legitimate interests in a domain name.

Dictionary terms

In general, Panels have acknowledged that accumulating and holding domain names consisting of acronyms, dictionary words, or common phrases (usually for resale) might be legitimate and is not illegal per se under the UDRP.

To find rights or legitimate interests in a domain name based on its dictionary meaning, the domain name should be genuinely used, or at least demonstrably intended for such use, in connection with the relied-upon dictionary meaning and not trade off third-party trademark rights[141] (see e.g. Rire et Chansons v. wangcheng Case No. D2021-3049).

Let's imagine that a potential respondent may have a legitimate interest in the domain name <apple.com>., for instance, if it uses the domain name for a website that provides information about apples and everything related to apples in its generic meaning. The same respondent would not, however, have a legitimate interest in the domain name if the corresponding website is aimed at goods or services that target a third-party trademark which uses the same term as a trademark in a non-dictionary sense. In this case: Apple, of course, can be immediately associated with a well-known technology company, accordingly, usage of the same term in the domain name is prohibited.

[141]Rire et Chansons v. wangcheng Case No. D2021-3049, WIPO Arbitration and Mediation Center, 23 October 2021, https://www.wipo.int/amc/en/domains/search/text.jsp?case=D2021-3049

Even if they resemble well-known trademarks, it is permissible to register domain names for their generic value. For the purposes of traditional trademark enforcement, arbitrary trademarks (i.e., when a term has a generic meaning but is used for entirely unrelated services) are strong. However, owners of arbitrary trademarks must exercise greater caution in domain name disputes.[142]

The fact that a domain name can be used and registered for generic purposes while a trademark cannot is a key distinction between trademark law and domain name dispute resolution that can cause brand owners to stumble. Nike (WIPO Case D2020-3067[143]) and Marlboro (WIPO Case D2015-1128[144]), among others, have lost UDRP cases after underestimating the legitimate interests of domain name registrants.

In such circumstances, panels have usually recognised that a respondent's registration of a trademark that corresponds to a disputed domain name typically (but not necessarily) establishes respondent rights or legitimate interests in that domain name for purposes of the second element of the UDRP.

For example, panels have generally refused to find respondent rights or legitimate interests in a domain name based on a corresponding trademark registration when the circumstances demonstrate that the registration was obtained primarily to circumvent the UDRP (see the Lewis Silkin LLP v. 高新区通安洛法克贸易商行 (gao xin qu tong an luo fa ke mao yi shang hang) Case No. D2020-0487).[145]

WIPO provides the following cases as examples:

- Madonna Ciccone, p/k/a Madonna v. Dan Parisi and "Madonna.com", WIPO Case No. D2000-0847[146], <madonna.com>, Transfer;

---

[142] James Taylor, "How strong trademarks such as NIKE and MARLBORO can fail in cybersquatting cases," *World Trademark Review magazine*, (26 May 2022), https://www.safenames.net/resources/blogs/safenames-blog/2022/06/14/how-strong-trademarks-such-as-nike-and-marlboro-can-fail-in-cybersquatting-cases

[143]Nike Innovate C.V. v. Contact Privacy, Inc. Customer 1243971962 / Ladinu Case No. D2020-3067, WIPO Arbitration and Mediation Center, 16 February 2021, https://www.wipo.int/amc/en/domains/decisions/text/2020/d2020-3067.html

[144]Philip Morris USA Inc. v. Borut Bezjak, A Domains Limited, Case No. D2015-1128, WIPO Arbitration and Mediation Center, 11 September 2015, https://www.wipo.int/amc/en/domains/search/text.jsp?case=D2015-1128

[145] Lewis Silkin LLP v. 高新区通安洛法克贸易商行 (gao xin qu tong an luo fa ke mao yi shang hang) Case No. D2020-0487, WIPO Arbitration and Mediation Center,24 April 2020, https://www.wipo.int/amc/en/domains/search/text.jsp?case=D2020-0487

[146] Madonna Case, *supra note, 132.*

- Chemical Works of Gedeon Richter Plc v. Covex Farma S.L., WIPO Case No. D2008-1379[147], <cavinton.com> inter alia, Transfer, Cancellation in Part;

- British Sky Broadcasting Group Plc. and British Sky Broadcasting Limited v. Global Access, WIPO Case No. D2009-0817[148], <skytravel.com>, Denial.

As we can see, at the present time, the principles for establishing rights or legitimate interests are not properly codified in the UDRP. It causes a lot of uncertainty for the Complainants who want to protect their brands and reputation though face a denial due to the simultaneous existence of the Respondent's rights and legitimate interests for the disputed domain. Even well-known huge brands can lose the case though if it was established that the disputed domain name is confusingly similar to that trademark.

That is why it is of high importance to create a sort of *guideline* for the Parties of the dispute in which all the grounds for establishing the second element under the UDRP procedure will be codified. It may help to create more certainty for all the parties involved and be a helpful measure to avoid recurrences of similar incidents in the future.

Third criteria

The complainant must show that the disputed domain name *was registered in "bad faith"* and that *the registration is currently being used in bad faith*. This involves investigating the domain name owner, the website's usage, as well as any misrepresentations concerning the trademark owner, etc.

Paragraph 4(b) of the UDRP Policy sets out the following examples of circumstances that an Administrative Panel will consider to be evidence of the bad faith registration and use of a domain name, including by showing that the domain name owner:

- registered the name primarily to sell or transfer the domain name to the trademark owner or a competitor of the trademark owner for a price greater than out-of-pocket costs;
- engaged in a pattern of registering trademarks of others to prevent the use of the domain name by the trademark owner;
- registered the domain name primarily to disrupt the business of a competitor; or

[147] Chemical Works of Gedeon Richter Plc v. Covex Farma S.L., WIPO Case No. D2008-1379, WIPO Arbitration and Mediation Center, 31 October 2008, https://www.wipo.int/amc/en/domains/decisions/html/2008/d2008-1379.html

[148] British Sky Broadcasting Group Plc. and British Sky Broadcasting Limited v. Global Access, WIPO Case No. D2009-0817, WIPO Arbitration and Mediation Center, 26 August 2009, https://www.wipo.int/amc/en/domains/decisions/html/2009/d2009-0817.html

- is attempting to attract users to a website for commercial gain by creating a likelihood of confusion with the trademark owner's trademark.

It is important to point out that if the respondent's primary intention was to sell the domain name to the trademark holder or one of its rivals for a sum greater than out-of-pocket costs associated with the name, the UDRP contends that the respondent acted in bad faith UDRP 4(b)(i). Numerous cases have been brought where some sort of attempt to sell was alleged or inferred under UDRP. [149]

However, the aforementioned examples are not exhaustive and other circumstances may arise from case to case that establish the registration and usage of a domain name in bad faith.

Bad faith can be considered *subjective* criteria which is the most challenging to establish. There are obvious cases when the attacker is trying to sell the disputed domains to the trademark owners for financial gain which deemed an act of bad faith. However, there are numerous other factors to consider when determining the third criteria.

For example, a landmark UDRP dispute demonstrating bad faith was Case No. D2000-0662 Wal-Mart Stores, Inc. v. Richard MacLeod d/b/a For Sale.[150] The respondent in that case used the domain intentionally in attempts to extort money from the Complainant. The Panel determined that the Respondent acted in bad faith and transferred the domain name to the Complainant.

To show bad faith, it is also helpful to investigate the history of the disputed owner to show patterns of illicit behaviour or habitual fraud. This can entail looking at the company's website and logo to see if they are imitating a legitimate business. These additional items are important to round out the totality of the UDRP case as Elisa Cooper outlines.[151]

Registration and *usage in bad faith*

While analysing the third criteria it is important to take into account that it is required to establish both the *registration* and the *current usage* in bad faith which might be difficult in some cases.

In the SHIRMAX RETAIL LTD./DÉTAILLANTS SHIRMAX LTÉE, [eResolution Case No. AF-0104], for instance, Panel determined that "the requirement of bad faith registration

[149]"Analysis of key UDRP issues", ICANN, accessed 5 November 2022, https://cyber.harvard.edu/udrp/analysis.html#precedent

[150] Wal-Mart Stores, Inc. v. Richard MacLeod d/b/a For Sale. Case No. D2000-0662, WIPO Arbitration and Mediation Center, 19 September 2000, https://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0662.html

[151] Elisa Cooper, "How to win UDRP domain name disputes," 26 July 2022. https://www.worldipreview.com/contributed-article/how-to-win-udrp-domain-name-disputes

and use in paragraph 4(a)(iii) is stated in the *conjunctive* rather than the disjunctive. Registration in bad faith is insufficient if the respondent does not use the domain name in bad faith, and conversely, use in bad faith is insufficient if the respondent originally registered the domain name for a permissible purpose.[152] Therefore, registration in bad faith alone does not give rise to a remedy under the UDRP.

The prominent decision is the Telstra Corporation Limited v. Nuclear Marshmallows Case where it is stated that "This interpretation is confirmed, and clarified, by the use of both the past and present tenses in paragraph 4 (a)(iii) of the Uniform Policy. The use of both tenses draws attention to the fact that, in determining whether there is bad faith on the part of the Respondent, consideration must be given to the circumstances applying both at the time of registration and thereafter. So understood, it can be seen that the requirement in paragraph 4(a)(iii) that the domain name "has been registered and is being used in bad faith" will be satisfied only if the Complainant proves that the registration was undertaken in bad faith and that the circumstances of the case are such that Respondent is continuing to act in bad faith." [153]

However, this approach does not effectively reflect circumstances in which attackers register a large number of domain names but do not use them or immediately cease using them after receiving a complaint; therefore without usage, the simplified dispute resolution procedure is unavailable.

It is also very problematic to the Panel and there are different approaches that co-exist in the Case practice of whether it is possible to use bad faith criteria *retroactively* in some cases.

For example, in Case City Views Limited v. Moniker Privacy Services / Xander, Jeduyu, ALGEBRALIVE, (Case No. D2009-0643) the Panel consider the possibility to use it retroactively. It is stated that "there is a duty on the part of the registrant to conduct an investigation at the time of registration, but also includes a representation and warranty by the registrant that it will not now or in the future use the domain name in violation of any laws or regulations…A party can register or acquire a domain name in good faith, yet use the domain name in the future in such a way that the representations and warranties that the registrant made at the time of the registration are violated. If a party uses the domain name in the future so as to

[152]SHIRMAX RETAIL LTD./DÉTAILLANTS SHIRMAX LTÉE, Case No. AF-0104, 20 March 2000, http://www.disputes.org/decisions/0104.htm

[153] Telstra Corporation Limited v. Nuclear Marshmallows Case No. D2000-0003, WIPO Arbitration and Mediation Center, 18 February 2000, https://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0003.html

call into question the party's compliance with the party's representations and warranties, there may be retroactive bad faith registration."[154]

It is expanded in the case Octogen Pharmacal Company, Inc. v. Domains By Proxy, Inc. / Rich Sanders and Octogen e-Solutions, outlining that "this representation and warranty are not limited to the moment at which the registrant registers the domain name; rather, it extends to any use of the domain name in the future. This obligation is an integral part of the Policy, and it cannot be ignored. And the Panel finds that the language of the Policy and the Telstra approach requires the Panel to examine the facts and circumstances of the case to determine whether the registration of the domain name could be said to be retroactively in bad faith".[155]

This causes a lot of problems, when, apart from unusual cases of a respondent's advanced knowledge of a trademark, it is not even logically possible for a respondent to register a domain name in bad faith contemplation of a mark that does not yet exist or of which the respondent was not aware.

Accordingly, another decision contains a different Panel opinion concerning the third criteria which shows us inconsistency of practice while establishing bad faith.

In the Validas, LLC v. SMVS Consultancy Private Limited Case the Panel outlines that "There is no provision in the warranty itself which deems any breach to have *retroactive effect*. Thus it is necessary to find a deeming provision elsewhere in the Policy if the idea of finding "retroactive" bad faith registration by reason of breach of warranty is to be supported."[156]

The panel further outlines that "the words "without limitation" simply make it clear that a complainant may always meet the conjunctive requirements of paragraph 4(a)(iii) by proving both of its required elements" though determining that "the only permissible way for this to be achieved is for ICANN to *amend the Policy*, paragraph 4(a)(iii) by changing "and" into "or".

Until then this Panel believes that (unsatisfying as it may be in its practical effect in the small number of cases in which it has been an issue) the view should prevail…registration of a domain name that at inception did not breach Policy 4(a)(iii) but is found later to be used in bad faith does not fall foul of Policy 4(a)(iii)".

---

[154]Case City Views Limited v. Moniker Privacy Services / Xander, Jeduyu, ALGEBRALIVE, Case No. D2009-0643, WIPO Arbitration and Mediation Center, 3 July 2009, https://www.wipo.int/amc/en/domains/decisions/html/2009/d2009-0643.html

[155]Octogen Pharmacal Company, Inc. v. Domains By Proxy, Inc. / Rich Sanders and Octogen e-Solutions Case No. D2009-0786, WIPO Arbitration and Mediation Center, 19 August 2009, https://www.wipo.int/amc/en/domains/decisions/html/2009/d2009-0786.html

[156] Validas, LLC v. SMVS Consultancy Private Limited Case No. D2009-1413, WIPO Arbitration and Mediation Center, 29 January 2010, https://www.wipo.int/amc/en/domains/decisions/html/2009/d2009-1413.html

The same opinion was discussed in the first place in Several comments (submitted by INTA and various trademark owners) that advocated various expansions to the scope of the definition of abusive registration.[157]

These comments fairly suggested that the definition should be expanded to include cases of either registration ***or*** use in bad faith, rather than both registration and use in bad faith. I consider this argument a good way to improve the current policy. As discussed further in this Chapter such wording is effectively reflected in the UA-UDRP.

C. Main problematic aspects of UDRP

Despite the drawbacks and practice inconsistency in the establishment of the "three criteria", while analysing a UDRP procedure in detail we can see some other significant *drawbacks* such as:

1. *Limited remedy available*

As previously discussed, UDRP only allows for the *cancellation* or *transfer* of the offending domain name, so monetary damages are not available.

A lot of lawyers claim that a cancellation remedy – instead of transferring – became outdated in our reality as it always bears a risk of re-registration even after the disputed domain name was cancelled as the result of UDRP proceedings. In accordance with the GigaLaw's Domain Dispute Digest[158] more than 95 percent of all cases ended up with transfer decisions and it was a small sliver of decisions, about 1 percent, in which trademark owners essentially won their cases but saw the disputed domain names cancelled instead of transferred (as of the second quarter of 2022).

Due to this reason, Doug Isenberg fairly outlines that it will cause the situation when the time and expense incurred by a trademark owner in filing a UDRP complaint may have to be repeated if the domain name is picked up by another cybersquatter which is inefficient for the Complainant.[159]

We also need to take into account an unfair aspect in the current UDRP procedure that the Complainant is solely responsible for paying the total fees, even if the case was resolved in its

---

[157]"Second Staff Report on Implementation Documents for the Uniform Dispute Resolution Policy," ICANN, 25 October 1999, https://archive.icann.org/en/udrp/udrp-second-staff-report-24oct99.htm

[158]Doug Isenberg, "Why NOT to Cancel a Domain Name in UDRP Cases," 24 August 2022, accessed 05 November 2022, https://giga.law/blog/2022/8/24/udrp-why-not-cancel

[159] *Ibid.*

favour. The fee is split equally between the complainant and the respondent only in cases where a three-member panel is requested by the Respondent.

That is why in order for the cancellation to be an efficient remedy under the UDRP procedure it is recommended to the policymakers to create a *database* of all cancelled under the UDRP procedures domain names in order to prevent their abusive re-registration by the third party (except the Complainant winning the case itself). It will help this Policy to be consistent and will be useful for the companies that already have large domain name portfolios and are not interested in adding more domain names to the mix, especially because every domain name has to be managed and renewed with an annual registration fee.

It also might be the case that the person/company has suffered significant financial damages as a result of the registrant's improper use of the domain name. Accordingly, despite all the benefits of the UDRP policy, initiating court proceedings may be reasonable if the person/company is seeking compensation and a domain name transfer.

2. Is the UDRP decision a *precedent*?

As of now, the panellists while resolving a case under the UDRP procedure, are not required to follow the doctrine of stare decisis (following case precedents of the previous decisions).

From the very beginning of the UDRP policy implementation, it caused some problems as it was difficult for the Parties to predict a possible outcome of the case, especially if the case is heard by one panellist only. The implementation of the precedent is very important to provide fairness in the dispute resolution procedure due to the desire of all the parties involved to have cases treated alike.

The consistency in the UDRP practice also remains of high importance now due to the increased number of decisions which gives rise to the problem of information overload. As fairly outlined by Andrew F. Christie and Fiona Rotstein with so many decisions, it is not possible for a complainant or respondent, let alone a Panellist, to read and understand them all. A precedential system could evolve only if there is a mechanism whereby the content of the decisions – or, at least, of the important decisions – are digested.[160]

This issue, among many others, is addressed in the WIPO Overview. Though unfortunately, the Overview is made by only one (WIPO) of six service providers. WIPO

[160] Andrew F. Christie and Fiona Rotstein, "The Evolution of Precedent in Mandatory Arbitration - Lessons from a Decade of Domain Name Dispute Resolutions," The Arbitrator & Mediator, (April 11, 2011): 73. http://www5.austlii.edu.au/au/journals/ANZRIArbMedr/2011/7.pdf

Overviews outline the "consensus view" reached by Panels on the most significant issues under the UDRP, summarise these consensus views in simple terms, and list the leading decisions that provide persuasive analysis and reasoning on those issues.[161]

The question raised in the Overview "what deference is owed to past UDRP decisions dealing with similar factual matters or legal issues?" was answered as follows:

> "While the UDRP does not operate on a strict doctrine of binding precedent, it is considered important for the overall credibility of the UDRP system that parties can reasonably anticipate the result of their case. Often noting the existence of similar facts and circumstances or identifying distinguishing factors, panels strive for consistency with prior decisions. In so doing, panels seek to ensure that the UDRP operates in a fair and predictable manner for all stakeholders while also retaining sufficient flexibility to address evolving Internet and domain name practices."[162]

As we can see, the establishment of the WIPO Overviews has been instrumental in the UDRP developing the de facto system of precedent that the Overview so accurately describes. Nowadays we can also observe more and more UDRP cases including citing back to previous panel decisions, which is a very positive aspect for the consistency of the UDRP practice. Although the trend appears to be that prior decisions will have at least some persuasive weight, the final determination will be still left to the discretion of each panel.[163]

That is why it is fair to agree with Andrew F. Christie and Fiona Rotstein's point of view recommending all service providers produce an "informal" codification of the decisions producing value-added resources for accessing the jurisprudence of the body of awards.[164]

3. Is it possible to *challenge* the UDRP decision?

There might be cases in which the UDRP issues a decision that one party regards as the final resolution of the dispute, but the other party is dissatisfied with the outcome. These examples demonstrate the lack of actual precedential force of the UDRP procedure discussed above.

---

[161] WIPO Overview, *supra note,* 122.
[162] *Ibid.*
[163] ICANN'S UDRP: Analysis, *supra note,* 149.
[164] Christie and Rotstein, *supra note,* 160: 74.

In accordance Guide to WIPO Domain name dispute resolution, there is no appeal procedure provided within the UDRP system. However, as an administrative mechanism, the UDRP leaves open the option for a party to seek recourse through a court proceeding.[165]

Lack of appeal procedure under UDRP may be considered both a drawback as well as a benefit, as a dissatisfied party can still pursue the matter in a national court if it does not consider the UDRP process a proper, final and binding.

However, the possibility to overrules the UDRP Panel under the court proceedings might cause a lot of problems, especially for the winning party. The court proceeding, initiated by the losing party, will be time-consuming and expensive, which nullifies all possible advantages of the UDRP procedure for the Complainant in the first place. Especially it might be challenging if the parties are not from the same country as the domain name disputes might be treated differently in different jurisdictions. That is why the application of the appeal stage within a clear time frame and with the established appeal costs (paid by the Appellant party only) may be a very useful tool.

Considering all the facts, it is recommended to reconsider the need for the development of a *WIPO-managed UDRP appeals process*[166] in order to omit the possibility of court involvement and provide a time- and cost-efficient appeal framework for the parties.

4. *Privacy* issues

Paragraph 1 of the UDRP Rules define the respondent as "the holder of a domain name registration against which a complaint is initiated." In many cases, however, the named respondent listed in the WhoIs register is not a person or corporation, but a "privacy" or "proxy" registration service. Regarding the latter, paragraph 4(b) of the UDRP Rules provides that:

> "Any updates to the Respondent's data, such as through the result of a request by a privacy or proxy provider to reveal the underlying customer data, must be made before the two (2) business day period concludes or before the Registrar verifies the information requested and confirms the Lock to the UDRP Provider, whichever occurs first. Any modification(s) of the Respondent's data following the two (2) business day period may be addressed by the Panel in its decision."

---

[165] Guide to WIPO Domain Name Dispute Resolution, *supra note,* 73: 18.

[166] John C. McElwaine and Christopher D. Casavale, "Tackling bad faith registration of domain names in a fast-changing landscape," *WIPO Magazine* (December 2019), https://www.wipo.int/wipo_magazine/en/2019/06/article_0006.html

Before implementing the GDPR, the public could conduct WHOIS searches using ICANN (the Internet Corporation for Assigned Names and Numbers), domain name registries, and other search engines to obtain the name and contact information of a domain name registrant. However, after the adoption of the GDPR, domain name registrants' names and contact information are no longer routinely made public via WHOIS searches. Even though it frequently isn't actually covered by the GDPR or other similar data privacy laws, the information is frequently concealed which makes it difficult for the Complainant to identify and reach the potential Resopdent.[167]

Current variations of UDRP policy in different states differently regulate privacy issues (while under some of them it is possible to find some personal information of the Respondent available such as company name etc, while others provide only email or no contact information at all). However, it could be useful in many cases, especially providing a possibility for the Complainant to contact the potential Respondent in order to settle the dispute in an informal manner (while using negotiations or mediation) before challenging the case under the official dispute resolution Policy such as UDRP. This can help even to omit having a case from the very beginning, especially when the registration of the domain name was not intended to be abusive or when the Respondent does not even know about the existence of the Complainant.

The valid fear of brand owners is that registrars may unjustly weigh their trademark interests against the privacy concerns of website operators. It is essential to have clear guidelines and precise protocols outlining how these companies should respond to trademark complaints.

Alternative options must be taken into account if a domain name registry or registrar refuses to provide the requested data. For a fee, one can access historical WHOIS details [168]about domain names from some companies, including the registrant's information. These, however, cannot help with domain names that were registered after the GDPR was implemented and will become more and more out of date.

In some circumstances, it might be possible to complain to ICANN about a registrar's refusal to provide information. In some cases, however, it might be necessary to file a lawsuit against the registrar in the nation where they are located to force them to disclose the information they have on the registrant. This can be an expensive and drawn-out process, just like any legal

[167]David Fyfield, "WHOIS the infringer - identifying the registrant of a domain name," 28 September 2021, accessed 05 November 2022, https://www.mewburn.com/news-insights/identifying-registrant-of-a-domain-name
[168]Matthew Woodward, "3 Ways To Check Domain Ownership History Easily," Updated on 1 September 2022. https://www.matthewwoodward.co.uk/seo/domain-ownership-history/

proceeding and it shows us a lack of a proper certain regulatory framework concerning privacy issues within the UDRP procedure.[169]

The issue of disclosure of information about registrants is still being considered by ICANN and other authorities responsible for the administration of domain names. Until new mechanisms are introduced, the task of identifying a registrant who wishes to remain hidden will remain a difficult task.

To sum up, depending on the nature of the dispute, litigating in a national court is generally more expensive and time-consuming than using the UDRP. For this reason, it is possible that the UDRP procedure will almost completely replace the judicial procedure for resolving domain name disputes.

The Unified Domain Name Dispute Resolution Policy (UDRP) has proven to be a versatile and valuable tool for brand owners in their efforts to address the myriad new ways in which trademark rights may be abused online by attackers. However, when the UDRP was implemented in 1999, a number of the specific challenges that brand owners have faced over the past two decades did not exist.

Accordingly, the UDRP has its critics concerning issues such as a) no mandatory adherence to case precedent which can cause some practice inconsistency and create uncertainty; b) limited remedy possibilities; c) there is also no appeal of the UDRP decisions as well as d) limitations with regard to the privacy issues.

ICANN as the main managing body needs to initiate academic discussions about whether the UDRP currently fulfils the purposes for which it was created, and discuss the improvements needed to face all the problematic aspects that currently arise.

The most logical course of action would be to amend the UDRP into a new and improved authoritative model that can then be used to reconcile all other policies as the UDRP is the source for the development of numerous other domain name policies.

2. UA-DRP

A. General overview

Domain name disputes in Ukraine have always been characterised by the variety of opinions on its resolution and lack of a general approach. For a long time, lawyers could not

[169] Fyfield, *supra note,* 167.

reach common ground, as well as court practice was inconsistent and unclear. The only possible scenario for dispute resolution was litigation without any alternative.[170]

Taking into account all the drawbacks of the court proceedings described above plus adding a high level of corruption and mistrust of the judicial system in Ukraine, protecting the rights in the domain name disputes was a challenging task.

The possibility of out-of-court settlement of disputes concerning the .UA and COM.UA domain names appeared only in 2019 when the UA-DRP administrative procedure which is applied to all the generic Top-Level Domains (gTLD), began to operate in Ukraine.

The conclusion of an agreement between the World Intellectual Property Organization (WIPO) and the Administrator of the .UA top-level domain, Hostmaster Ltd., was a long-awaited event. Under this Agreement, the WIPO Arbitration and Mediation Center become an exclusive authority competent to consider any disputes regarding private second-level domain names in the .UA domain based on the UA-DRP policy. As of May 6, 2021 the .UA Policy will apply to the following third-level domain name registrations: .KYIV.UA, .KIEV.UA, .IVANO-FRANKIVSK.UA, .IF.UA, .POLTAVA.UA, .PL.UA, .UZHGOROD.UA, and .UZ.UA., etc.[171]

.UA Domain Name Dispute Resolution Policy has been designed to secure the fast and impartial process for the resolution of domain name disputes and to remedy the procedural difficulties of protection of intellectual property rights, which are typical for court disputes in Ukraine, such as[172]:

- difficulties in the establishment of the defendant: the status of a domain name registrar - should the registrar be a defendant in such a dispute or a third party?
- lengthy procedure for securing the action by blocking a domain name (assigning the status “Lock” to the domain name);
- length and costs associated with the court action;
- difficulties at the stage of execution of a decision of the court;
- the future of a disputed domain name - should the delegation of the disputed domain name be cancelled or should the disputed domain name be re-delegated to a claimant?

[170]Victoria Sopilnyak and Anastasia Kazankina, “Domain name disputes in Ukraine: is there any alternative?” https://www.iplaw.com.ua/en/base/pressroom/domain-name-disputes-in-ukraine-is-there-any-alternative

[171]WIPO Domain Name Dispute Resolution Service for .UA., accessed 13 November 2022, https://www.wipo.int/amc/en/domains/cctld/ua/index.html

[172] Kateryna Oliinyk and Taras Kyslyy, “Launch of the second phase of implementation of UA-DRP in the domain .UA,” *Legal Alert, Intellectual Property Practice*, https://www.multilaw.com/Multilaw/Documents/Ukraine_IP_UADRP.pdf

- the "inviolability" of contractual relations between a registrant and a domain name registrar - does a court intervenes with its decision in economic relations between the defendant (registrant) and the domain name registrar?
- the process of obtaining data of a registrant which presents a number of challenges as far the domain name registrars have a position of impermissibility of disclosure of personal data of the registrants who are individuals. In the opinion of the registrars, the personal data of such registrants are protected by Personal Data Protection Law and may not be disclosed in response to an attorney's request.[173]

The remedies available to the complainant are the same as under the UDRP: the domain name cancellation or its transfer to the complainant.

In order to file a complaint under the UA-UDRP Policy trademark owners need to consider the Policy for registration of .UA domain names[174].

This policy is restricted to such extent that if a trademark owner does not satisfy the eligibility criteria to register a .UA domain name in the first place then its only remedy may be a cancellation, not a transfer of the disputed domain name as indicated in the Rules for .UA Domain Name Dispute Resolution Policy (the .UA Rules)[175].

B. Differences between UA-UDRP and UDRP Policies

UA-DRP Policy is based on the UDRP Policy, and nowadays can be considered the best possible way to resolve domain name disputes in Ukraine.

The advantages of UA-DRP are mostly the same as UDRP: UA-DRP is much faster than the resolution of a dispute under the jurisdiction of Ukrainian courts, because of the possibility to conduct the UA-DRP case online as UA-DRP does not require the personal presence of the parties, and the defendant's website might be blocked on the second working day after payment for the service by the plaintiff.

This is a positive aspect compared to Ukrainian courts which are more often limited only to the prohibition of the transfer of the site by its owner to anyone other than the plaintiff. The site will be blocked only in the event that the lawsuit contains relevant facts that testify to the bad-faith use of the domain name.

---

[173] Sopilnyak and Kazankina, *supra note,* 170.

[174]Policy for registration of .UA domain names as of April 01, 2014. Accessed 10 November 2022. https://www.hostmaster.ua/policy/Reglament_UA_1.0_UK.pdf

[175]Rules for .UA Domain Name Dispute Resolution Policy, effective as of 19 December 2019, accessed 10 November 2022, https://www.hostmaster.ua/policy/ua-drp/files/UA-Rules-EN.pdf

The registration of the domain name under UA-DRP requires the obligatory ownership of a trademark. For a complaint to be successful under UA-DRP, the following criteria must be proven (see .UA Policy, Paragraph 4(a)[176] and the .UA Rules, Paragraphs 3(b)[177]:

1. The complainant's trademark is identical or confusingly similar to the domain name;
2. The domain name registrant has no rights or legitimate interests in respect of the domain name in question; and
3. The domain name is registered *and/or* used in bad faith.

All the criteria seem to be similar to those of UDRP, however, there are certain differences:

Mutual jurisdiction

This issue arises only in case the losing registrar in a domain name dispute decided to file suit in court to stop the transfer or cancellation of the disputed domain name under the UA-UDRP.

While the UA-DRP procedure allows for the dispute to be transferred only to a Ukrainian court, or for WIPO's Administrative Panel decision to be challenged in a Ukrainian court, the UDRP allows for the dispute to be transferred to the location of either the registrar's principal office or the domain name holder's address.[178]

Language of the proceeding

While both the UA-DRP and the UDRP state that unless otherwise agreed by the parties, the language of the proceeding will be the language of the registration agreement, the UA-DRP further specifies in Section 11 of the .UA Rules that it should be English, Russian or Ukrainian.

This provision of the UA-DRP is limited compared to UDRP and should be modified in the nearest future in order to provide better protection for all the possible parties involved. As a suggestion it is possible at least to exclude the russian language as one of the possible languages of the proceeding or to indicate the Language provision without any limits as follows:

> "the language of the administrative proceeding shall be the language of the Registration Agreement, subject to the authority of the Panel to determine otherwise, having regard to the circumstances of the administrative proceeding".

---

[176].UA Domain Name Dispute Resolution Policy, effective as of 06 May 2021, accessed 11 November 2022, https://www.hostmaster.ua/policy/ua-drp/files/UA-Policy-EN.pdf

[177] .UA Rules, *supra note,* 175.

[178]Igor Alfiorov, "UKRAINE ADOPTS UA-DRP, DOMAIN-NAME DISPUTE-RESOLUTION POLICY SIMILAR TO UDRP," 28 March 2019, https://www.petosevic.com/resources/news/2019/03/4071

Policy modifications

The Administrator of the .UA public domain (Hostmaster) but not ICAAN, as in the case of the UDRP, reserves the right to modify the UA-DRP at any time under Section 9 of the .UA Domain Name Dispute Resolution Policy. The revised policy will be published at least 30 calendar days before its entry into force.

Dispute consolidation

WIPO's Administrative Panel can not consolidate domain disputes governed by both the UDRP and the UA-DRP. Only disputes governed by a single policy may be consolidated, e.g. it is impossible to consolidate disputes regarding <domain.ua> and <domain.com>, because they are governed by different policies – the UA-DRP and the UDRP – but it is possible to consolidate disputes regarding <domain1.ua> and <domain2.ua>.

Bad-faith criteria

The most significant difference is that the complainant under UA-UDRP proves that *either the registration or the use of the contested domain name is in bad faith*, whereas the UDRP requires the complainant to prove both. There is a need to describe this provision in detail as it is crucial for the dispute resolution process though it might seem insufficient.

This subtle difference replacing the word *and* with the word *or* is quite important because the bad faith test under the UDRP is often described as a "conjunctive requirement" (as discussed above). It requires a trademark owner to prove that bad faith exists at two distinct points in time:

a) when the disputed domain was registered and
b) when a complaint is filed.

Doug Isenberg fairly outlines that this can create an impossible requirement for many trademark owners, especially in the situation where a domain name was registered before a trademark owner's rights arose. However, at the same time, the UA-UDRP Policy includes what is referred to as a "disjunctive bad faith requirement". This means that a trademark owner has to prove only that a domain name was registered in bad faith *or* that it is currently being used in bad faith. This little difference makes the UA-UDRP Policy more favourable for trademark owners.[179]

Taking into account the fact that the purpose of a domain name dispute policy is to protect brand owners and their consumers the most important thing would seem to be whether

[179]Doug Isenberg, "Domain Name Disputes in Ukraine," 06 April 2022, accessed 13 November 2022, https://www.youtube.com/watch?v=2T16kKJjI2A

there is any current ongoing harm regardless of what a domain name registrant's previous intention may have been.

UA-UDRP drawbacks

While analysing UA-UDRP, it is also important to indicate some drawbacks of the existing procedure.

Rights or legitimate interests criteria problems

The UA-UDRP is applied to all the generic Top-Level Domains (gTLD) with some peculiarities of functioning of the .UA ccTLD, taking into account the Policy for registration of .UA domain names.

One of them is a requirement to delegate the private second-level domain name in the .UA domain only in the event, when it or its component (before the symbol ".", but not including it) coincides in spelling with a trademark, the rights to use of which within the territory of Ukraine are owned by the appropriate registrant. It means that the Registrant of the .UA domain shall be a trademark owner and own a certificate of Ukraine for the corresponding trademark.

Accordingly, though being a good peculiarity, it may cause some problems while dealing with domain name disputes. Victoria Sopilnyak and Anastasia Kazankina outline that this peculiarity of the functioning of ccTLD.UA currently raises questions about the implementation and successful functioning of the UA-DRP policy[180] due to the following.

As was established before, the UDRP was created to fight against the unfair use of someone else's trademarks in domain names. When submitting a complaint, it is important to prove *all three criteria* in accordance with the UDRP as well as the .UA Policy successfully.

One of the criteria is that it should be described why the Respondent (domain-name holder) should be considered as having *no rights or legitimate interests* in respect of the domain name(s) that is/are the subject of the complaint.

That is why in cases with second-level domains in the .UA domain, the violator, who shall be a trademark owner under the Policy for registration of .UA domain names, *will always have the right or legitimate interest* in respect of the domain name(s) that is/are the subject of the complaint.

It creates a lot of uncertainty when disputes regarding the second-level domains in the .UA domain arises because it always be a dispute between the trademark of the Complainant (right holder) and the trademark of the Respondent (domain-name holder).

[180] Sopilnyak and Kazankina, *supra note,* 170.

Article 495 of the Civil Code of Ukraine establishes that proprietary intellectual property rights in a trademark shall be, in particular, the right to use a trademark.[181] Within the scope of the Law of Ukraine "On Protection of Rights in Trademarks and Service Marks", the use of a mark shall include, among other things, the use thereof on the Internet and *in domain names*.[182]

Consequently, the registration by an actual right holder of a domain name (the future Respondent in the dispute) based on a trademark it owns and the subsequent use of that domain name is an inalienable right of the trademark owner. That is why, as the legitimate domain name holder, the Respondent will almost always be able to demonstrate that it has legitimate rights or interests in the contested domain name which is described in the second UA-UDRP criteria.

This situation causes the following problem: there are two legitimate trademark owners while only one second-level domain name under the .UA can be registered at the same time. Accordingly, in case the Respondent will not be satisfied with the decisions issued in favour of the Complainant and would like to appeal it in court (which is the only possible way to appeal), most likely the case will be overturned.

As disputes of a similar nature, which have been decided exclusively by the courts to date, the courts always emphasise the legitimate intellectual property rights in the defendant's trademark which leads to the impossibility of restricting the right holder's use of its intellectual property rights which is provided under the Ukrainian law.[183]

Let's consider the case of PPG Industries Ohio, Inc., a Delaware corporation against «Internet Invest» LLC as an example[184]. PPG Industries Ohio, Inc. is the owner of several trademarks in Ukraine containing the word element "PPG." Products bearing this trademark, such as paints, varnishes, and lacquers, are sold and well-known to consumers on the Ukrainian market. A dispute arises with regard to the "PPG" trademark for services in Class 36 of the ICGS, as well as the domain name “ppg.ua.” which was registered by an individual later.

The court established that “under the disputed domain name “ppg.ua.” there is a resource (website) on which goods which are identical and related to the goods for which the

[181]Civil Code of Ukraine, 16 January 2003 No. 435-IV, accessed 19 November 2022, https://cis-legislation.com/document.fwx?rgn=8896

[182] Law of Ukraine “On Protection of Rights to Marks for Goods and Services”, *supra note, 15.*

[183] Sopilnyak and Kazankina, *supra note,* 170.

[184] Рішення Солом’янського районного суду м. Києва від 22 травня 2018 р. у справі №760/15666/16-ц, https://reyestr.court.gov.ua/Review/74156496

plaintiff's trademarks are registered are offered for sale" (while after filing the claim, the offer for sale disappeared).

Eventually, the case concluded in favour of the Complainant and the Defendant`s trademark was declared null and void. Accordingly in the next proceeding with the same parties involved the domain name was redelegated to the Complainant.[185]

As we can see, in such cases in order to fight for the domain the Complainant needs to be ready to contest the defendant's trademark registration first (invalidation of the certificate), and only after asking for the domain name transfer, which is time-consuming and expensive in Ukraine. Without doing that, the Complainant might face a lot of difficulties while acquiring the desired domain.

To sum up, the existence of such inconsistency creates problems for the effective application of the UA-DRP policy procedure in Ukraine. Taking into account the fact that there is no appeal available under the UA-UDRP procedure, such cases will also be challenging and a lot of effort will be required to resolve them. Accordingly, the inexpensive and efficient dispute resolution in the first place will become time- and money-consuming while involving the court in the appeal stage.

Though still, despite some significant drawbacks of the UDPR and its variation (such as UA-UDRP), this alternative dispute resolution policy prevails over traditional litigation in a lot of criteria. Some benefits of the judicial system such as the possibility to seek compensation as a remedy are difficult to achieve in court, especially in Ukraine. That is why it is fair to describe UDRP as the easiest and fastest way to resolve domain name disputes nowadays.

In order to make the UDRP and related policies even more efficient, it is important to make certain amendments to the existing regulation suggested in this thesis. Especially law-makers need to reconsider and make applicable corrections to the following issues such as bad faith criteria, remedy and privacy issues, the force of UDRP precedent, as well as create a possibility to appeal under the UDRP framework.

C. Impact of War in Ukraine on the regulation of domain name disputes

Domain name disputes may seem like an unimportant topic in the context of a real war between two countries, but the russian invasion of Ukraine and the ongoing devastation there

[185]Рішення Печерськго районного суду м. Києва від 07 серпня 2018 р. у справі №757/50935/16-ц, https://reyestr.court.gov.ua/Review/76051310

may have some people wondering how cybersquatting issues are handled in those parts of the world.[186]

russia's invasion of Ukraine, for the most part, seems like an old-fashioned war of invasion and terror that demands boots on the ground. In reality, it has blended traditional and innovative elements, and while the cyber dimension has been less visible, it has been full-fledged from the very start. In the words of the Vice Prime Minister and Minister of Digital Transformation Mykhailo Fedorov Fedorov, the world is observing the twenty-first century's "first cyber world war."[187]

Though it is interesting to observe the current challenges in the cyber defence sphere (which is, unfortunately, outside the scope of this thesis), the changes in the domain name dispute regulation also were caused by the illegal invasion of russia in Ukraine.

It is interesting also to underline that while 41 countries have adopted the UDRP Policy to resolve cybersquatting issues and other 42 countries use a variation of the UDRP (such as UA-UDRP), we can see that the russian federation is among a group of countries that don't fall into either of those categories nor has it created a different domain name dispute policy of its own. As a result cybersquatting in the .ru ccTLD is a difficult problem to address and it is typically handled through the russian court system making it impractical for many trademark owners to take any action at all.[188]

Following the invasion, in March 2022, the Ukrainian government asked ICANN to "revoke domains issued in russia and shut down primary Domain Name System servers in the country, a move that would effectively bar access to russian Internet sites, with the potential for knocking the entire country offline."[189]

Eamon Javers outlines that it is true that the move could be unprecedented and such a sanction on the aggressor russian nation would cripple its economy, and force the russian people to feel the negative effects of what their government has done in Ukraine. However, the request

---

[186]Doug Isenberg, "Domain Name Disputes in Ukraine," (06 April 2022), https://giga.law/blog/2022/4/6/domain-disputes-ukraine

[187]Gregory F. Treverton, "Will the Ukraine War Reshape the Internet?" Center for Strategic and International Studies (20 October 2022), https://www.csis.org/analysis/will-ukraine-war-reshape-internet

[188] Isenberg*, supra note,* 179.

[189] Kat Bouza and Noah Shachtman,"Exclusive: Ukraine Pushes to Unplug Russia From the Internet," *Rolling Stone Magazine* (01 March 2022), https://www.rollingstone.com/politics/politics-news/ukraine-icann-russia-internet-runet-disconnection-1314278/

was denied, though sparked a robust debate online about whether removing russia's access to the global Internet is wise amid concern for the future of both the web and the world economy.[190]

"Disconnecting people from the Internet based on nationality, especially during the time of conflict, would cause irreparable damage to both russian and Ukrainian people's ability to fight and resist russian state violence," said Natalia Krapiva, Tech Legal Counsel at Access Now.[191]

The direct impact of war on the Domain name regulation was caused on April 25, 2022, when the WIPO Arbitration and Mediation Center announced that it had temporarily suspended its domain name dispute resolution services under the .UA Domain-Name Dispute-Resolution Policy (UA-DRP) and that it will not accept any new .UA domain name registration requests until further notice.

This decision was taken following WIPO's consultations with the Ukrainian .UA domain operator Hostmaster and was based on the fact that Ukrainian registrars and parties to a dispute may have difficulties participating in arbitration proceedings during the ongoing military actions.

The UA-DRP administrative proceedings will resume once the martial law regime, which was first introduced on February 24, 2022, and currently remains effective, is lifted in Ukraine.[192]

However, it is unclear what the exact implication of this statement may be, but the WIPO may extend deadlines for affected parties, as it did during the COVID pandemic. Also, there is no certainty on how and when the domain name dispute resolution services under the UA-DRP will be held after the end of the WIPO suspension.

In contrast to that, in early April many Ukrainian courts, including those in Kyiv, resumed their activities and began to schedule hearings for April and May. The Ukrainian IPO has also recently published various updates on its activities, online seminars and its cooperation with other countries' IPOs.[193]

To sum up, it shows us that even under these difficult circumstances in the martial law regime, it is crucial for Ukrainian lawyers, lawmakers as well as courts to continue providing the

---

[190] Eamon Javers, "Ukraine asked the internet's governing body to remove Russian sites," *CNBC* (01 March 2022), https://www.cnbc.com/2022/03/01/ukraine-asked-icann-to-revoke-russian-domains-shut-dns-servers.html

[191]"Updates: Digital rights in the Russia-Ukraine conflict," last update 18 August 2022, accessed 15 November 2022, https://www.accessnow.org/digital-rights-ukraine-russia-conflict/

[192]Igor Alfiorov, "WIPO TEMPORARILY SUSPENDS UA-DRP PROCEEDINGS," (04 May 2022), https://www.petosevic.com/resources/news/2022/05/4619

[193]Yuriy Karlash, "IP Protection in Ukraine during the Ongoing War," (20 May 2022). https://www.petosevic.com/resources/articles/2022/05/4622

best possible services to protect Intellectual Property rights avoiding possible future complications and delays with the resumption of temporarily suspended services.

It is important to create a solid base for the protection and enforcement of intellectual property rights in the post-war economy that will strive for innovation and growth.

3. Tendencies related to Domain Name Dispute regulation

Artificial intelligence (AI) 's potential to generate efficiency gains

It is crucial to pay attention to the latest developments in the IT sphere since they may also help resolve domain name disputes successfully.

With the introduction of many digital technologies such as AI that can replicate and even outperform humans, e.g. looking for information while registering domain names can be simplified. Though the application of this technology is still in its primary stage, it is accelerating rapidly, as is the case in many other businesses.

For example, Artificial intelligence (AI)-based technologies may be used in the coming years to streamline this arbitration procedure. As an illustration, it may be used as the foundation for an algorithm designed to find recurring fact patterns or domain names that might be infringing. Similar technologies have been used to automate trademark searches in other industries, for instance.[194]

AI may potentially be used to evaluate and quantify additional impartial signs of "bad faith." To identify domain names that may have been registered with an infringement or illegal intent, for instance, EURid, the.EU registry is successfully using AI to develop tools that proactively examine domain name registration data.

The Abuse Prediction and Early Warning System (APEWS) was created in 2019, designed to prevent the abusive use of domain names before any damage can occur. Domain registrations were evaluated over a period of eleven months to pinpoint patterns that indicate malicious registrations. When APEWS identifies a registered domain as potentially harmful, domain delegation in the .eu zone is delayed. WHOIS displays "server hold" as a status. The domain is delegated for the .eu zone only if the registrant provides appropriate confirmation of identification. If the domain was registered with criminal intent, it is blocked and revoked. After a certain amount of time, it becomes open for registration once more.[195]

---

[194]Gopal Singh Rawat and Rahul Rana, "Role of Artificial Intelligence in Trademark Search," accessed 16 November 2022, https://sagaciousresearch.com/blog/artificial-intelligence-trademark-search/

[195]EURid uses artificial intelligence against domain misuse, 28 April 2020, accessed 18 November 2022, https://www.internetx.com/en/news-detailview/eurid-uses-artificial-intelligence-against-domain-misuse-1/

These studies led to the identification of 22 characteristics that are already evident at the time of registration. They are derived via a Convex Polytope Machine and automatically recognised by the developed system.[196]

It is a very important step as the abuse prevention and early warning system recognises potentially malicious domain registrations before the associated domains are made publicly available which is way much better than providing protection after some damage has occurred.

As we can see, Artificial intelligence-based technologies may and should be used in the coming years to streamline this arbitration procedure while resolving domain name disputes. By analogy to the .EU domain, such technologies also should be used all around the world to battle the possible abusive registration of domain names from the very beginning.

Further active implementation of AI technologies might be a very helpful tool for all the parties involved. For example, as was recommended previously in this thesis, AI might be used to operate and simplify the usage of the database of all cancelled under the UDRP decision domain names. This database might help the registrars to prevent cancelled domain names' abusive re-registration and save time and money on third parties winning the decision concerning the same domain in the first place.

It also might be used to create a database and codify the principles for establishing rights or legitimate interests established by the Panelists in the UDRP decisions as they are not properly codified in the UDRP which causes a lot of uncertainty for the parties involved in the dispute (as was demonstrated above).

What to do to prevent or reduce the possibility of a dispute regarding the domain name?

It is also important to mention some other possible ways to prevent or reduce the possibility of domain name disputes:

1. The possible registrants of the domain name need to make sure that they have not violated the prior third-party rights when composing a domain name. For example, search the label used in the domain name in the national, European Union and international databases (if possible) and in the Register of Legal Entities accordingly.
2. To minimise the risk of a dispute, it is better to avoid registering a domain name that is similar to the trademark or name of the competitor or large well-known companies. Even

[196]Jan Spooren et al. "Premadoma: An Operational Solution for DNS Registries to Prevent Malicious Domain Registrations". https://eurid.eu/media/filer_public/ca/a6/caa62c34-741f-45f1-bbe1-4f5a87f5fd60/official_paper_4_-_premadoma.pdf

if you may have a legitimate right to use such domain, some big businesses might be very aggressive during the dispute resolution process.

3. The persons who apply to register a trademark or establish a legal entity e.g. in Ukraine to make sure there are no existing domain names containing such labels in the .UA WHOIS database, available via the following link: https://www.eurodns.com/whois-search/ua-domain-name;
4. This also might be a case when the business does not own any trademark, however, it is recommended at least to create and register a domain name which contains the name of the business legal entity;
5. It is recommended to the owners of the registered trademarks whose labels consist of the individual commonly used words (for example, “apple”, “shop”, etc.) to establish a second-level domain including the same name as soon as possible, as the first come first serve principle will be implemented for the use of the commonly used words on the Internet;
6. Domain name registrants should use the domains in good faith, link them to their own active websites and publish the information on the actual purpose of the domain creation, create and use the related emails accordingly, etc.
7. One of the reasons for cybersquatting is the simple failure to pay for hosting and domain after the expiration of the domain registration period by the owner. Therefore, domain name owners should carefully follow the terms of payment for the use of the domain in order to avoid resource-consuming problems in the future. There is an auto-renewal system available for some domains, so they get renewed automatically. It's a good idea to use this facility, as even big brands occasionally may forget to renew their domains.

These simple recommendations can be used in order to minimise the potential conflicts in the domain name sphere which might be very challenging and tricky to face in some cases as we can see from this thesis. The best strategy to deal with domain name disputes is to prevent them.

CONCLUSIONS

1. Our names, nationalities, and addresses serve as very important identification tools. However, we are living in an extremely changing world where modern technologies and the Internet, as an integral part of our life, also become crucial instruments for self-expression. Domain names, which are simply our addresses on the Internet, are nowadays one of the most prominent building blocks for a good website and a good company or person's reputation, consumer loyalty and popularity.

Each domain name is unique, so e.g. two “domain.com” can not coexist on the World Wide Web. That is why potential domain name owners need to be very careful while choosing and registering their domain in order to stand out and be recognisable in the Internet space. At the same time getting it wrong may be harmful and cause a lot of problems in terms of profit and goodwill both to the business itself and to the third parties involved in the potential dispute.

2. With the transition of businesses to “online”, the number of conflicts involving domain names is growing every year. The most challenging types of disputes that may occur in the domain name field currently are Cybersquatting, Typosquatting, Passing off domain names, Cyber twin and Reverse domain name hijacking. While new types of conflicts such as Soudnsquatting and Levelsquatting rapidly arrises creating a loophole in the existing regulatory framework. That is why a proper regulatory framework to resolve problematic situations is of high importance.

4. Nowadays, the legal protection of domain names requires more and more attention from their owners due to the lack of clarity in the legislation worldwide. As we can see from this thesis, the new domain name phenomenon is not directly enshrined in the US, EU as well as Ukrainian legislation, and is mostly covered within the trademark regulatory framework, which is not able to reflect all domain name specifics.

5. To answer the research question “Whether the existing dispute resolution proceedings are able to effectively deal with all the challenges arising in domain name disputes?” we can sum up the following. Depending on the nature of the dispute, there are 3 possible domain name dispute resolution mechanisms: UDRP (and similar related procedures), litigation and mediation (which is rarely used in such cases).

Since its implementation in 1999 UDRP procedure became the one that is most often used due to its supranational nature. It is assumed that the UDRP procedure will almost completely replace the judicial procedure in the nearest future as it has a lot of advantages

compared to litigating in a national court: e.g. UDRP is much faster, cheaper and all the procedure is held online.

However, in its current edition UDRP has its fair critics concerning issues such as a) no mandatory adherence to case precedent which can cause some practice inconsistency and create uncertainty; b) unclarity while establishing all three criteria of abusive registration of a domain name (confusing similarity, legitimate rights and interests and “bad-faith” criteria); c) limited remedy possibilities (only cancellation or domain name transfer); d) no appeal of the UDRP decisions; e) limitations with regard to the privacy issues.

UA-UDRP procedure in Ukraine since 2019 became an alternative tool for resolving domain name disputes arising with regard to .UA domain. Though still, some inconsistency within the Policy exists which creates problems for the effective application of the UA-DRP policy procedure in Ukraine. As of now, in order to fight for the domain in Ukraine the Complainant needs to be ready to contest the defendant's trademark registration first (invalidation of the certificate), and only after asking for the domain name transfer, which makes the dispute resolution process time-consuming and expensive.

The UDRP will remain in effect for the foreseeable future, however, all these drawbacks point out the need of amending the UDRP in order to provide an effective domain name dispute resolution mechanism which can deal with the new challenges in cyberspace. ICANN as the main managing body in this sphere needs to initiate academic discussions about whether the UDRP currently fulfils the purposes for which it was created, and discuss the improvements needed to face all the problematic aspects that currently arise.

6. Nowadays, protecting the company's name and reputation, and saving time and money invested in IP became one of the key tasks for each owner in running their business. Prevention (following the recommendations on how to reduce the possibility of a dispute regarding the domain name described above) or early resolution of the disputes in the domain name sphere (while using mediation where possible) is an important guarantee of safe and secure business online.

7. Usage of Artificial intelligence (AI) ’s potential might be an efficient way to simplify a lot of processes in the domain name sphere. It also might be used worldwide (and is now used effectively, though only by a few institutions) to tackle and omit possible conflict situations in the domain name field in the future.

RECOMMENDATIONS

On the basis of this research, the lawmakers can be recommended to take the following steps, which are targeted to put a detailed legal framework in place to address both legal and practical matters arising in the resolution of domain name disputes:

1. **Law on Domain names**. As there is no consistency concerning the legal regulation of domain names all around the world it is important to consider adopting a *special law*, to single out a separate object of intellectual property rights - a domain, establish its legal regime, the status of the domain name owner, and ensure effective protection of their rights and interests. Policymakers should take into account the supranational nature of the Internet and the cross-border usage of domain names when they decide on adopting specific domain name legislation. However, this thesis only reflects academic and legal research on domain name nature and identifies their legal status. Though this recommendation will help to resolve the problem of uncertainty in the domain name & trademark field while establishing clear and unified rules for domain name holders and interested third parties involved, thus ensuring consistency among states' legal provisions.

2. **Amendments to existing UDRP procedure**. After identifying the problematic aspects in the legal regulation of domain name disputes, suggestions will be made to resolve them in the best possible way. It requires to review the existing UDRP and UA-UDRP policies, including whether to:

a) change the element of bad faith from *bad faith registration "**and**" use* to *bad faith registration "**or**" use* in the UDRP Policy – to address scenarios, among others, where an older domain name openly infringes a newer brand;
b) develop a *WIPO-managed UDRP appeal process* within a clear time frame and with the established appeal costs (paid by the Appellant party only). The current system requires appeals to be brought before a court of competent jurisdiction, which requires significant time and money and is not efficient in every case. This also can make the whole UDRP resolution process useless as the losing party may use the appeal in order to delay time and obstruct the execution of the UDRP decision;
c) it is important for the ICANN to pay attention to the increased number of new types of potential domain name disputes such as Soudnsquatting and Levelsquatting and initiate academic discussions in order to develop a mechanism and sort of guideline for the

Panelists on how to face such cases effectively and fairly. It will help to avoid “grey zones” in the UDRP regulation.

d) modify Section 11 of the .UA Rules as follows: a) “Unless otherwise agreed by the Parties, the language of the administrative proceeding shall be the language of the Registration Agreement, subject to the authority of the Panel to determine otherwise, having regard to the circumstances of the administrative proceeding”.

e) create *a database of all cancelled under the UDRP procedures domain names* in order to prevent their abusive re-registration by the third party (except the Complainant winning the case itself);

f) create a *guideline* for the Parties of the dispute in which the principles for establishing rights or legitimate interests (the second element under the UDRP procedure) will be outlined.

BIBLIOGRAPHY

Articles

1. Sara María Ballester Climent, and Begoña Payá Todolí, “Domain names.” https://www.uaipit.com/uploads/publicaciones/files/0000002011_dn.pdf
2. Singh, Snehlata. “Conflicts between Trademarks and Domain Names: A Critical Analysis.” 14 September 2011. https://ssrn.com/abstract=2045222
3. Efroni, Zohar. “Names as Domains, Names as Marks: Issues Concerning the Interface between Internet Domain Names and Trademark Rights.” *INTELLECTUAL PROPERTY AND INFORMATION WEALTH: ISSUES AND PRACTICES IN THE DIGITAL AGE,* Peter K. Yu, ed., Praeger Publishers, (2007). https://ssrn.com/abstract=957750
4. Dimitrov, George. “INTELLECTUAL PROPERTY THE INTERNET AND ELECTRONIC COMMERCE LEGAL PROTECTION OF DOMAIN NAMES.” Paper presented at International Conference on Intellectual Property, the Internet, Electronic Commerce and Traditional Knowledge, May 2001. https://www.wipo.int/edocs/mdocs/ip-conf-bg/en/wipo_ectk_sof_01/wipo_ectk_sof_01_1_6.pdf
5. Sauliūnas, Darius. “Problems of legal nature of internet domain names.” Jurisprudencija, 2003, t. 47(39), 15 December 2003: 29-37. https://repository.mruni.eu/bitstream/handle/007/13436/3330-6980-1-SM.pdf?sequence=1&isAllowed= y
6. Kalinauskas, Marius, and Mantas Barčys. “Legal Challenges Related to the Regulation of a Domain Name System.” *Social Technologies* ISSN 2029-7564 (2012): 366–375. https://www3.mruni.eu/ojs/social-technologies/article/view/203/194
7. “International Telecommunication Union - ICANN and the Global Internet.” Workshop on Member States' experiences with ccTLD Geneva, 3-4 March 2003. Accessed 28 October 2022. https://archive.icann.org/en/cctlds/icann-and-the-global-internet-25feb03.pdf
8. Farrell, Maria. "Quietly, symbolically, US control of the internet was just ended." The Guardian. ISSN 0261-3077 (14 March 2016). https://www.theguardian.com/technology/2016/mar/14/icann-internet-control-domain-names-iana

9. Tanner, Michael "Trademarks, Internet Domain Names, and the NSI: How Do We Fix a System That Is Already Broken," *Journal of Technology Law & Policy*: Vol. 3: Iss. 2, Article 3 (1998). https://scholarship.law.ufl.edu/jtlp/vol3/iss2/3
10. Бааджи Н.П. "Доменне ім'я як об'єкт права інтелектуальної власності." 669-671. http://dspace.onua.edu.ua/bitstream/handle/11300/7281/%D0%91%D0%B0%D0%B0%D0%B4%D0%B6%D0%B8%D0%BD%20%D0%94%D0%BE%D0%BC.%20%D1%96%D0%BC%E2%80%99%D1%8F.pdf?sequence=1&isAllowed=y
11. Wang, Alice A."Diversifying the Domain Name Governance Framework." *Berkeley Technology Law Journal* 32, no. 1 (2017): 137–78. https://www.jstor.org/stable/26488663
12. Ramirez, Natalia. "Will the Anticybersquatting Consumer Protection Act Create More Problems Than It Solves?" *Washington University Journal of Law & Policy*, Vol. 8 (2002): 395-419. https://docplayer.net/230894928-Will-the-anticybersquatting-consumer-protection-act-create-more-problems-than-it-solves-natalia-ramirez.html
13. WIPO "WIPO cybersquatting case filing surges during COVID-19 crisis." 3 June 2020. Accessed 01 November 2022. https://www.wipo.int/amc/en/news/2020/cybersquatting_covid19.html
14. Medha, Mehta. "10 interesting cybersquatting examples to learn from" InfoSec Insights. 19 February 2021. https://sectigostore.com/blog/cybersquatting-examples/
15. Yadav, Sharad. "Domain name disputes in Cyberspace." iPleaders, 14 July 2021. https://blog.ipleaders.in/domain-name-disputes-cyberspace/
16. Pratibha, Ahirwar. "Domain name disputes and cybersquatting in India," 22 February 2019. https://www.mondaq.com/india/trademark/783958/domain-name-disputes-and-cybersquatting-in-india-part-i
17. Chen, Zhanhao, and Janos Szurdi. "Cybersquatting: Attackers Mimicking Domains of Major Brands Including Facebook, Apple, Amazon and Netflix to Scam Consumers," 1 September 2020, https://unit42.paloaltonetworks.com/cybersquatting/
18. Kun Du, Hao Yang, Zhou Li, Haixin Duan, Shuang Hao, Baojun Liu, Yuxiao Ye, Mingxuan Liu, Xiaodong Su, Guang Liu, Zhifeng Geng, Zaifeng Zhang, and Jinjin Liang - DR Hazard, "A Comprehensive Study of Levelsquatting Scams." 2019. https://cpb-us-e2.wpmucdn.com/faculty.sites.uci.edu/dist/5/764/files/2019/07/securecomm19.pdf

19. Speres, Jeremy. “Subdomains and online brand protection: What you need to know. World Trademark Review.” 01 October 2020. https://www.worldtrademarkreview.com/article/subdomains-and-online-brand-protection-what-you-need-know-long-read
20. Warren B. Chik, “Lord of Your Domain, But Master of None: The Need to Harmonize and Recalibrate the Domain Name Regime of Ownership and Control.” *International Journal of Law and Information Technology*, Volume 16, Issue 1 (Spring 2008): 8–72. https://doi.org/10.1093/ijlit/eam005
21. Sourabh Ghosh, “Domain Name Disputes and Evaluation of The ICANN’s Uniform Domain Name Dispute Resolution Policy”, *Journal of Intellectual Property Rights* Vol 9. September 2004: 424-439. http://nopr.niscpr.res.in/bitstream/123456789/4883/1/JIPR%209%285%29%20424-439.pdf
22. Brian W. Borchert. “Imminent Domain Name: The Technological Land-Grab and ICANN's Lifting of Domain Name Restrictions.” Valparaiso University Law Review, Volume 45, Number 2, (2011): 505-549. https://scholar.valpo.edu/cgi/viewcontent.cgi?article=1437&context=vulr
23. Eric Perrott and Sophie Edbrooke, “Domain Name and UDRP Disputes – a Definitive Guide,” Gerben Intellectual Property 7 November 2022. https://www.gerbenlaw.com/blog/the-definitive-guide-to-udrp-proceedings-and-domain-disputes/
24. Christine Haight Farley, "Confusing the Similarity of Trademarks Law in Domain Name Disputes," Akron Law Review: Vol. 52 : Iss. 3 , Article 1 (July 2019). https://ideaexchange.uakron.edu/cgi/viewcontent.cgi?article=2473&context=akronlawreview
25. Taylor, James. “How strong trademarks such as NIKE and MARLBORO can fail in cybersquatting cases.” World Trademark Review magazine, (26 May 2022). https://www.safenames.net/resources/blogs/safenames-blog/2022/06/14/how-strong-trademarks-such-as-nike-and-marlboro-can-fail-in-cybersquatting-cases
26. Cooper, Elisa. “How to win UDRP domain name disputes.” 26 July 2022. https://www.worldipreview.com/contributed-article/how-to-win-udrp-domain-name-disputes
27. Andrew F. Christie and Fiona Rotstein. “The Evolution of Precedent in Mandatory Arbitration - Lessons from a Decade of Domain Name Dispute Resolutions.” *The Arbitrator*

& Mediator, (April 11, 2011): 65-74. http://www5.austlii.edu.au/au/journals/ANZRIArbMedr/2011/7.pdf

28. John C. McElwaine and Christopher D. Casavale. "Tackling bad faith registration of domain names in a fast-changing landscape." *WIPO Magazine* (December 2019). https://www.wipo.int/wipo_magazine/en/2019/06/article_0006.html
29. Sopilnyak, Victoria, and Anastasia Kazankina. "Domain name disputes in Ukraine: is there any alternative?" https://www.iplaw.com.ua/en/base/pressroom/domain-name-disputes-in-ukraine-is-there-any-alternative
30. Oliinyk, Kateryna, and Taras Kyslyy. "Launch of the second phase of implementation of UA-DRP in the domain .UA." *Legal Alert, Intellectual Property Practice*. https://www.multilaw.com/Multilaw/Documents/Ukraine_IP_UADRP.pdf
31. Alfiorov, Igor. "UKRAINE ADOPTS UA-DRP, DOMAIN-NAME DISPUTE-RESOLUTION POLICY SIMILAR TO UDRP." (28 March 2019). https://www.petosevic.com/resources/news/2019/03/4071
32. Isenberg, Doug. "Domain Name Disputes in Ukraine." (06 April 2022). https://giga.law/blog/2022/4/6/domain-disputes-ukraine
33. Gregory F. Treverton. "Will the Ukraine War Reshape the Internet?" *Center for Strategic and International Studies* (20 October 2022). https://www.csis.org/analysis/will-ukraine-war-reshape-internet
34. Bouza, Kat, and Noah Shachtman. "Exclusive: Ukraine Pushes to Unplug Russia From the Internet." *Rolling Stone Magazine* (01 March 2022). https://www.rollingstone.com/politics/politics-news/ukraine-icann-russia-internet-runet-disconnection-1314278/
35. Javers, Eamon."Ukraine asked the internet's governing body to remove Russian sites." CNBC (01 March 2022). https://www.cnbc.com/2022/03/01/ukraine-asked-icann-to-revoke-russian-domains-shut-dns-servers.html
36. Alfiorov, Igor. "WIPO TEMPORARILY SUSPENDS UA-DRP PROCEEDINGS." (04 May 2022). https://www.petosevic.com/resources/news/2022/05/4619
37. Karlash, Yuriy. "IP Protection in Ukraine during the Ongoing War." (20 May 2022). https://www.petosevic.com/resources/articles/2022/05/4622

38. Spooren, Jan, Thomas Vissers, Peter Janssen, Wouter Joosen, and Lieven Desmet. "Premadoma: An Operational Solution for DNS Registries to Prevent Malicious Domain Registrations". https://eurid.eu/media/filer_public/ca/a6/caa62c34-741f-45f1-bbe1-4f5a87f5fd60/official_paper_4_-_premadoma.pdf
39. Кудрицька, Тетяна. "Доменні спори в Україні: останні тенденції та перспективи застосування альтернативних способів вирішення." *Журнал "Інтелектуальна власність України" №10* (21.11.2012). https://vkp.ua/publication/domain_disputes_in_ukraine_latest_trends_and_perspectives_of_alternative_dispute_resolution
40. Гордеюк А. О. "Проблема вдосконалення правового регулювання веб-сайтів і доменних імен в умовах інформатизації суспільства." *Гуманітарний часопис* - № 2 (2019): 73-83. http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=gumc_2019_2_10

Books

1. Rony, Ellen, and Peter. R. Rony. *The Domain Name Handbook: High Stakes and Strategies in Cyberspace*. Lawrence, Kan.: R&D Books, 1998.
2. Nikiforakis, N., Balduzzi, M., Desmet, L., Piessens, F., and Joosen, W.,"Soundsquatting: Uncovering the Use of Homophones in Domain Squatting." In: Chow, S.S.M., Camenisch, J., Hui, L.C.K., Yiu, S.M. (eds) Information Security. Part of the Lecture Notes in Computer Science, vol 8783. Springer, Cham, 2014. https://doi.org/10.1007/978-3-319-13257-0_17

Legal Documents

1. "Lanham (Trademark) Act," (1946). Accessed 17 October 2022. https://www.bitlaw.com/source/15usc/index.html
2. Communication from the Commission to the Council and the European Parliament. "The Organisation and Management of the Internet International and European Policy Issues 1998 – 2000." Brussels, COM(2000) 202 final. 11 April 2000. Accessed 15 October 2022. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52000DC0202&from=EN

3. Regulation (EU) 2019/517 of the European Parliament and of the Council of 19 March 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. Accessed 29 October 2022. https://eur-lex.europa.eu/eli/reg/2019/517/oj
4. Anticybersquatting Consumer Protection Act. Pub. L. No. 106-113, 113 Stat. 1536, 1501A-545 (1999). Accessed 30 October 2022. https://www.govinfo.gov/content/pkg/PLAW-106publ113/html/PLAW-106publ113.htm
5. Rules for Uniform Domain Name Dispute Resolution Policy approved by ICANN on 24 October 1999. Accessed 02 November 2022. https://www.icann.org/resources/pages/udrp-rules-2015-03-11-en
6. Uniform Domain Name Dispute Resolution Policy, Approved by ICANN on 24 October 1999. http://icann.org/udrp/udrp-policy-24oct99.htm
7. Law of Ukraine "On Telecommunications", November 18, 2003. Accessed 17 October 2022. https://www.wto.org/english/thewto_e/acc_e/ukr_e/wtaccukr98a13_leg_1.pdf
8. Law of Ukraine "On Protection of Rights to Marks for Goods and Services", December 15, 1993. Accessed 17 October 2022. https://ukrpatent.org/atachs/tm-law-of-ukraine.pdf
9. Civil Code of Ukraine, 16 January 2003 No. 435-IV. Accessed 19 November 2022. https://cis-legislation.com/document.fwx?rgn=8896
10. Rules for .UA Domain Name Dispute Resolution Policy, effective as of 19 December 2019. Accessed 10 November 2022. https://www.hostmaster.ua/policy/ua-drp/files/UA-Rules-EN.pdf
11. .UA Domain Name Dispute Resolution Policy, effective as of 06 May 2021. Accessed 11 November 2022. https://www.hostmaster.ua/policy/ua-drp/files/UA-Policy-EN.pdf

Case law and UDRP decisions

1. Shaffer v. Heitner, 433 U.S. 186 (1977). Accessed 30 October 2022. https://supreme.justia.com/cases/federal/us/433/186/
2. Vilnius Regional Court, Civil Division, Case No. 2-1061-623/2008. 1 October 2008.
3. Lithuanian Supreme Court's Civil Division, Case No. 3K-3-272/2009, 22 June 2009.
4. Bytedance Ltd. v. Registration Private, Domains By Proxy, LLC / Fotios Tsiouklas, Kickspan Case № D2020-2439. WIPO Arbitration and Mediation Center, 13 January 2021. https://www.wipo.int/amc/en/domains/decisions/text/2020/d2020-2439.html

5. SIEMENS AG v. Omur Topkan, Case №D2013-1318, WIPO Arbitration and Mediation Center 30 September 2013. https://www.wipo.int/amc/en/domains/search/text.jsp?case=D2013-1318
6. Twitter, Inc. v. Ahmet Ozkan, Case №D2014-0469Humana Inc. v. Cayman Trademark Trust Case No. D2006-0073, WIPO Arbitration and Mediation Center 15 June 2014. https://www.wipo.int/amc/en/domains/search/text.jsp?case=D2014-0469
7. LinkedIn Corporation v. Daphne Reynolds, Case №D2015-1679, WIPO Arbitration and Mediation Center 16 November 2015. https://www.wipo.int/amc/en/domains/search/text.jsp?case=D2015-1679
8. Humana Inc. v. Cayman Trademark Trust, Case №D2006-0073, WIPO Arbitration and Mediation Center 7 March 2006. https://www.wipo.int/amc/en/domains/decisions/html/2006/d2006-0073.html
9. PartyGaming Plc., PartyGaming IA Limited v. Harry Thomas, Case №D2008-1275, WIPO Arbitration and Mediation Center 14 November 2008. https://www.wipo.int/amc/en/domains/decisions/html/2008/d2008-1275.html
10. Chanel, Inc. v. Sandy Goldman Case № D2000-1837, WIPO Arbitration and Mediation Center, 13 February 2001. https://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-1837.html
11. EFG Bank European Financial Group SA v. Domain Consults Case № D2011-1907, WIPO Arbitration and Mediation Center, 23 December 2011. https://www.wipo.int/amc/en/domains/search/text.jsp?case=D2015-1679
12. British Telecommunications Plc v One in A Million Ltd, 1 WLR 903 - English Court of Appeal, 1999. https://app.justis.com/case/british-telecommunications-plc-v-one-in-a-million-ltd/overview/c4yZmXqdm5Wca
13. Qtrade Canada Inc. vs. Bank of Hydrov, Case №AF-0169, WIPO Arbitration and Mediation Center, 19 June 2000. http://www.disputes.org/decisions/0169.htm
14. Smart Design LLC v Carolyn Hughes Case №D2000-0993, WIPO Arbitration and Mediation Center, 18 October 2000. https://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0993.html

15. Sydney Opera House Trust v. Trilynx Pty. Limited, Case №D2000-1224, WIPO Arbitration and Mediation Center, 31 October 2000. https://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-1224.html
16. Canon City Property Management, LLC v. David Borden, NAF Claim Number: FA2203001987569, 4 May 2022. https://www.adrforum.com/domaindecisions/1987569.htm
17. Indian Farmers Fertiliser Cooperation Ltd v. International Foodstuffs Co, Case № D2001-1110, WIPO Arbitration and Mediation Center, 4 January 2002. https://www.wipo.int/amc/en/domains/decisions/html/2001/d2001-1110.html
18. Google Inc. v. 1&1 Internet Limited, Claim Number: FA1708001742725, FORUM, 31 August 2017. https://www.adrforum.com/domaindecisions/1742725.htm
19. Zimmermann Wear Pty Ltd v. Sam Dumond, FORUM, 17 September 2018. https://www.adrforum.com/domaindecisions/1802176.htm
20. LEGO Juris A/S v. Legoverhuur.nl, Frank Schuermans, Case No. D2011-1559, WIPO Arbitration and Mediation Center, 13 December 2011. https://www.wipo.int/amc/en/domains/decisions/text/2011/d2011-1559.html
21. Canyon Bicycles GmbH v. Domains by Proxy, WIPO Case No. D2014-0206, WIPO Arbitration and Mediation Center, 14 March 2014. https://www.wipo.int/amc/en/domains/decisions/text/2014/d2014-0206.html
22. Mr Green Ltd. v. Alfred Zeiselberger, Mediapool Communications Limited Case No. D2017-1944, WIPO Arbitration and Mediation Center, 30 November 2017. https://www.wipo.int/amc/en/domains/search/text.jsp?case=D2017-1944
23. Tesco Stores Limited v. Mat Feakins, WIPO Case No. DCO2013-0017, WIPO Arbitration and Mediation Center, 04 October 2013. https://www.wipo.int/amc/en/domains/decisions/text/2013/dco2013-0017.html
24. Bayerische Motoren Werke AG v. Masakazu/Living By Blue Co., Ltd., WIPO Case No. DMW2015-000, WIPO Arbitration and Mediation Center, 22 September 2015. https://www.wipo.int/amc/en/domains/searach/text.jsp?case=DMW2015-0001
25. Swarovski Aktiengesellschaft v. Aprensa UG haftungsbeschraenkt, Mike Koefer, WIPO Case No. D2016-2036, WIPO Arbitration and Mediation Center, 2 December 2016. https://www.wipo.int/amc/en/domains/search/text.jsp?case=D2016-2036

26. WeWork Companies, Inc. v. Michael Chiriac, Various Concepts Inc., WIPO Case No. D2016-1817, WIPO Arbitration and Mediation Center, 17 October 2016. https://www.wipo.int/amc/en/domains/search/text.jsp?case=D2016-1817
27. Madonna Ciccone, p/k/a Madonna v. Dan Parisi and "Madonna.com" Case No. D2000-0847, WIPO Arbitration and Mediation Center, 12 October 2000. https://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0847.html
28. Paris Hilton v. Turvill Consultants, Case No. D2012-0965, WIPO Arbitration and Mediation Center, 10 July 2012. https://www.wipo.int/amc/en/domains/search/text.jsp?case=D2012-0965
29. Victoria Beckham, David Beckham v. Contact Privacy Inc. Customer 1247653581/ Cynthia Panford, Case No. D2021-1841, WIPO Arbitration and Mediation Center, 26 August 2021. https://www.wipo.int/amc/en/domains/search/text.jsp?case=D2021-1841
30. Monsieur le Président de la République française, Emmanuel Macron contre Samy Thellier, Litige No. D2022-0036, WIPO Arbitration and Mediation Center, 18 May 2022. https://www.wipo.int/amc/en/domains/decisions/pdf/2022/d2022-0036.pdf
31. Jim Carrey v. BWI Domains, Case No. D2009-0563, WIPO Arbitration and Mediation Center, 16 June 2009. https://www.wipo.int/amc/en/domains/decisions/html/2009/d2009-0563.html
32. Israel Harold Asper v Communication X Inc, WIPO Case No. D2001-0540, WIPO Arbitration and Mediation Center, 11 June 2001. https://www.wipo.int/amc/en/domains/decisions/html/2001/d2001-0540.html
33. Chinmoy Kumar Ghose v ICDSoft.com and Maria Sliwa, WIPO Case No. D2003-0248, WIPO Arbitration and Mediation Center, 22 May 2003. https://www.wipo.int/amc/en/domains/decisions/html/2003/d2003-0248.html
34. Sibyl Avery Jackson v Jan Teluch, WIPO Case No. D2002-1180, WIPO Arbitration and Mediation Center, 4 March 2003. https://www.wipo.int/amc/en/domains/decisions/html/2002/d2002-1180.html
35. Oki Data Americas, Inc. v. ASD, Inc. Case No. D2001-0903, WIPO Arbitration and Mediation Center, 6 November 2001. https://www.wipo.int/amc/en/domains/decisions/html/2001/d2001-0903.html

36. Rire et Chansons v. wangcheng Case No. D2021-3049, WIPO Arbitration and Mediation Center, 23 October 2021. https://www.wipo.int/amc/en/domains/search/text.jsp?case=D2021-3049
37. Nike Innovate C.V. v. Contact Privacy, Inc. Customer 1243971962 / Ladinu Case No. D2020-3067, WIPO Arbitration and Mediation Center, 16 February 2021. https://www.wipo.int/amc/en/domains/decisions/text/2020/d2020-3067.html
38. Philip Morris USA Inc. v. Borut Bezjak, A Domains Limited, Case No. D2015-1128, WIPO Arbitration and Mediation Center, 11 September 2015. https://www.wipo.int/amc/en/domains/search/text.jsp?case=D2015-1128
39. Lewis Silkin LLP v. 高新区通安洛法克贸易商行 (gao xin qu tong an luo fa ke mao yi shang hang) Case No. D2020-0487, WIPO Arbitration and Mediation Center, 24 April 2020. https://www.wipo.int/amc/en/domains/search/text.jsp?case=D2020-0487
40. Chemical Works of Gedeon Richter Plc v. Covex Farma S.L., WIPO Case No. D2008-1379, WIPO Arbitration and Mediation Center, 31 October 2008. https://www.wipo.int/amc/en/domains/decisions/html/2008/d2008-1379.html
41. British Sky Broadcasting Group Plc. and British Sky Broadcasting Limited v. Global Access, WIPO Case No. D2009-0817, WIPO Arbitration and Mediation Center, 26 August 2009. https://www.wipo.int/amc/en/domains/decisions/html/2009/d2009-0817.html
42. Wal-Mart Stores, Inc. v. Richard MacLeod d/b/a For Sale. Case No. D2000-0662, WIPO Arbitration and Mediation Center, 19 September 2000. https://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0662.html
43. SHIRMAX RETAIL LTD./DÉTAILLANTS SHIRMAX LTÉE, Case No. AF-0104, 20 March 2000. http://www.disputes.org/decisions/0104.htm
44. Telstra Corporation Limited v. Nuclear Marshmallows Case No. D2000-0003, WIPO Arbitration and Mediation Center, 18 February 2000.
45. https://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0003.html
46. Case City Views Limited v. Moniker Privacy Services / Xander, Jeduyu, ALGEBRALIVE, Case No. D2009-0643, WIPO Arbitration and Mediation Center, 3 July 2009. https://www.wipo.int/amc/en/domains/decisions/html/2009/d2009-0643.html
47. Octogen Pharmacal Company, Inc. v. Domains By Proxy, Inc. / Rich Sanders and Octogen e-Solutions Case No. D2009-0786, WIPO Arbitration and Mediation Center, 19 August 2009. https://www.wipo.int/amc/en/domains/decisions/html/2009/d2009-0786.html

48. Validas, LLC v. SMVS Consultancy Private Limited Case No. D2009-1413, WIPO Arbitration and Mediation Center, 29 January 2010. https://www.wipo.int/amc/en/domains/decisions/html/2009/d2009-1413.html
49. Рішення Солом'янського районного суду м. Києва від 22 травня 2018 р. у справі № 760/15666/16-ц, https://reyestr.court.gov.ua/Review/74156496
50. Рішення Печерськго районного суду м. Києва від 07 серпня 2018 р. у справі №757/50935/16-ц. https://reyestr.court.gov.ua/Review/76051310

Website

1. "Domain name disputes." BITLAW. Accessed 03 October 2022. https://www.bitlaw.com/internet/domain.html
2. Cooper, Elisa. "How to win UDRP domain name disputes." 26 July 2022. Accessed October 05. https://www.worldipreview.com/contributed-article/how-to-win-udrp-domain-name-disputes
3. "The Domain Name System (DNS)." The Council of European National Top-Level Domain Registries (CENTR). Accessed 18 October 2022. https://www.centr.org/about-the-industry/item/the-dns.html
4. Lutkevich, Ben, and John Burke. "Domain name system (DNS)." last updated in August 2021. Accessed 20 October 2022. https://www.techtarget.com/searchnetworking/definition/domain-name-system
5. "History of Internet Resources Management in Japan Focusing on Domain Name and IP Address." April 2015. Accessed 12 October 2022. https://www.nic.ad.jp/timeline/en/20th/appendix1.html
6. Kruch, Jane. "DNS: what is it and how it works." Accessed 15 October 2022. https://en.wikiversity.org/wiki/User:Jane_Kruch/DNS:_what_is_it_and_how_it_works
7. Ricart, J. R. ".ORG vs .COM vs .NET: What Do They Mean and Which Is Better?" Wix Blog. Accessed 20 October 2022. https://www.wix.com/blog/2020/06/org-vs-com-vs-net-domain-extensions/
8. ".EU domain name: Questions and answers. | Shaping Europe's digital future." European Commission. Last update 22 February 2022. Accessed 19 October 2022. https://digital-strategy.ec.europa.eu/en/faqs/eu-domain-name-questions-and-answers
9. Scott, Rebecca. "The evolution of Domains. Crazy Domains Learn." 4 October 2022. Accessed 25 October 2022. https://www.crazydomains.com.au/learn/evolution-of-domains/

10. "What are ccTLDs? Why do they matter?" Moz. Accessed 25 October 2022. https://moz.com/learn/seo/cctlds
11. "Second-level domain - MDN web docs Glossary: definitions of web-related terms: MDN." Last update 21 September 2022. Accessed 27 October 2022. https://developer.mozilla.org/en-US/docs/Glossary/Second-level_Domain
12. "What's in a Domain Name: Sub, Second-Level, Top-Level and Country Code Domains Insight." Hover Blog. 24 December 2020. Accessed 27 October 2022. https://hover.blog/whats-a-domain-name-subdomain-top-level-domain/
13. "What are third level domain names?" Softlink Options Limited. 14 September 2022. Accessed 28 October 2022. https://softlinkoptions.co.ke/third-level-domain-names/
14. "ICANN, Internet corporation for assigned names and numbers." Accessed 28 October 2022. https://www.livinginternet.com/i/iw_mgmt_icann.htm
15. "Domain name registration process." ICANN. Last update July 2017. Accessed 29 October 2022. https://whois.icann.org/en/domain-name-registration-process
16. "How to find a domain name owner." 12 March 2021. Accessed 30 October 2022. https://www.domain.com/blog/find-a-domain-name-owner/
17. "Domain conflicts in the legal system." Norid AS. 28 October 2020, last update 21 March 2022. Accessed 01 November 2022. https://www.norid.no/en/om-domenenavn/veiledere/domenekonflikter-i-rettssystemet/
18. Halberstam, Simon. "Key Issues in Domain Name Law." Weblaw. 29 January 2019. Accessed 17 November 2022. https://www.weblaw.co.uk/domain-name-disputes/domain-name-key-issues/
19. "Domain names, online fraud and UDRP proceedings." 11 December 2020. Accessed 02 November 2022. https://www.allenovery.com/en-gb/global/blogs/digital-hub/domain-names-online-fraud-and-udrp-proceedings
20. "Domain Name Dispute Resolution." WIPO - ADR. https://www.wipo.int/amc/en/domains/
21. "Analysis of key UDRP issues." ICANN. Accessed 5 November 2022. https://cyber.harvard.edu/udrp/analysis.html#precedent
22. Doug Isenberg, "Why NOT to Cancel a Domain Name in UDRP Cases," 24 August 2022. Accessed 05 November 2022. https://giga.law/blog/2022/8/24/udrp-why-not-cancel

23. Fyfield, David. “WHOIS the infringer - identifying the registrant of a domain name.” 28 September 2021. Accessed 05 November 2022. https://www.mewburn.com/news-insights/identifying-registrant-of-a-domain-name
24. Woodward, Matthew. “3 Ways To Check Domain Ownership History Easily.” 1 September 2022. https://www.matthewwoodward.co.uk/seo/domain-ownership-history/
25. “Updates: Digital rights in the Russia-Ukraine conflict.” Last update 18 August 2022. Accessed 15 November 2022. https://www.accessnow.org/digital-rights-ukraine-russia-conflict/
26. Gopal Singh Rawat, and Rahul Rana. “Role of Artificial Intelligence in Trademark Search.” Accessed 16 November 2022. https://sagaciousresearch.com/blog/artificial-intelligence-trademark-search/
27. EURid uses artificial intelligence against domain misuse, 28 April 2020. Accessed 18 November 2022. https://www.internetx.com/en/news-detailview/eurid-uses-artificial-intelligence-against-domain-misuse-1/

Miscellaneous

1. International Telecommunication Union Statistics. “Individuals using the Internet.” 29 July 2022. Accessed 05 September 2022. https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx
2. “DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION.” The Internet Engineering Task Force (IETF). November 1987. Accessed 22 October 2022. https://datatracker.ietf.org/doc/html/rfc1035
3. Photo by Jane Kruch “The structure of DNS.” December 01, 2013. Accessed 15 October 2022. https://uk.wikipedia.org/wiki/%D0%A4%D0%B0%D0%B9%D0%BB:Structure_DNS.jpg
4. “What is a root domain?” Online Marketing Glossary. 10 January 2019. Accessed 19 October 2022. https://raventools.com/marketing-glossary/root-domain/
5. Domain names Discussion Paper “Challenges and good practices from registrars and registries to prevent the misuse of domain names for IP infringement activities.” European Union Intellectual Property Office. March 2021. Accessed 19 October 2022. https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/docu

ments/reports/2021_Discussion_Paper_on_Domain_Names/2021_Discussion_Paper_on_Domain_Names_FullR_en.pdf

6. “New gTLDs.” ICANN. Accessed 26 October 2022. https://newgtlds.icann.org/en/program-status/delegated-strings
7. RFC 3912, WHOIS Protocol Specification, L. Daigle. September 2004. Last update 02 March 2013. Accessed 30 October 2022. https://datatracker.ietf.org/doc/rfc3912/
8. Schwemer, Sebastian, Wallberg Knud, Thomas Riis, Ana Nordberg, and Thomas Elholm. “Study on legislative measures related to online IPR infringements.” European Union Intellectual Property Office, 2018. Accessed 01 November 2022. https://data.europa.eu/doi/10.2814/819909
9. EU policy. CENTR. https://www.centr.org/policy/eu-policy.html
10. Guide to WIPO Domain Name Dispute Resolution. WIPO Publication No. 892(E), ISBN: 92-805-1426-1. https://www.wipo.int/export/sites/www/amc/en/docs/guide-en-web.pdf
11. “Research on Online Business Models Infringing Intellectual Property Rights,” EUIPO, Phase 1, (July 2016): 10. https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/resources/Research_on_Online_Business_Models_IBM/Research_on_Online_Business_Models_IBM_ex_sum_en.pdf
12. “WIPO Guide to the Uniform Domain Name Dispute Resolution Policy (UDRP).” WIPO. https://www.wipo.int/amc/en/domains/guide/#a3
13. List of Approved Dispute Resolution Service Providers, ICANN. https://www.icann.org/resources/pages/providers-6d-2012-02-25-en
14. Schedule of Fees under the UDRP, WIPO (valid as of 1 December 2002). https://www.wipo.int/amc/en/domains/fees/index.html
15. WIPO Overview of WIPO Panel Views on Selected UDRP Questions, 2017. https://www.wipo.int/amc/en/domains/search/overview3.0/
16. “Second Staff Report on Implementation Documents for the Uniform Dispute Resolution Policy,” ICANN, 25 October 1999. https://archive.icann.org/en/udrp/udrp-second-staff-report-24oct99.htm
17. WIPO Domain Name Dispute Resolution Service for .UA. Accessed 13 November 2022. https://www.wipo.int/amc/en/domains/cctld/ua/index.html

18. Isenberg, Doug. “Domain Name Disputes in Ukraine.” 06 April 2022. Accessed 13 November 2022. https://www.youtube.com/watch?v=2T16kKJjI2A

ABSTRACT

This thesis describes the phenomenon of a domain name, outlines the DNS specifics and examines domain name evolution in the context of Internet development and governance. The research represents the analysis of domain name legislative framework and regulation within the USA, the EU and Ukraine.

The thesis outlines the types of disputes arising in the domain name sphere while establishing the causes of their creation. Mainly this research intends to explore the current legal regulation of domain name disputes. Based on the comparative analysis of scientific literature, as well as court practise and UDRP decisions, the problematic issues which may arise in domain name dispute regulation procedure were explored in detail in this thesis.

As the result, the recommendations to the legal framework addressing both practical and legal matters arising from the domain name and domain name disputes regulation are delivered.

Keywords: Internet, domain name, DNS, ICANN, UDRP, WIPO.

SUMMARY

PROBLEMATIC ASPECTS OF LEGAL REGULATION OF DOMAIN NAME DISPUTES

The growth and development of the Internet have drastically changed global business, economic, and management processes. Nowadays, the active " online " movement occurs in all spheres of our lives. Considering the supranational nature of the Internet, we can observe the increase in the number of domain name conflicts that challenge the existing legal regulatory framework.

The key aim of the research is to find out whether current dispute resolution proceedings are able to effectively deal with all the challenges arising in domain name disputes.

To achieve that, firstly, attention is drawn to the phenomena of the domain names, the DN system and the evolution of its management and governance. With regard to the supranational nature of the Internet domain name disputes can occur in a country different from where it is registered. That is why the current legislation in the domain name sphere (mostly trademark law) within the USA, EU and Ukraine is examined. The drawbacks of the legislation including its ambiguity and non-uniformity are determined and suggestions are made to create a specific harmonised, unambiguous and similar universal regulatory framework to cover domain names.

Secondly, this thesis identifies the most problematic types of disputes that may occur in the domain name field (such as Cybersquatting, Typosquatting, Passing off domain names, Cyber twin and Reverse domain name hijacking, as well as new types of DND like Soundsquatting and Levelsquatting) and analyses their causes.

The existing Policy in domain name dispute resolution is examined in detail in this research, paying particular attention to UDRP and UA-UDRP procedures. The above examination leads to the conclusion that alternative dispute resolution prevails over traditional litigation while dealing with domain name disputes. Though still there are a lot of problematic aspects that exist and create uncertainty and inconsistency while dealing with conflict situations. That is why certain amendments are required in order to keep up with a rapid Internet development pace and respond effectively to problematic challenges governing new types of domain name disputes in a modern and consistent manner. This thesis describes what kind of amendments or innovations are needed in order to improve the existing regulatory framework.

The purpose of all information provided by the thesis is to safeguard domain name and trademark owners' rights and interests while providing them with an informative and grounded

description of the existing regulatory framework outlining the possible challenges that may arise in the domain name sphere. The modern tendencies and possible changes to the legal regulation of domain name disputes have been analysed in detail in this thesis in order to prevent or alleviate the number of domain name disputes in the future.