Cybersquatting as a Type of Trademark Infringement and its Impact on Fair Competition

Submitted: 27 October 2025
Reviewed: 25 November 2025
Revised: 9 December 2025
Accepted: 10 December 2025

Endi Kalemaj[*]
https://orcid.org/0009-0001-0172-2019
Ervis Çela[**]
https://orcid.org/0009-0004-1630-3644
Maksim Qoku[***]
https://orcid.org/0009-0005-0173-6057

Article submitted to peer blind review

DOI: https://doi.org/10.26512/lstr.v18i2.59972

Abstract

[Purpose] The aim of the study was to critically analyse cybersquatting as a legal and economic anomaly of the digital market.

[Methodology/approach/design] The methodology of the work was based on a combination of the comparative-legal method, detailed analysis of legal acts, international policies and the generalisation of key precedents of judicial and arbitration practice

[Findings] During the study it was established that cybersquatting encompassed various unfair practices, including typosquatting, name-jacking and abuses by registrars. Key protection instruments were analysed: the administrative Uniform Domain-Name Dispute-Resolution Policy and the judicial American Anticybersquatting Consumer Protection Act. In particular, the American approach was based on proving "bad faith intent" under nine judicial factors, whereas the international administrative procedure required the complainant to prove three cumulative criteria to satisfy the complaint. As a result of the comparative analysis of the legal models of the United States of America, Germany, France and Albania, four distinct approaches to regulation were identified: judicial with financial sanctions, hybrid with domain blocking, hybrid with alternative dispute resolution and a model of direct implementation of international standards. It was proved that this phenomenon created artificial barriers to market entry, especially for small and medium-sized businesses, undermined trust in e-commerce, as well as caused significant direct (costs of domain redemption, legal support) and indirect (loss of traffic, reputational damage) economic losses.

[*]PhD, Specialist at the Faculty of Law, University of Tirana, 1010, 4 Mother Teresa Sq., Tirana, Albania. kalemajendi146@gmail.com.
[**]Full Doctor, Professor at the Faculty of Law, University of Tirana, 1010, 4 Mother Teresa Sq., Tirana, Albania. ervis-cela@outlook.com.
[***]Full Doctor, Professor at the Faculty of Law, University of Tirana, 1010, 4 Mother Teresa Sq., Tirana, Albania. mak.qoku@hotmail.com.

[Practical implications] The practical significance of the work lay in the fact that its results could be used to improve national legislation in the field of intellectual property, to develop more effective corporate strategies for the protection of digital assets, as well as serve as methodological material for the training of lawyers and arbitrators specialising in the resolution of domain disputes.
[Originality/value] The study's scholarly contribution lies in its systematic comparative analysis that identifies four distinct regulatory models across jurisdictions (the strict judicial model of the USA, Germany's hybrid administrative-blocking approach, France's specialized ADR system, and Albania's direct implementation of international standards), while demonstrating how cybersquatting functions as both a legal anomaly exploiting regulatory gaps and an economic distortion that disproportionately affects small and medium-sized enterprises through the creation of artificial market barriers and "cyber-inequality."

Keywords: Domain Disputes. Legal Protection. Trademark. Jurisdiction. National Model.

INTRODUCTION

The modern development of the digital economy caused radical changes in the system of protection of intangible assets, especially in the field of management and use of online identifiers (Zhetpisbayev et al., 2017; Hari et al., 2024). One of the most pressing challenges undermining the stability of market competition was the destructive phenomenon known as “cybersquatting”. It represented unfair and speculative registration of domain names identical or similar to trademarks, for the purpose of the further resale or manipulative use. The analysis by Tomer et al. (2024) demonstrated that a domain name had effectively become a new type of property, while the legal regime of its use did not always correlate with the institution of intellectual rights enshrined in international treaties such as the Paris Convention or the Trademark Law Treaty (TLT). The problem was aggravated by the cross-border nature of the Internet space. As Buletsa and Tegza (2022) emphasised, there was no single mechanism for enforcing decisions on domain disputes between jurisdictions. This created a legal asymmetry, whereby cybersquatters deliberately registered disputed domains in so-called “safe harbours” or jurisdictions with minimal regulatory density. The absence of harmonised enforcement practices hindered the protection of both consumers and trademark owners (Omarova et al., 2017; Uderbayeva, 2024). At the same time, cybersquatting was increasingly used as an effective tool of pressure in business negotiations, blackmail, and price speculation. Limongelli and Sposini (2025) recorded a rise in the number of offers to buy out domain names at deliberately inflated prices in cases where the target was start-ups and small enterprises that had not yet managed to register a name linked to the

trademark. Such actions formed unfair barriers to market entry, violated freedom of competition and obstructed technological innovation. On the other hand, in international practice it was recognised that not every registration of a similar domain constituted an infringement. Feng (2025) raised the issue of the necessity of maintaining a balance between the protection of the rights of sign owners and the right to free use of the Internet space. This issue became especially acute in disputes over domains containing commonly used words, abbreviations or personal names. Legal uncertainty in such cases provided opportunities for abuse both by cybersquatters and by corporations (reverse cybersquatting). The formation of the institution of domain dispute resolution within Internet Corporation for Assigned Names and Numbers (ICANN) (in particular, the Uniform Domain-Name Dispute-Resolution Policy (UDRP) mechanism) became an attempt at an institutional response to the challenges of cybersquatting. However, as Vihikan et al. (2021) noted, UDRP arbitration procedures did not always provide full legal protection, especially for small entrepreneurs who did not have sufficient financial and legal resources to conduct lengthy and complex cases. Moreover, practice showed the presence of inconsistency in decisions taken by different domain dispute providers, which complicated the formation of a predictable legal environment. In countries with a transitional economy, including Albania, the situation was further complicated by the absence of a fixed model for the regulation of domain names at the level of national legislation. As Hakiki and Sanusi (2023) emphasised, in the absence of a clear legal mechanism, state authorities were forced to rely on general norms of civil and antitrust law, which created legal uncertainty and slowed down the protection of small and medium-sized businesses. An important aspect was the role of domain registrars, who held technical authority over the delegation of domains. The study by Wibowo et al. (2022) showed that in a number of cases, registrars became active participants in schemes of domain warehousing or domain speculation in the secondary market, profiting from artificial scarcity. Such behaviour undermined the fundamental principles of fairness in the distribution of Internet resources and required strict legal regulation. The issue of reverse cybersquatting also became pressing, whereby large corporations initiated proceedings against private individuals who had legitimately registered a domain, in order to seize the resource without economic costs. As Rajendran and Palaniappan (2022) noted, the centralised nature of the domain name system created risks of abuse and undermined trust in digital assets, which in the long run could lead to monopolisation of the Internet space.

Thus, the study of cybersquatting at the present stage required a comprehensive and in-depth analysis: from legal and institutional mechanisms to economic consequences and threats to competition. Considering that in a

globalised digital environment any actions in one segment could cause cross-border effects, it was extremely important to review existing regulatory approaches, assess the effectiveness and identify legal gaps. The aim of this study was to identify and critically interpret cybersquatting as a legal and economic distortion of the digital market. Within the study the following tasks were set: to analyse legal instruments of stopping cybersquatting in international and national jurisdictions; to identify the consequences of domain capture for overall market balance and digital fairness; to justify practical directions for improving existing mechanisms of protection of the identification space on the Internet.

MATERIALS AND METHODS

This study had a theoretical and empirical character. The methodological basis of the work was grounded on the combination of general scientific and special methods of cognition, among which the key ones were documentary analysis and the comparative-legal method. The application of these methods allowed a comprehensive study of cybersquatting as a legal and economic phenomenon. The basis of the research was a corpus of legal acts, international policies, analytical reports and court precedents. At the first stage, an in-depth analysis of the fundamental instruments regulating domain disputes was conducted. In particular, the key international administrative procedure – the Uniform Domain-Name Dispute-Resolution Policy (Internet Corporation for Assigned Names and Numbers, 1999) – was studied. In parallel, the main judicial mechanism of the USA was analysed, enshrined in the Anticybersquatting Consumer Protection Act (U.S. Government Publishing Office, 1999), in its connection with the general provisions of the Lanham Act (was originally enacted in 1946) (Cornell Law School, 2008) and its predecessor – the Federal Trademark Dilution Act (Congress.gov, 1995). Principles of functioning of proactive protection mechanisms, such as the Trademark Clearinghouse (Internet Corporation for Assigned Names and Numbers, 2025a) and the Uniform Rapid Suspension (URS) (Internet Corporation for Assigned Names and Numbers, 2025b) were also considered. At the second stage, the comparative-legal method was applied to compare different national models of counteracting cybersquatting. The constitutional foundations of the American model were studied through the prism of the Fifth Amendment. Constitution of the United States (Congress.gov, 2025b) and the Fourteenth Amendment (Congress.gov, 2025a) to the US Constitution. To understand the antitrust context, the Sherman Anti-Trust Act (National Archives, 1890) and the Clayton Antitrust Act (Cornell Law School, 1914) were analysed. The legal model of Germany was studied on the basis of the Basic Law of the Federal Republic of Germany (Federal Ministry of Justice and Consumer Protection, 2025a), the Act on the Protection of Trade Marks and other

Signs (Federal Ministry of Justice and Consumer Protection, 2023) and the German Civil Code (Federal Ministry of Justice and Consumer Protection, 2025b). The French model was analysed through the Declaration of the Rights of Man (Yale Law School, 1789) and the Intellectual Property Code (The Public Service for the Dissemination of Law, 2025). The model of Albania was studied on the basis of its Constitution (2025) and the Law No. 9947 On Industrial Property, Albania (World Intellectual Property Organization, 2021). The pan-European context was considered through the provisions of the Treaty on the Functioning of the European Union (TFEU) (University of Oslo, 1957).

Jurisdictional selection was strategically limited to four distinct regulatory models: the United States as a representative of the judicial approach with financial sanctions, Germany and France exemplifying hybrid European Union systems, and Albania representing direct implementation of international standards in a transitional economy context. The temporal scope covered legislative instruments and policies ranging from foundational acts such as the 1890 Sherman Anti-Trust Act through to contemporary mechanisms like the 2025 WIPO-ICA UDRP review project, thereby capturing the historical evolution and current state of cybersquatting regulation. Case selection was based on precedential significance and illustrative value, with specific instances like the Michael Jordan trademark dispute chosen to demonstrate particular forms of cybersquatting such as name-jacking, while registrar practices like GoDaddy's activities illustrated systemic abuses at the administrative level. The exclusion criteria implicitly limited the analysis to documented legal and policy frameworks while deliberately omitting primary empirical data collection such as business surveys or arbitrator interviews, focusing instead on comparative legal analysis of established regulatory instruments and their documented application in domain dispute resolution.

For the analysis of specific unlawful practices and the consequences, data from open sources and reports were used. Certain precedents were considered, such as the case regarding the Michael Jordan brand (2016), as well as registrar practices, illustrated by information about the activity of the company GoDaddy (TechCrunch, 2008). The assessment of the systemic impact of cybersquatting on the economic environment and cybersecurity was carried out on the basis of key conclusions and statistical data presented in the reports Global Cybersecurity Outlook 2025 (World Economic Forum, 2025) and Initial report of the World Intellectual Property Organization (WIPO)-Internet Commerce Association (ICA) UDRP review project team (2025). The comprehensive application of the mentioned materials and methods ensured the achievement of the set goal and the fulfilment of the tasks of the study.

RESULTS

Systematisation and Legal Qualification of the Phenomenon of Cybersquatting

Analysis of primary sources made it possible to establish that the legal qualification of cybersquatting was formed at the intersection of norms regulating the functioning of the Internet and intellectual property legislation. The fundamental document regulating the administrative consideration of disputes was the UDRP (1999), adopted by ICANN. Analysis of the UDRP (Internet Corporation for Assigned Names and Numbers, 1999) text showed that the policy did not provide a single definition of cybersquatting, instead establishing a three-cumulative system of criteria for identifying bad-faith registration. According to paragraph 4(a) UDRP (Internet Corporation for Assigned Names and Numbers, 1999), the complainant had to prove that: the domain name was identical or confusingly similar to its trademark; the domain owner had no legal rights or interests in respect of that name; and the domain had been registered and was being used in bad faith. The third criterion became the key for qualifying actions as cybersquatting. Paragraph 4(b) UDRP (Internet Corporation for Assigned Names and Numbers, 1999) provided a non-exhaustive list of circumstances indicating bad faith, in particular the registration of a domain with the primary purpose of selling it to the trademark owner at a price exceeding documented costs, or registration aimed at obstructing the activities of a competitor. At the national level in the USA, the Anticybersquatting Consumer Protection Act (ACPA) (U.S. Government Publishing Office, 1999) was analysed, which amended the Lanham Act (Cornell Law School, 2008). In the European Union, no unified pan-European act exists that is analogous to the U.S. Anti-Cybersquatting Consumer Protection Act (ACPA), which specifically targets bad-faith domain name registrations mimicking trademarks. Instead, EU law enforcement against such practices relies on harmonized trademark regulations, such as those under the EU Trade Mark Regulation, which protect against confusion, unfair advantage, and parasitism involving trademarks. Unfair competition law, partially harmonized through directives like the Unfair Commercial Practices Directive (UCPD) and Misleading and Comparative Advertising Directive (MCAD), addresses misleading practices and free-riding at both EU and national levels, supplemented by country-specific rules. Additionally, policies governing country-code top-level domains (ccTLDs) provide further mechanisms for resolving disputes over domain names that infringe trademarks or engage in unfair practices. Unlike the UDRP (Internet Corporation for Assigned Names and Numbers, 1999), this legal act directly criminalised cybersquatting, establishing liability for a person who, with bad-faith

intent to profit, registered, used or trafficked a domain name identical, confusingly similar or (for well-known marks) dilutive of the distinctiveness of a trademark. Analysis of the ACPA (U.S. Government Publishing Office, 1999) text made it possible to identify nine non-exhaustive factors that courts had to take into account when determining bad-faith intent, including: the registrant's rights to the trademark, non-commercial use of the domain, an offer to sell the domain without intent to use it for offering goods, and the provision of false contact information upon registration. Thus, whereas the UDRP (Internet Corporation for Assigned Names and Numbers, 1999) focused on the administrative resolution of obvious cases, the ACPA created a full-fledged judicial mechanism to combat this phenomenon. The systematisation of unfair practices was carried out on the basis of analysis of the factual circumstances of court cases and complaints considered under the UDRP (Internet Corporation for Assigned Names and Numbers, 1999), where such actions were qualified as evidence of bad-faith use.

Typosquatting was defined as the intentional registration of domain names that were spelling variations of popular domains, aimed at intercepting Internet traffic from users who made mistakes when entering a web address (Arkabaev et al., 2025; Issayeva et al., 2024). Several common techniques were identified: registering a domain with another top-level domain (e.g. .org instead of .com), using another grammatical form of a word, deliberate misspelling, or phonetically similar names. Cases were also recorded where the "www" part became part of the name without a separating dot (e.g. wwwcnn.com). The study also showed the existence of related practices such as bitsquatting (registration of domains differing by one bit from the original) and combosquatting. Combosquatting involves adding generic words or symbols to a well-known trademark within a domain name to make it appear legitimate, for example paypal-login.net.. Name-jacking was characterised as the registration of domain names containing the names of famous individuals for unauthorised redirection of traffic and exploitation of the popularity. The protection against it was complicated by the fact that a personal name received legal protection as a trademark in US jurisdiction only if it acquired so-called "secondary meaning". An example was the name "Michael Jordan", which had been registered as a trademark, giving the owner exclusive control over the use of the name. The "Michael Jordan" case exemplifies cybersquatting through Qiaodan Sports' bad-faith registration of trademarks using the Chinese characters for "Jordan" (乔丹), mimicking the basketball legend's name without permission to profit from his fame. Qiaodan Sports registered "Qiaodan" – the phonetic equivalent of Michael Jordan's name in Chinese – over a decade before Jordan's 2012 lawsuit, building a sportswear empire around it while also trademarking his jersey number "23" and his sons' names. This unauthorized use confused Chinese consumers into associating the

products with Jordan, diluting his personal brand and goodwill. In 2016, China's Supreme People's Court ruled in Jordan's favor, revoking Qiaodan's use of the name as an infringement after years of lower court losses for him (BBC News, 2016). In cases where the name did not have such status, its protection under the ACPA was problematic. Such actions gave cybersquatters unlawful "free-rider" advantages, allowing parasitising on the reputation of others, which violated the principles of fair competition and devalued trademark protection mechanisms. Reverse Cybersquatting was identified as abuse of rights by trademark owners who attempted to seize a domain name from its lawful owner through unfounded lawsuits. It was found that such actions were often applied by large corporations against smaller companies that had registered the domain in good faith. Reverse cybersquatting was recognised as a serious threat to fair competition, since it allowed dominant market players to eliminate potential competitors and created barriers to market entry for small businesses. To counter such abuses, ICANN (Internet Corporation for Assigned Names and Numbers, 1999) introduced certain safeguards, such as a 60-day waiting period after a change of registration data, which complicated unauthorised domain transfers. Domain name warehousing and abuse of the grace period (Domain Kiting/Tasting) were classified as abuses at the registrar level. Domain warehousing consisted in the registrar intercepting control over domains whose registration had expired and holding the domains for sale at auction or at a significantly higher price. An example of such a practice was the activity of GoDaddy (TechCrunch, 2008). Abuse of the grace period was based on the exploitation of the so-called Add Grace Period (AGP) – a short time span (usually five days) after domain registration, during which it could be cancelled with a full refund. Domain kiting consisted in continuous registration and cancellation of the same domain for its virtually free use, whereas domain tasting meant short-term registration for assessing traffic and potential revenue.

Analysis of Legal Mechanisms to Combat Cybersquatting: Administrative and Judicial Approaches

The next stage of the study was devoted to an in-depth analysis of the legal instruments developed to combat cybersquatting, which included international administrative procedures and national judicial mechanisms. It was found that the UDRP (Internet Corporation for Assigned Names and Numbers, 1999) became the first global mechanism developed specifically for resolving domain disputes. Its creation was initiated in 1998 by the WIPO at the proposal of the USA in response to the inefficiency and expense of traditional litigation in cross-border cases. ICANN implemented this policy by creating a standardised administrative procedure, which became mandatory for domain owners in most generic top-level domains. Analysis of the procedure showed that the UDRP (Internet Corporation

for Assigned Names and Numbers, 1999) functioned as a system of alternative dispute resolution (ADR), which was much faster, cheaper, and less formalised than judicial proceedings. Proceedings were initiated by a trademark owner filing a complaint with one of the accredited dispute resolution centres, such as WIPO, the Asian Domain Name Dispute Resolution Centre (ADNDRC), or the Czech Arbitration Court (CAC). To satisfy a complaint, the claimant had to prove the existence of three mandatory elements: that the disputed domain name was identical or confusingly similar to its trademark; that the respondent had no legal rights or interests in relation to this domain; that the domain had been registered and was being used with bad-faith intent. In turn, the respondent could defend its rights by proving one of three facts: use of the domain for a bona fide offering of goods before the dispute arose; the fact that the respondent had been widely known under that domain name; or legitimate non-commercial or fair use of the domain without intent to obtain commercial gain. At the same time, the study revealed significant shortcomings of the UDRP (Internet Corporation for Assigned Names and Numbers, 1999). Firstly, remedies were limited only to the transfer or cancellation of the domain, with no possibility of recovering monetary damages. Secondly, the procedure was criticised for a possible lack of due process, since the accelerated nature of the consideration could limit the parties' ability to submit evidence. It was important to note that a decision taken within the UDRP (Internet Corporation for Assigned Names and Numbers, 1999) framework was not final and did not deprive the parties of the right to apply to a national court for substantive resolution of the dispute. At the national level in the USA, the main instrument was the ACPA (U.S. Government Publishing Office, 1999). The reason for its adoption was the ineffectiveness of the previous Federal Trademark Dilution Act (Congress.gov, 1995), which required proof that a trademark was "famous", creating significant financial and procedural barriers for many rights holders. The ACPA (U.S. Government Publishing Office, 1999) directly recognised cybersquatting as unlawful and created a new basis for claims in federal courts. The key difference from the UDRP (Internet Corporation for Assigned Names and Numbers, 1999) was that the ACPA (U.S. Government Publishing Office, 1999) focused on proving "bad-faith intent to profit" from registering a domain identical or confusingly similar to a protected trademark. At the same time, unlike the UDRP (Internet Corporation for Assigned Names and Numbers, 1999), the ACPA (U.S. Government Publishing Office, 1999) did not require mandatory proof of the "use" of the domain for bad-faith purposes – the very fact of bad-faith registration was sufficient. The greatest advantage of the ACPA (U.S. Government Publishing Office, 1999) was a much wider range of remedies. In addition to transfer of the domain, the trademark owner could request preliminary injunctions, as well as the recovery of actual or statutory damages

ranging from USD1,000 to USD100,000 per domain name. Comparative analysis of the UDRP Internet Corporation for Assigned Names and Numbers, 1999) and ACPA (U.S. Government Publishing Office, 1999) revealed that these two mechanisms did not compete but complemented each other. The UDRP (Internet Corporation for Assigned Names and Numbers, 1999) proved optimal for quick and inexpensive resolution of obvious cases of cybersquatting, whereas the ACPA (U.S. Government Publishing Office, 1999) provided a broader range of remedies, which was appropriate in more complex cases. For clarity, the key characteristics of these two approaches were summarised in Table 1.

Criterion	Uniform Domain-Name Dispute-Resolution Policy (UDRP)	Anticybersquatting Consumer Protection Act (ACPA)
Procedure type	Administrative, extrajudicial (alternative dispute resolution)	Judicial, considered in US federal courts
Basic criterion of violation	Bad-faith registration and use of a domain	Bad-faith intent to profit from domain registration
Burden of proof	The complainant had to prove all three elements: similarity, absence of rights, bad faith	The claimant had to prove bad-faith intent; the law provided 9 factors for the court's assessment
Available remedies	Only transfer or cancellation of domain name registration	Transfer of the domain, judicial injunctions, compensation of damages (actual or statutory from USD1,000 to USD100,000)
Duration and cost	Fast (on average 45-60 days) and less costly (WIPO started from approximately USD1,500-4,000 depending on the number of domains and the composition of the arbitration panel)	Long (months or years) and much more expensive (might include court fees, payment for lawyers' and experts' services, which overall reached tens of thousands of US dollars)
Status of decision	Binding for the registrar, but did not exclude further appeal to court	Final judicial decision, which had the force of law

Table 1 – Comparative analysis of key mechanisms for resolving domain disputes: UDRP and ACPA

Notes: World Intellectual Property Organisation (WIPO).

Source: compiled by the authors based on the analysis of Uniform Domain-Name Dispute-Resolution Policy Internet Corporation for Assigned Names and Numbers, 1999), Anticybersquatting Consumer Protection Act (U.S. Government Publishing Office, 1999)

Apart from reactive mechanisms, proactive tools were also developed. Central among these tools was the Trademark Clearinghouse (Internet Corporation for Assigned Names and Numbers, 2025a), created by ICANN together with the launch of new generic top-level domains. Trademark Clearinghouse (TMCH) (Internet Corporation for Assigned Names and Numbers, 2025a) functioned as a single centralised database of verified trademarks. Its main function was to provide trademark owners with a priority right to register domains during the "sunrise period". In addition, TMCH (Internet Corporation for Assigned Names and Numbers, 2025a) performed a warning function: the system automatically sent a notification to a potential registrant about the existence of rights, and also informed the rightsholder about the fact of registration itself, which allowed prompt reaction. Another proactive mechanism was the Uniform Rapid Suspension system (Internet Corporation for Assigned Names and Numbers, 2025b). It was developed as an even faster and cheaper alternative to UDRP (Internet Corporation for Assigned Names and Numbers, 1999), intended exclusively for obvious and undisputed cases of trademark infringement. Unlike UDRP (Internet Corporation for Assigned Names and Numbers, 1999), the result of the URS (Internet Corporation for Assigned Names and Numbers, 2025b) procedure was not the transfer of the domain but its temporary suspension. It was specified that URS (Internet Corporation for Assigned Names and Numbers, 2025b) applied only to domains registered after 1 January 2013.

The Impact of Cybersquatting on Fair Competition and the Economic Environment

The final stage of the research was dedicated to the analysis of the impact of cybersquatting on the principles of fair competition and the general state of the market environment. The negative consequences of this practice went far beyond the financial losses of individual companies and affected the fundamental foundations of the digital economy. The trademarks were not just identifiers but key carriers of information on the market, signalling to consumers the origin, quality, and reputation of goods and services.

Cybersquatting, especially in forms that involved the creation of deceptive websites, directly interfered with this process, creating "information noise" and distorting market signals. As noted in the Global Cybersecurity Outlook (World Economic Forum, 2025) report, cyberattacks that used social engineering methods, such as phishing, significantly increased due to the use of generative artificial intelligence, which made deceptive sites even more convincing. This not only harmed a specific company but also reduced the overall level of trust in e-commerce. According to the same report, brand reputation damage and the loss of customer trust were among the key threats that worried company executives.

Thus, cybersquatting destroyed one of the main assets of the market economy – trust, which was necessary for effective interaction between sellers and buyers.

The principles of fair competition assumed that the success of a company depended on the quality of its products and innovativeness, not on the ability to overcome artificially created obstacles (Fedotova et al., 2021; Kerimkhulle et al., 2025). The research showed that cybersquatting created exactly such artificial barriers. The Initial report of the WIPO-ICA UDRP review project team (World Intellectual Property Organization, 2025) emphasised that UDRP (Internet Corporation for Assigned Names and Numbers, 1999) played a critical role in maintaining the secondary market for domain names, codifying certain protective measures for good-faith registrants. However, when a domain name was captured in bad faith, a company, especially a small or medium-sized one, was forced either to pay an exorbitant ransom or to choose a less favourable name, which placed it at a disadvantage. This was confirmed by World Economic Forum (WEF) (2025), which highlighted the growing "cyber inequity" between large and small organisations. 35% of small organisations considered the cyber resilience insufficient, and 71% of cyber leaders believed that small organisations had reached a critical point where the organisations could no longer adequately be protected. This increased the initial costs of doing business and complicated brand promotion. It was established that the economic impact of cybersquatting manifested in direct and indirect losses.

Direct losses included ransom payments for domain names, as well as significant expenses for legal and administrative processes. Although UDRP (Internet Corporation for Assigned Names and Numbers, 1999) was an economically efficient alternative, according to the WIPO-ICA (World Intellectual Property Organization, 2025) report, over 125,000 cases were considered by WIPO alone, which testified to the enormous scale of the problem and the cumulative expenses of businesses to protect the rights. Indirect losses were even more significant. According to the Global Cybersecurity Outlook (World Economic Forum, 2025) report, the US Federal Bureau of Investigation estimated losses from cybercrime in 2023 at more than USD12.5 billion. These losses included lost revenue due to Internet traffic redirection, reduced sales due to consumer confusion, as well as expenses on marketing campaigns aimed at restoring reputation.

The foundation in the USA was the Sherman Anti-Trust Act (National Archives, 1890) and the Clayton Antitrust Act (Cornell Law School, 1914), which were aimed against monopolistic trusts and price-fixing agreements. In the European Union, competition law, enshrined in the Treaty on the Functioning of the EU (TFEU) (University of Oslo, 1957), also aimed to ensure a level playing field for all market participants. Although cybersquatting was not a classic object

of antitrust regulation, it was concluded that its impact on the market had a pronounced anti-competitive character. It distorted the competitive environment, gave undue advantages, and created barriers to market entry. Thus, the fight against cybersquatting was considered not only as a matter of intellectual property protection but also as an integral part of broader efforts to ensure fair competition, which was a fundamental goal of any market economy.

Comparative Analysis of National Legal Models: USA, EU Countries (Germany, France) and Albania

For a deeper understanding of the global landscape of combating cybersquatting, a detailed analysis of national legal models was carried out in key jurisdictions, which represented different approaches to regulation: the United States of America, leading EU countries (Germany and France), and a candidate country for EU membership – Albania. This analysis made it possible to identify fundamental differences in approaches, ranging from the creation of specialised judicial mechanisms to the implementation of administrative procedures and the direct adoption of international standards. The US model was characterised as a judicial model with financial sanctions, based on strong constitutional protection of property. The Fifth Amendment of the Constitution of the United States (Congress.gov, 2025b) and the Fourteenth Amendment to the US Constitution (Congress.gov, 2025a) created a legal presumption in favour of protecting property rights, which extended to intellectual property, including trademarks. On this foundation, the specialised ACPA (U.S. Government Publishing Office, 1999) was developed. Analysis of the text of this law revealed that its uniqueness lay in granting the trademark owner the right to apply to federal court and demand not only the transfer of the domain name but also the imposition of preliminary judicial injunctions and the recovery of statutory damages ranging from USD1,000 to USD100,000 per domain. The law set out nine non-exhaustive factors that courts had to consider when determining "bad-faith intent", including: the registrant's own rights to a trademark in the domain name; the degree of similarity between the domain name and a person's name; prior good-faith non-commercial use of the domain; intent to mislead consumers; offering to sell the domain to the trademark owner without intent to use it; and providing false contact information (U.S. Government Publishing Office, 1999). The possibility of obtaining significant financial compensation made the American model one of the strictest in the world and created a financial deterrent factor for cybersquatters.

The models of leading European Union countries, particularly Germany and France, were hybrid, combining general judicial legislation and specialised administrative procedures for national domains. Unlike the USA, the EU had no single legislative act analogous to the ACPA (U.S. Government Publishing

Office, 1999). In Germany, cybersquatting cases were considered by courts under the provisions of the Act on the protection of trade marks and other signs (Trade Mark Act – MarkenG) (Federal Ministry of Justice and Consumer Protection, 2023) and the German Civil Code (Federal Ministry of Justice and Consumer Protection, 2025b). The constitutional basis for this was Article 14 of the Basic Law of the Federal Republic of Germany (FRG) (Federal Ministry of Justice and Consumer Protection, 2025a), which guaranteed the right to property, including intellectual property. Judicial practice usually qualified cybersquatting as a trademark infringement under § 14 MarkenG (Federal Ministry of Justice and Consumer Protection, 2023) or as a violation of the right to a name under § 12 German Civil Code (Federal Ministry of Justice and Consumer Protection, 2025b). At the same time, the national domain .de had a specific DISPUTE policy administered by the Deutsches Network Information Center (DENIC) registry. Analysis of this policy showed that it was not an arbitration procedure like UDRP (Internet Corporation for Assigned Names and Numbers, 1999). The trademark owner could file an application, and if it met the criteria, the disputed domain was blocked (a DISPUTE record was set), which prevented its transfer to third parties. However, for the actual transfer of the domain, the claimant still had to go to a general jurisdiction court. Thus, the German model used an administrative tool to "freeze" the asset, while leaving the resolution of the dispute on the merits exclusively to the judiciary. In France, judicial protection was also based on the general norms of the Intellectual Property Code (The Public Service for the Dissemination of Law, 2025), and the constitutional basis was Articles 2 and 17 of the Declaration of the Rights of Man and of the Citizen of 1789 (Yale Law School, 1789), which was part of the constitutional block and proclaimed property a "sacred and inviolable right". Cybersquatting could be prosecuted as trademark infringement (contrefaçon de marque) or on the grounds of unfair competition (concurrence déloyale) (Smailov et al., 2025; Kotukov et al., 2025). However, for the national domain .fr, the Système de Résolution des Litiges (SYRELI) procedure operated, administered by the Association Française pour le Nommage Internet en Coopération (AFNIC). Unlike the German DISPUTE, SYRELI was a full-fledged ADR procedure, very similar to UDRP (U.S. Government Publishing Office, 1999). It allowed trademark owners to obtain the transfer or deletion of a domain name quickly (within two months) and at low cost, without going to court. This created an effective two-level system: a fast administrative route for obvious cases and a full judicial process for complex disputes.

The Albanian model could be characterised as a model of direct implementation of international standards. Analysis showed that Albania lacked a special law aimed at combating cybersquatting. Trademark protection was regulated by the general Law No. 9947 "On Industrial Property" (World

Intellectual Property Organization, 2021) and the constitutional basis was Article 41 of the Constitution of Albania (2025), which protected private and intellectual property. Analysis of Articles 131-134 of this law (Albania constitution, 2025) showed that it granted the owner of a registered mark the exclusive right to use it and the right to prohibit third parties from using similar signs, creating a general legal basis for claims. However, the law contained no special provisions or remedies adapted to the specifics of domain disputes. A key feature of the Albanian model was the regulation of disputes in the national top-level domain .al. The dispute resolution policy in the .al domain zone was partly based on principles similar to UDRP (U.S. Government Publishing Office, 1999) but was not its official implementation. Disputes were resolved through national administrative or judicial bodies, without direct involvement of international arbitration institutions (such as WIPO). This approach provided predictability and access to a recognised procedure. It limited remedies only to the transfer or cancellation of the domain, without providing the possibility of recovering financial damages, which was available in judicial models such as the American one. The key differences between the analysed national models, from constitutional foundations to specific remedies, were presented in Table 2.

Parameter	**USA**	**EU (Germany/France)**	**Albania**
Constitutional basis	Fifth and Fourteenth Amendments (protection of property)	Article 14 of the Basic Law of FRG; Articles 2, 17 of the Declaration of the Rights of Man and of the Citizen of 1789 (France)	Article 41 of the Constitution (protection of intellectual property)
Basic legal tool	Specialised ACPA law	General trademark and unfair competition legislation	General Law "On Industrial Property"
Role of administrative procedures	Absent (disputes resolved mainly in courts)	Hybrid: DISPUTE (Germany) – domain blocking; SYRELI (France) – full ADR procedure	UDRP not implemented
Available remedies	Damages: actual losses, lost profits, statutory compensation (USD1,000-	Damages: actual losses and lost profits; possibility of cost recovery. Instrument: lawsuits (transfer, damages,	Damages: compensation not provided, only loss of the domain name. Instrument:

	100,000 per domain under ACPA). Instrument: lawsuits in federal courts. Actions: domain transfer, judicial injunctions, compensation recovery.	prohibition of use); administrative procedures: DISPUTE (Germany – temporary blocking) and SYRELI (France – full ADR procedure). Actions: transfer or blocking of domain, recovery of damages, cessation of use.	international administrative procedure UDRP. Actions: transfer or cancellation of domain.
Model characteristic	Judicial, with financial deterrence	Hybrid, with two-level protection (judicial and administrative for national domains)	Direct implementation of international standard
Efficiency and cost of procedures	The procedure was long (from several months to years), costly (court fees + lawyers' fees could reach tens of thousands of dollars). At the same time, it allowed recovery of significant compensation (up to USD100,000 per domain).	The SYRELI system in France provided online administrative dispute resolution within a few weeks, at minimal cost. DISPUTE in Germany worked as temporary domain blocking until the dispute was resolved, which also made the process more accessible.	Protection occurred exclusively within the international administrative UDRP procedure, which lasted about 45-60 days and cost from USD1,500 to USD4,000, making it accessible but without the possibility of compensation recovery.

Table 2 – Comparative legal analysis of national legal models for combating cybersquatting

Source: compiled by the authors based on analysis of legislation and policies of the USA (U.S. Government Publishing Office, 1999), Germany (Federal Ministry of Justice and Consumer Protection, 2023), France (The Public Service for the Dissemination of Law, 2025), and Albania (World Intellectual Property Organization, 2021).

Thus, the comparative analysis revealed four different strategies of legal regulation. The USA chose the path of creating a powerful judicial instrument

with financial sanctions. Germany relied on general legislation, supplementing it with an administrative mechanism of domain blocking. France created a hybrid system, where general legislation coexisted with a specialised administrative procedure for its own domain. Albania, in turn, relied in its national domain zone on a proven international standard. This diversity of approaches illustrated the global search for the optimal balance between efficiency, accessibility, and the strength of legal remedies in the fight against cybersquatting.

DISCUSSION

The results of the conducted research confirmed that cybersquatting was a significant and multifaceted phenomenon, which affected the system of fair competition, going far beyond the traditional violation of trademark rights. \The issue of domain name capture covered not only legal but also economic, institutional, and reputational parameters of the functioning of the digital market. The comparison of these findings with the works of other researchers revealed both a significant number of points of convergence and certain problematic discrepancies, especially in the context of transnational differences in regulatory frameworks. Modern research emphasised that a domain name in the digital economy functioned not just as an identifier but as a highly liquid market asset. This conclusion correlated with the position of Laketić (2024), according to which domains with high commercial value turned into objects of speculative registration. The results of this analysis confirmed this observation, as cases were recorded when cybersquatting became an obstacle to market positioning and led to the loss of client traffic. This, in turn, confirmed the conclusions of Almarzooqi et al. (2022), who emphasised that the domain name was an integral part of branding strategy, and its loss affected the entire value chain. A significant impact on consumer behaviour was also exerted by forms of typosquatting, when unfair actors registered domain names with orthographically and visually similar symbols to the original brand. Such actions became an instrument of traffic manipulation, phishing, and content substitution, which had earlier been analysed by Ahammad et al. (2022). The functional use of domain names in such schemes was examined in detail by Wang et al. (2024). The authors focused on attacks using homographs of international domain names (IDN homograph attacks), when attackers used similar characters of different languages to create fake domains almost indistinguishable from legitimate ones. The study emphasised that traditional detection methods were mainly oriented towards identifying typosquatting, while the detection of homographs in international domains remained less effective due to the problem of data imbalance. In this study, similar practices were identified, especially in cases related to the registration of domains

for redirection to competitors' resources, which fully corresponded with the cited works.

Some scholars drew attention to the phenomenon of reverse cybersquatting – situations when large brands used legal mechanisms to pressure domain owners acting in good faith. The study of Imayani et al. (2024) described such cases, however, within this analysis such precedents were recorded only episodically. On the contrary, the prevailing situations were those in which small and medium-sized companies became the affected parties, deprived of effective legal protection. This confirmed the thesis about institutional inequality in access to legal protection, described by Bush et al. (2025), which was traced in cases where large companies dominated over local actors, violating the principle of equality. The analysis of regulatory instruments, such as UDRP and ACPA, showed the limitations in local domain zones, especially in the context of country code top-level domain. Arnott (2014) pointed out the low degree of adaptation of these mechanisms in developing countries. Empirical data obtained during the analysis of the legal model of Albania confirmed this: although the country implemented UDRP, this forced local businesses to conduct case consideration in international bodies, creating barriers. The fragmentation of national domain arbitration procedures, analysed by Šutova and Vlaškovic (2022), found confirmation in the situation in Albania, where the absence of its own specialised tribunal slowed down the formation of national judicial practice. Particular attention in the literature was given to the instability of the definitions of "fair use" and "legitimate interest". The analysis of Jon and Park (2025) showed that these concepts were interpreted with a high degree of variability, which complicated achieving legal certainty. The legal subjectivism in the evaluation of domain disputes, presented in detail in the analysis of Mukhopadhyay et al. (2025), was confirmed by the fact that the absence of unified criteria generated ambiguous interpretations and reduced the predictability of outcomes. The analysis in this study confirmed this tendency, as it was revealed that even with clear criteria in ACPA and UDRP, the application remained largely at the discretion of the court or arbitration panel. In the European context, it became increasingly evident that the protection of digital brands required the integration of consumer protection mechanisms with intellectual property protection tools.. De Paula Castro et al. (2022) emphasised the necessity of converging these approaches. In practice, as the analysis showed, it was consumers who became the objects of disorientation in conditions of domain name abuse, which undermined trust in the market. The idea that judicial protection against cybersquatting should be considered as an element of public interest was put forward by Chaisse and Friedmann (2024). However, empirical materials, especially concerning countries with transitional economies, testified to the opposite: domain disputes rarely became the subject of

priority judicial consideration. An important aspect concerned the territorial applicability of legal decisions. The study of Ramsey (2020) recorded that the extraterritorial effect of ACPA decisions was limited, especially in cross-border disputes. These data correlated with the results of this analysis, where international decisions were not always easily implemented at the level of national judicial instances, especially in the absence of direct integration, as in the case of Albania with UDRP.

The underestimation of the significance of digital identity as an object of legal protection, recorded by Lasisi and Tembe (2025), was also traced in the studied jurisdictions. Despite the presence of regulatory provisions, the implementation mechanisms in the digital context turned out to be fragmented. This indicated not only institutional gaps but also the absence of strategic awareness of the importance of digital assets. The problem of the absence of effective legal protection for local brands was emphasised by Singh (2025). Empirically, this manifested in the inability of small businesses, particularly in Albania, to defend the right to a domain even with evident good faith of claims. In this same context, the deepening of digital inequality as a result of cybersquatting received attention in the studies of Binhammad et al. (2024), who showed that the absence of equal access to legal resources intensified market asymmetries. This observation was confirmed within the analysis of cases from Albania, where the limitation of legal support significantly reduced the possibilities of protection. A particular category of disputes consisted of cases with geographical indications, about which Ma et al. (2025) wrote. The study reflected similar cases of domain registration containing city and region names by third parties, which prevented legitimate use. Finally, the absence of verification mechanisms at the stage of registration and blocking of domains that violated rights was raised in the works of Huertas-García et al. (2023). All the cases in this analysis confirmed that domains were registered without prior filtering, which enabled the emergence of conflict. Thus, the comparison of empirical data with academic sources confirmed the necessity of a systemic transformation of mechanisms of counteraction to cybersquatting. Individual authors, in particular Moura et al. (2017), emphasised the necessity of involving international organisations in forming a unified standard for regulating domain disputes. The obtained results demonstrated that the absence of unified procedures led to legal fragmentation. Modern research proved that only a comprehensive combination of preventive technical solutions (such as TMCH and URS), unified legal procedures (such as UDRP and ACPA), and institutional support for small and medium-sized businesses could provide sustainable protection of digital identifiers. Strengthening legal predictability, transparency of arbitration

procedures, and international coordination remained key conditions for restoring trust in the system of online identifiers and ensuring fair competition.

CONCLUSIONS

The conducted research achieved its aim by performing a critical analysis of cybersquatting as a complex legal and economic problem, which distorted the fundamental principles of fair competition in the modern digital environment. The cybersquatting was not simply an isolated form of trademark infringement but a multifaceted systemic phenomenon, functioning at the intersection of economic incentives, technical vulnerabilities, and gaps in national and international regulation. It exploited these weaknesses for obtaining undue benefit, thereby creating significant, and sometimes insurmountable, barriers for business and seriously undermining end-user trust in e-commerce. In the course of the work, the key unlawful practices were successfully systematised and typologised, from obvious forms, typosquatting and name-jacking, to more hidden abuses at the level of registrars, including domain warehousing. The comparative legal analysis made it possible to identify and describe in detail four main national models of counteraction to this phenomenon: the strict judicial model of the USA, emphasising financial deterrence; the flexible hybrid German model, which combined judicial proceedings with administrative domain blocking; the effective hybrid French model with a specialised alternative dispute resolution procedure; and the model of direct implementation of international standards, exemplified by Albania. This diversity of approaches clearly testified to the absence of a global consensus regarding the optimal balance between efficiency, accessibility, and the strength of legal remedies. The cybersquatting had a pronounced anti-competitive effect, creating the so-called "cyber-inequality" and disproportionately affecting small and medium-sized enterprises, which, unlike large corporations, did not have either financial resources or staff lawyers for prolonged and costly protection of the digital assets. Based on the obtained results, a number of practical recommendations were formulated. At the international level, it was proposed to consider the possibility of modernising UDRP policy by introducing mechanisms for more effective counteraction against repeat offenders, for example, through the creation of a public offenders' register, as well as expanding the range of possible sanctions. At the national level, states relying solely on international procedures should develop the own hybrid systems. Such an approach would not only provide businesses with access to national courts for recovering damages but also contribute to the formation of national judicial expertise in the field of digital law. Proactive measures also needed to be strengthened by expanding the functionality of such tools as the Trademark Clearinghouse (TMCH) and introducing stricter, possibly automated, verification

procedures at the stage of domain name registration, which would allow the prevention of a significant part of conflicts before these conflicts arose.

A limitation of this research was its predominantly theoretical and legal nature, based on the analysis of normative documents, policies, and analytical reports. The work did not include the collection of primary empirical data, such as surveys of business representatives or interviews with arbitrators. Accordingly, directions for further research could include a quantitative study of the economic losses of small and medium-sized businesses from cybersquatting in different jurisdictions for an accurate assessment of the scale of the problem. A promising direction was the analysis of the impact of new technologies, particularly generative artificial intelligence, on the tactics of cybersquatters.

REFERENCES

Ahammad, S.H., Kale, S.D., Upadhye, G.D., Pande, S.D., Babu, E.V., Dhumane, A.V., & Bahadur, D.K.J. (2022). Phishing URL detection using machine learning methods. *Advances in Engineering Software*, *173*, 103288. https://doi.org/10.1016/j.advengsoft.2022.103288

Albania constitution. (2025). https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-REF(2016)064-e

Almarzooqi, A., Mahmoud, J., Alzaabi, B., Ghebremichael, A., & Aldwairi, M. (2022). Detecting malicious domains using statistical internationalized domain name features in top level domains. In *14th Annual Undergraduate Research Conference on Applied Computing (URC), Dubai, United Arab Emirates* (pp. 1-6). IEEE. https://doi.org/10.1109/URC58160.2022.10054226.

Arkabaev, N., Rahimov, E., Abdullaev, A., Padmanaban, H., & Salmanov, V. (2025). Modelling and analysis of optimization algorithms. *Jurnal Ilmiah Ilmu Terapan Universitas Jambi,* *9*(1), 161-177. https://doi.org/10.22437/jiituj.v9i1.38410

Arnott, J.A. (2014). Navigating cybersquatting enforcement in the expanding internet infrastructure. *UIC law review: Intellectual property law, 13*(2), 324-340.

BBC News. (2016). *Michael Jordan wins trademark case in China's top court.* https://www.bbc.com/news/world-asia-38246196

Binhammad, M., Alqaydi, S., Othman, A., & Abuljadayel, L.H. (2024). The role of AI in cyber security: Safeguarding digital identity. *Journal of Information Security*, *15*(02), 245-278. https://doi.org/10.4236/jis.2024.152015

Buletsa, S.B., & Tegza, A.V. (2022). Cybersquatting as a violation of intellectual property rights. *Uzhhorod National University Herald Series Law*, *67*, 59-63. https://doi.org/10.24144/2307-3322.2021.67.11

Bush, S., DeLorenzo, M., Tieu, P., & Rajendran, J. (2025). Free and fair hardware: A pathway to copyright infringement-free verilog generation using LLMs. In *62nd ACM/IEEE Design Automation Conference (DAC), San Francisco, CA, USA* (pp. 1-7). IEEE. https://doi.org/10.1109/DAC63849.2025.11132658.

Chaisse, J., & Friedmann, D. (2024). Law of the digital domain: Trademarks, domain names, and the AI frontier. *IDEA: The Law Review of the Franklin Pierce Center for Intellectual Property, 64*(2), 399-455.

Congress.gov. (1995). *Federal Trademark Dilution Act of 1995.* (1995). https://www.congress.gov/bill/104th-congress/house-bill/1295

Congress.gov. (2025a). *Fourteenth Amendment. Constitution of the United States.* https://constitution.congress.gov/constitution/amendment-14/

Congress.gov. (2025b). *Fifth Amendment. Constitution of the United States.* https://constitution.congress.gov/constitution/amendment-5/

Cornell Law School. (1914). *Clayton Antitrust Act.* Legal Information Institute. https://www.law.cornell.edu/wex/clayton_antitrust_act

Cornell Law School. (2008). *Lanham Act*. Legal Information Institute. https://www.law.cornell.edu/wex/lanham_act

De Paula Castro, C.F., Silva, D.A.A., Souto, G.A., & De Medeiros Albrecht, N.F.M. (2022). Domain names and intellectual property: Reflections on dispute resolution from the perspective of Law and Economics. *GV Law Journal*, *18*(1), e2208. https://doi.org/10.1590/2317-6172202208

Federal Ministry of Justice and Consumer Protection. (2023). *Act on the protection of trade marks and other signs (Trade Mark Act – MarkenG).* Federal Office of Justice. https://www.gesetze-im-internet.de/englisch_markeng/

Federal Ministry of Justice and Consumer Protection. (2025a). *Basic Law for the Federal Republic of Germany.* Federal Office of Justice. https://www.gesetze-im-internet.de/gg/BJNR000010949.html

Federal Ministry of Justice and Consumer Protection. (2025b). *German Civil Code*. Federal Office of Justice. https://www.gesetze-im-internet.de/bgb/

Fedotova, I., Shersheniuk, O., Prokopenko, M., Britchenko, I., & Vazov, R. (2021). Management of a viable enterprise on the basis of the approach to management of a «living» organization and the concept of viable systems. In *Problems and Prospects of Development of the Road Transport Complex: Financing, Management, Innovation, Quality, Safety - Integrated Approach* (pp. 63-80). PC TECHNOLOGY CENTER. https://doi.org/10.15587/978-617-7319-45-9.CH5

Feng, S. (2025). Fair use of trademarks in Chinese law: A daunting defence to trademark infringement. *Queen Mary Journal of Intellectual Property*, *15*(2), 196-218. https://doi.org/10.4337/qmjip.2025.02.03

Hakiki, N., & Sanusi, S. (2023). Settlement of disputes over domain names ownership and cybersquatting in Indonesia and Singapore. *Student Journal of International Law*, *3*(1), 95-107. https://doi.org/10.24815/sjil.v3i1.24872

Hari, S.S., Porkodi, S., Saranya, R., & Vijayakumar, N. (2024). Intelligent model to improve the efficacy of healthcare content marketing by auto-tagging and exploring the veracity of content using opinion mining. *International Journal of Electronic Marketing and Retailing, 15*(2), 240-260. https://doi.org/10.1504/IJEMR.2024.136978

Huertas-García, Á., Martín, A., Huertas-Tato, J., & Camacho, D. (2023). Countering malicious content moderation evasion in online social networks: Simulation and detection of word camouflage. *Applied Soft Computing*, *145*, 110552. https://doi.org/10.1016/j.asoc.2023.110552

Imayani, I., Marbun, M., & Ananto, R.W. (2024). Legal protection for registered trademark holders against trademark infringement. *International Journal of Research and Innovation in Social Science*, *VIII*(I), 638-650. https://doi.org/10.47772/ijriss.2024.801049

Internet Corporation for Assigned Names and Numbers. (1999). *Uniform Domain-Name Dispute-Resolution Policy.* Contracted Parties. https://www.icann.org/en/contracted-parties/consensus-policies/uniform-domain-name-dispute-resolution-policy/uniform-domain-name-dispute-resolution-policy-01-01-2020-en

Internet Corporation for Assigned Names and Numbers. (2025a). *Trademark Clearinghouse (TMCH).* New Generic Top Level Domains 2012 Program. https://newgtlds.icann.org/en/about/trademark-clearinghouse

Internet Corporation for Assigned Names and Numbers. (2025b). *Uniform Rapid Suspension (URS)*. https://www.icann.org/en/contracted-parties/registry-operators/services/rights-protection-mechanisms-and-dispute-resolution-procedures/urs

Issayeva, A., Niyazbekova, S., Semenov, A., Kerimkhulle, S., & Sayimova, M. (2024). Digital technologies and the integration of a green economy: legal peculiarities and electronic transactions. *Reliability Theory and Applications, 19*(6), 1088-1096. https://doi.org/10.24412/1932-2321-2024-681-1088-1096

Jon, W., & Park, S. (2025). Comparative analysis of trademark protection in the metaverse and registration of virtual goods and NFTs. *Computer Law & Security Review*, *57*, 106137. https://doi.org/10.1016/j.clsr.2025.106137

Kerimkhulle, S., Turtkarayeva, G., Mussaibekov, R., Ospanova, N., Kuttykozhayeva, S., & Adalbek, A. (2025). Using Markov Chain Model to Forecasting of the Agricultural Industry Development. *Lecture Notes in Networks and Systems, 1489*, 148-158. https://doi.org/10.1007/978-3-031-96798-6_14

Kotukov, O., Karamyshev, D., Kotukova, T., Chernoivanenko, A., & Serenok, A. (2025). Can digital transparency tools systematically reduce corruption in government? Evidence from Estonia, Ukraine and Brazil. *Journal of Theoretical and Applied Information Technology, 103*(10), 4256-4257. https://www.jatit.org/volumes/Vol103No10/18Vol103No10.pdf

Laketić, J. (2024). Trademarks on the blockchain: NFT domains and collisions. *Michigan Technology Law Review*, *30*(2), 4. https://doi.org/10.36645/mtlr.30.2.trademarks

Lasisi, M., & Tembe, U. (2025). Digitization and Intellectual Property Right. In D. Baker and L. Ellis (Eds.), *Encyclopedia of Libraries, Librarianship, and Information Science* (pp. 140-146). Elsevier. https://doi.org/10.1016/B978-0-323-95689-5.00237-6

Limongelli, R., & Sposini, L. (2025). The (virtual) battle for intellectual property rights in the metaverse: The case of copyright, trademarks and the NFT technology. *Metaverse*, *6*(1), 3056. https://doi.org/10.54517/m3056

Ma, K., He, N., Huang, J., Zhang, B., Wu, P., & Wang, H. (2025). Cybersquatting in Web3: The Case of NFT. In *2025 IEEE 10th European Symposium on Security and Privacy (EuroS&P), Venice, Italy* (pp. 549-564). IEEE. https://doi.org/10.1109/EuroSP63326.2025.00038.

Moura, G. C., Müller, M., Davids, M., Wullink, M., & Hesselman, C. (2017). Domain names abuse and tlds: from monetization towards mitigation. In *2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)* (pp. 1077-1082). IEEE. https://doi.org/10.23919/INM.2017.7987441.

Mukhopadhyay, S., Mukherjee, J., Das, D., Chaudhuri, A.D., Sarkar, S., Chaudhuri, T.D., & Paul, K. (2025). Learning fuzzy decision trees for predicting outcomes of legal cases relating to intellectual property rights. *Applied Soft Computing*, *176,* 113179. https://doi.org/10.1016/j.asoc.2025.113179

National Archives. (1890). *Sherman Anti-Trust Act.* Milestone Documents. https://www.archives.gov/milestone-documents/sherman-anti-trust-act

Omarova, A.B., Taitorina, B.A., Yermekov, A.T., Doszhanov, B., Buribayev, Y.A., & Khamzina, Z.A. (2017). Application of international rules ensuring social rights of families and children in Kazakhstan. *Journal of Advanced Research in Law and Economics, 8*(1), 153-163. https://doi.org/10.14505/jarle.v8.1(23).17

Rajendran, B., & Palaniappan, G. (2022). A universal domain name resolution service-need and challenges-study on blockchain based naming services. In *2022 IEEE Region 10 Symposium (TENSYMP)* (pp. 1-6). IEEE. https://doi.org/10.1109/tensymp54529.2022.9864361

Ramsey, L. (2020). Using failure to function doctrine to protect free speech and competition in trademark law. *Iowa Law Review, 104,* 70-103.

Singh, J. (2025). Domain name dispute in the age of social media and e-commerce. *Indian Journal of Integrated Research in Law*, *5*(1), 634.

Smailov, N., Kadyrova, R., Abdulina, K., Uralova, F., Kubanova, N., & Sabibolda, A. (2025). Application of facial recognition technologies for enhancing control in information security systems. *Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Srodowiska, 15*(3), 55-58. https://doi.org/10.35784/iapgos.7073

Šutova, M., & Vlaškovic, K. (2022). European Court of Justice on the use of a previous trademark reputation in terms of infringement. In XVIII Majsko savetovanje (pp. 495–504). https://doi.org/10.46793/XVIIIMajsko.495S

TechCrunch. (2008) *GoDaddy uses standard tactics to warehouse domains.* https://techcrunch.com/2008/12/03/godaddy-uses-standard-tactics-to-warehouse-domains/

The Public Service for the Dissemination of Law. (2025). *Intellectual Property Code.* https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006069414/

Tomer, A., Daksh, A., Gautam, J. K., Prajapati, P., Tomer, A., & Singh, R. Enforcing Trademark Rights in the Digital Age: International Complications. In *2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE)* (pp. 1933-1939). IEEE. https://doi.org/10.1109/IC3SE62002.2024.10593334.

U.S. Government Publishing Office. (1999). *Anticybersquatting Consumer Protection Act. (ACPA).* Senate Report 106-140. https://www.govinfo.gov/content/pkg/CRPT-106srpt140/html/CRPT-106srpt140.htm

Uderbayeva, B. (2024). Legal aspects of the security of the Caspian region in light of the Russia-Ukraine conflict. In *Eurasian Legal Systems in a World in Transition: Economic prosperity or disparity, and the return of politics in international law* (pp. 267-278). Peter Lang AG.

University of Oslo. (1957). *Treaty on the Functioning of the European Union (TFEU).* The Faculty of Law. https://www.jus.uio.no/english/services/library/treaties/09/9-01/tfeu_cons.html

Vihikan, W.O., Mistica, M., Levy, I., Christie, A., & Baldwin, T. (2021). Automatic resolution of domain name disputes using machine learning. In *Proceedings of the Natural Legal Language Processing Workshop 2021* (pp. 228-238). Association for Computational Linguistics.

Wang, M., Zang, X., Cao, J., Zhang, B., & Li, S. (2023). PhishHunter: Detecting camouflaged IDN-based phishing attacks via Siamese neural network. *Computers & Security*, *138*, 103668. https://doi.org/10.1016/j.cose.2023.103668

Wibowo, S.H., Irawan, J.D., Wahyuddin, & Winardi, B. (2022). Cybercrime in the digital era.

World Economic Forum. (2025). *Global Cybersecurity Outlook 2025.* https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

World Intellectual Property Organization. (2021). *Law No. 9947 On Industrial Property, Albania.* https://www.wipo.int/wipolex/en/legislation/details/21588

World Intellectual Property Organization. (2025). *Initial report of the WIPO-ICA UDRP review project team.* https://www.wipo.int/export/sites/www/amc/en/docs/wipoicareportapril2025.pdf

Yale Law School. (1789). *Declaration of the Rights of Man – 1789*. Lillian Goldman Law Library. https://avalon.law.yale.edu/18th_century/rightsof.asp

Zhetpisbayev, B.A., Baisalova, G.T., Shadiyev, K.K., Khamzin, A.S., Buribayev, Y.A., & Khamzina, Z.A. (2017). Legal support of the process of Kazakhstan accession to the OECD: Potential for improving quality of individual's labour rights regulation. *Journal of Advanced Research in Law and Economics, 8*(7), 2302-2307. https://doi.org/10.14505//jarle.v8.7(29).31

The Law, State and Telecommunications Review / Revista de Direito, Estado e Telecomunicações

Contact:
Universidade de Brasília - Faculdade de Direito - Núcleo de Direito Setorial e Regulatório
Campus Universitário de Brasília
Brasília, DF, CEP 70919-970
Caixa Postal 04413

Phone: +55(61)3107-2683/2688

E-mail: getel@unb.br

Submissions are welcome at: https://periodicos.unb.br/index.php/RDET