

ÖZEL HUKUK/PRIVATE LAW

Araştırma Makalesi / Research Article

Domain Name Disputes and Dispute Resolution Methods for “.tr” Domain Names Under Turkish Law*

Alan Adı Uyuşmazlıkları ve Türk Hukukunda “.tr” Uzantılı Alan Adlarına İlişkin Uyuşmazlık Çözüm Yöntemleri

Zeliha KARAMAN-OKAY**

ABSTRACT

With the increasing global reliance on the internet, domain names have transformed from basic technical identifiers into valuable digital assets representing identity, brand equity, and commercial value. This transformation has also led to a rise in disputes, particularly when domain names conflict with pre-existing rights such as trademarks, personal names, trade names, or culturally sensitive terms. This article focuses on the legal remedies available in Turkish law for resolving domain name disputes. Although judicial remedies based on grounds such as trademark infringement, unfair competition or the unauthorized use of personal names are available, they are frequently criticized for being procedurally complex, time-consuming and financially burdensome. As an alternative, the study highlights the administrative procedure operated by Dispute Resolution Service Providers (DRSPs), which applies particularly to disputes involving domain names registered under the “.tr” country code top-level domain. These proceedings are conducted online, based solely on written submissions, and typically result in decisions within 45 days, though their scope is limited to cancellation, transfer, or retention of the domain name. The

* Makale gönderim tarihi: 13.04.2025. Makale kabul tarihi: 24.07.2025. Zeliha Karaman-Okay, “Domain Name Disputes and Dispute Resolution Methods for “.tr” Domain Names Under Turkish Law”, *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi*, Cilt 12, Sayı 2, 2025, ss. 792-826, DOI: <https://doi.org/10.46547/imuhfd.2025.12.2.4>

** Lecturer, Mehmet Akif Ersoy University Ağlasun Vocational School Department of Office Services and Secretariat, zkaraman@mehmetakif.edu.tr

Çatışma Beyanı: Yazar herhangi bir çatışma beyanı bildirmemiştir.

Conflict of Interest Statement: The author(s) have declared no conflict of interest.

Yazar Notu/Author Note: This article is based on the author’s master’s thesis titled *Internet Domain Name Disputes and Resolution Methods: A Comparative Analysis* and has been revised and expanded for academic publication.

article also analyzes the categories and root causes of domain name conflicts, offering a critical assessment of existing regulations and suggesting both individual and structural preventive strategies. It concludes that the evolving nature of domain name law necessitates ongoing legislative and procedural refinement in Turkey.

Keywords: Domain name disputes, .tr domain names, Dispute Resolution Service Providers, trademark infringement, Turkish internet law.

ÖZ

İnternet kullanımının küresel ölçekte yaygınlaşmasıyla birlikte, alan adları yalnızca teknik erişim araçları olmaktan çıkarak kimlik, marka değeri ve ekonomik anlam taşıyan dijital varlıklara dönüşmüştür. Bu gelişme, özellikle alan adlarının daha önce var olan marka, kişisel ad, ticaret unvanı veya kültürel açıdan anlamlı ifadelerle örtüşmesi durumunda çeşitli hukuki uyumsuzlukları beraberinde getirmiştir. Bu makalede, Türk hukukunda alan adı uyumsuzluklarının çözümüne yönelik mevcut hukuki yollar ele alınmaktadır. Marka hakkı ihlali, haksız rekabet veya kişisel adların izinsiz kullanımı gibi hukuki gerekçelerle yargı mercilerine başvuru mümkündür. Ancak bu yolların usul bakımından karmaşık, uzun süreli ve maliyetli olabildiği yönünde eleştiriler bulunmaktadır. Bu nedenle, özellikle “.tr” uzantılı alan adlarına ilişkin uyumsuzluklar bakımından alternatif bir yol olarak Uyuşmazlık Çözüm Hizmet Sağlayıcıları tarafından sunulan idari başvuru süreci incelenmektedir. Tamamen çevrimiçi yürütülen bu süreç yaklaşık 45 gün içinde sonuçlanmakta ve yalnızca alan adının iptali, devri veya korunması yönünde karar alınabilmektedir. Makalede ayrıca alan adı uyumsuzluklarının türleri ve nedenleri değerlendirilmekte, mevcut yasal düzenlemelerin yeterliliği eleştirel biçimde incelenmekte ve geleceğe yönelik önleyici önerilere yer verilmektedir. Sonuç olarak, alan adı hukukunun değişken yapısı dikkate alındığında, Türk hukukunun bu alanda sürekli bir yasal ve usuli güncellemeye ihtiyaç duyduğu vurgulanmaktadır.

Anahtar Kelimeler: Alan adı uyumsuzlukları, .tr uzantılı alan adları, Uyuşmazlık Çözüm Hizmet Sağlayıcıları, marka ihlali, Türk internet hukuku.

Introduction

In today's rapidly evolving digital landscape, the internet has transformed from a mere communication tool into a primary platform for promotion, representation, and commerce for both individuals and institutions.

Throughout this transformation, domain names, initially used for technical access purposes only, have become key components that represent digital identity, carry brand value, and generate economic impact. The registration of domain names identical or similar to personal names, trade names, trademarks, or culturally significant expressions has increasingly led to conflicts of interest, giving rise to legal disputes over domain name ownership.

As the use of domain names has grown globally, the number of related disputes has also increased significantly. However, it has become evident that the current legal framework often falls short in addressing these new and technically complex conflicts. This has highlighted the growing need for effective and accessible resolution mechanisms, whether through judicial channels or alternative administrative and online procedures.

This study adopts a systematic approach to examining the primary methods available under the Turkish legal system for resolving domain name disputes. It particularly focuses on the application procedure before Dispute Resolution Service Providers (*DRSPs*) concerning country code top-level domains ending in “.tr”. Compared to conventional judicial proceedings, applications made to DRSPs offer a more practical solution due to faster resolution times and lower costs. Nonetheless, the DRSP system is limited to issuing decisions regarding the cancellation, transfer, or maintenance of domain names. Therefore, parties seeking broader remedies such as injunctions, compensation, or public notice must still resort to judicial proceedings.

Another aim of this study is to classify the types and causes of domain name disputes within a doctrinal framework and to demonstrate, through examples, how such disputes may be addressed under various legal bases, including trademark protection, unfair competition, personal name rights, and trade name laws.

In conclusion, the study analyzes the existing legal regulations and practical applications in Turkey related to internet domain name disputes, particularly within the context of “.tr” domains. It evaluates the operation of both judicial and administrative resolution mechanisms and emphasizes the ongoing need for legal reform in this dynamic and evolving area.

I. Overview of Domain Name Disputes

The domain name system was originally developed to meet technical needs and, prior to widespread use of the Internet, had not been subject to any legal regulation¹. During the early stages of the system’s development, technical

1 David Lindsay, *International Domain Name Law ICANN and the UDRP*, Hart Publishing, Oxford, 2007, p. 95.

necessities were prioritized, and it was not anticipated that domain names could overlap with legally protected elements such as personal names, trade names, or trademark rights². Therefore, it was not foreseen that the Internet would eventually be used so extensively and intensively that it could lead to widespread rights violations³.

As the Internet gradually became commercialized, not only economic relationships but also legal structures began to evolve. Traditional legal norms have often proven insufficient to address the novel legal challenges arising in the digital environment⁴. Consequently, new types of disputes have emerged, particularly involving infringements of rights, with domain name disputes representing a considerable part of these conflicts⁵.

II. Causes of Domain Name Disputes

It is common for internet users to choose short, memorable, and descriptive words or phrases as domain names to enhance visibility and recognition⁶. However, it is frequently the case that the desired domain names have already been registered by other individuals or entities. In such situations, the individual may either negotiate with the current owner for a transfer, select a different domain name, or initiate judicial or administrative proceedings to obtain the desired domain. The process of recovering previously registered domain names from third parties is generally referred to as a “*domain name dispute*”⁷.

The most significant underlying cause of domain name disputes is the uniqueness of domain names, similar to IP addresses. Since each domain name can only be registered by one person or entity, conflicts of interest become inevitable, particularly when well-known trademarks, trade names, or personal names are involved⁸. The transformation of domain names from mere technical identifiers into elements that reflect a business’s digital identity and commercial value has further increased the frequency of such disputes⁹. Additionally, the significant reduction in domain name registration

2 Neval Okan, *Aç Reklamları ve Haksız Rekabet*, Seçkin Yayıncılık, Ankara, 2011, p. 4.

3 Lindsay, p. 95; Okan, p. 4.

4 Nurullah Bal, “İnternet Alan Adları ve İnternet Alan Adı Uyuşmazlıklarının Tahkim Yoluyla Çözümlemesi”, *Gazi Üniversitesi Hukuk Fakültesi Dergisi*, Volume 17, Issue 1-2, 2013, p. 315.

5 Bal, p. 315.

6 John Levine, Carol Baroudi, Margaret Levine-Young, *The Internet for Dummies*, 6th Edition, IDG Books Worldwide, Foster City, 1999, p. 7.

7 Robert Badgley, *Domain Name Disputes*, Aspen Law and Business, New York, 2002, p. 2.

8 Jean Bedord, *I’ve Got a Domain Name-Now What? A Practical Guide to Building a Website and Your Web Presence*, Happy About, Silicon Valley, 2008, p. 12.

9 Badgley, p. 3; Bedord, p. 12.

fees compared to earlier periods has contributed to the rise in disputes. While domain registration once required a payment of around 70 US dollars, competition in the domain industry has driven this cost below 10 dollars per year. This shift has led to a surge in speculative domain name registrations, encouraging bad faith conduct in the process¹⁰.

As domain names began to be seen not only as technical tools but also as economically valuable assets, this perspective prompted malicious actors to register names with high brand value and later attempt to sell them to the legitimate owners or competing businesses at inflated prices¹¹.

Because domain names serve both as technical addressing tools and as instruments of brand promotion, the dual nature of their function blurs the boundaries between trademarks and domain names. This ambiguity stems from the fact that the two systems are governed by different registration procedures¹². While trademarks are typically registered through national or geographically limited public institutions, domain names are managed by international private registrars. Thus, although a trademark may be protected at the national level, a domain name containing the same sign can be registered globally by a third party. As a result, under the “*first-come, first-served*” principle, domain names containing trademarks can be lawfully registered by individuals who are not the rightful owners, leading to legal disputes¹³.

Furthermore, the current structure of the domain name system does not provide adequate safeguards to protect the interests of parties who share the same name but operate in different sectors or geographical regions. For instance, once a business registers “*amazon.com*” it may also secure extensions like “*amazon.net*” and “*amazon.org*” thereby effectively preventing other legitimate right holders from using similar domain names¹⁴.

Due to the multilayered and global nature of the Internet, it is extremely difficult to define the causes of domain name disputes within a fixed and limited framework. Therefore, this study seeks to present a systematic overview of the most frequently encountered types of disputes in practice and to provide readers with an instructive perspective on their underlying causes.

10 Bedord, p. 12.

11 Fangfai Wang Faye, “Domain Name Management and Legal Protection”, *International Journal of Information Management*, Volume 26, Issue 2, 2006, p. 119.

12 Torsten Bettinger, Allegra Waddell, *Domain Name Law and Practice: An International Handbook*, 2nd Edition, Oxford University Press, London, 2015, p. 64.

13 Bettinger, Waddell, p. 119.

14 Jacqueline Lipton, *Internet Domain Names, Trademarks and Free speech*, Edward Elgar Publishing, Cheltenham 2010, p. 4, (Book).

III. Types of Domain Name Disputes

Disputes concerning domain names have become increasingly diverse and widespread in parallel with the global expansion of the internet and the rising economic value of digital assets. In the early stages of internet development, such disputes were mostly limited to basic rights violations, such as classic cybersquatting and typosquatting. However, they have since evolved into more sophisticated and multidimensional legal issues, including domain name espionage and domain name tasting. In recent years, the registration of not only trademarks but also personal names, geographical indications, and common expressions as domain names has broadened the scope of these disputes and significantly altered their nature. These developments indicate a shift from traditional trademark infringement-based disputes to more complex and unique legal conflicts.

Within the scope of this study, commonly encountered types of domain name disputes will be examined through a systematic approach. It must be emphasized, however, that these classifications are not absolute. Many disputes may overlap across multiple categories, and similar types of disputes may also be analyzed under different headings.

A. Classic Cybersquatting

Classic cybersquatting is a type of domain name dispute that has been observed since the early stages of the internet's widespread use and remains common today. In such cases, well-known trademarks, trade names, personal names, or other distinctive identifiers are registered as domain names by third parties who are not the owners. This is typically done based on the "*first come, first served*" principle, with the intent of later transferring the domain to the legitimate right holders in exchange for high fees. The United States Court of Appeals for the Second Circuit has defined this practice as the registration of famous trademarks by individuals who have no trademark rights, followed by attempts to sell them to the rightful owners for a high price¹⁵.

The actions of cybersquatters sometimes aim solely to generate economic profit through the resale of registered domain names. In other instances, they are used to create websites that generate advertising revenue. Accordingly, classic cybersquatting can manifest in various ways, including attempts to:

¹⁵ The case in which the definition of domain name cybersquatting was established is the lawsuit filed by Sport's Farm L.L.C. against Sportsman's Market, Inc. in 2000 (202 F.3d 489, 493 - 2d Cir.).

- Sell the registered domain name to the rightful owner at an inflated price
- Retain domain names anticipated to have high future economic value¹⁶.

One of the most well-known examples of such conduct is the case of *Intermatic Inc. v. Dennis Toeppen*. The defendant, Toeppen, registered domain names such as “Panavision.com” “Panaflex.com” and “Intermatic.com” and attempted to sell them to the rightful trademark owners. The court ruled that Toeppen’s conduct diluted the trademarks and obstructed the companies’ ability to operate online, ordering the transfer of the domain names to the plaintiffs¹⁷.

Similar disputes have also occurred in Turkey. In 1999, Mehmet Kahveci registered the domain name “akbank.com” thereby preventing Akbank from using it¹⁸. Akbank filed a complaint with the World Intellectual Property Organization (WIPO), which, in a 2002 decision, ordered the domain to be transferred to Akbank. It was later discovered that Kahveci had registered approximately 50 other domain names corresponding to well-known trademarks¹⁹.

In another Turkish case, involving Koçbank and the domain “kocbank.com” the registrant Hasan Yağız offered to sell the domain for 100,000 USD and published obscene content on the corresponding website²⁰. Koçbank applied to WIPO, which ruled in favor of Koçbank and ordered the transfer of the domain. Similarly, in 2015, Koç Holding A.Ş. initiated proceedings for the domains “kocgroup.com” and “kocgoup.org” alleging bad-faith registration. WIPO decided in favor of Koç Holding and ordered the transfer of both domain names²¹.

Over time, classic cybersquatting has extended to other platforms, particularly social media. Malicious actors have begun registering fake social media

16 Jeffrey Weidmann, “Evolving Property Rights in Domain Names”, *Law School Student Scholarship*, Volume 86, Issue 1, 2010, p. 6.

17 Weidmann, p. 3. Details of the decision can be accessed via the following link: <https://cyber.harvard.edu/property00/domain/IntermaticShort.html> (27.06.2025).

18 For details of the dispute, see: <https://www.wipo.int/amc/en/domains/search/case.jsp>; Case Number: D2001-1488 (10.04.2025).

19 Some of the domain names owned by Mehmet Kahveci include: uki.com, yapi.com, akpa.com, cebitas.com, cukurova.com, showtv.com, denizcilik.com, iktisat.com, vakif.com, turyat.com, cankurtaran.com, profilo.com, tekel.com, santeks.com, bilkont.com, tarmak.com, orsa.com, ulusoy.com, ziraat.com, transturk.com, yasar.com, tupras.com, and ulker.com.

20 For details of the dispute, see: <https://www.wipo.int/amc/en/domains/search/case.jsp>; Case Number: D2001-0849 (09.04.2025).

21 For details of the dispute, see: <https://www.wipo.int/amc/en/domains/search/case.jsp>; Case Number: D2015-1046 (10.04.2025).

accounts under the names of public figures. These accounts are used to publish defamatory content or are offered for sale to the actual individuals concerned, often accompanied by financial demands.

An illustrative example of this phenomenon is the lawsuit filed by Tony La Russa against Twitter in 2009. A fake Twitter account had been created under La Russa's name, complete with his photograph and personal information, creating the impression of an official profile. La Russa filed a lawsuit due to the publication of offensive and defamatory content. However, the case was withdrawn after Twitter promptly removed the account. This dispute highlights that social media platforms can also be exploited in ways similar to classic cybersquatting, thereby extending the scope of misuse beyond traditional domain names²².

B. Noncommercial Cybersquatting

Noncommercial cybersquatting refers to disputes arising from the registration of domain names containing trademarks, trade names, or distinctive signs by individuals who do not hold legitimate rights, and who do not seek direct financial gain. Although these actions may not aim to generate monetary profit, the unauthorized use of third-party rights still falls within the scope of “*cybersquatting*”²³.

Unlike classic cybersquatting, these disputes often do not reveal a clear element of bad faith. The registrants generally act under the pretext of freedom of expression, often claiming their intent is to criticize, evaluate, or raise social awareness. In this context, domain names may include suffixes such as “*sucks*” “*parody*” or “*fun*” thereby referencing a particular trademark while adopting a critical tone²⁴.

In such cases, the purpose and manner of use of the domain name play a decisive role. If the domain is used honestly and without misleading the public, courts often consider such use legitimate under the framework of freedom of expression. However, if the use creates confusion, harms the reputation of the trademark, or conveys misleading information, legal liability and infringement may arise.

22 Thomas Curtin, “The Name Game: Cybersquatting and Trademark Infringement on Social Media Websites”, *Journal of Law and Policy*, Volume 19, Issue 1, 2011, p. 357. For details of the dispute, see: <http://www.dmlp.org/threats/la-russa-v-twitter-inc#description> (12.04.2025).

23 Jacqueline Lipton, “Beyond Cybersquatting: Taking Domain Name Disputes Past Trademark Policy”, *Wake Forest Law Review*, Volume 40, Issue 4, 2005, p. 26.

24 When a domain name includes the suffix “*...sucks*,” it is generally intended to emphasize how bad the associated goods or services are; similarly, when suffixes like “*...parody*” or “*...fun*” are added, the aim is usually to mock or trivialize the subject in a humorous or sarcastic manner.

A landmark case in this context is *Bally Total Fitness Holding Corp. v. Faber*, which illustrates the judiciary’s approach to domain names used for criticism. The defendant, Andrew Faber, registered the domain name “*ballysucks.com*” and used the website as a platform for publishing customer complaints against the Bally fitness chain. The website included a disclaimer stating it was not the official site and offered practical information such as how to cancel memberships. Although the plaintiff claimed trademark infringement, dilution, and unfair competition and sought the website’s removal, the U.S. District Court for the Central District of California ruled that Faber’s actions lacked commercial intent and fell under the protection of free speech, ultimately dismissing the case²⁵.

On the other hand, some users register domain names under the guise of parody, satire, or criticism and rely on a “*parody defense*” in court²⁶. However, this defense is typically insufficient if the use tarnishes the commercial reputation of the trademark or creates confusion among the public.

One notable example is the lawsuit brought by *People for the Ethical Treatment of Animals Inc.* (PETA). The defendant, Doughney, registered the domain “*peta.org*” and used it to host content under the title “*People Eating Tasty Animals*” promoting the consumption of meat. PETA argued that the public associated the domain with them, which resulted in trademark infringement and reputational harm. The court rejected Doughney’s parody defense, concluding that the content harmed PETA’s brand and ordered the transfer of the domain²⁷.

In conclusion, while noncommercial cybersquatting may not directly aim at economic gain, when such use exceeds the limits of free expression or involves elements of bad faith, it can amount to trademark infringement. Therefore, judicial authorities carefully assess the purpose and context of the domain name registration and use in each individual case, applying content, context, and impact as key evaluative criteria.

C. Reverse Domain Name Hijacking

Reverse domain name hijacking refers to a type of dispute in which a party seeks to wrongfully acquire a domain name that is lawfully and legitimately owned

25 For details of the case, see: https://itlaw.fandom.com/wiki/Bally_Total_Fitness_v._Faber (12.04.2025).

26 Parody is an art form that aims to create a work by imitating a particular artistic style, person, or group, with the intention of highlighting and exaggerating their humorous or exaggerated aspects, either to criticize or simply to entertain.

27 For details of the case, see: <https://law.justia.com/cases/federal/appellate-courts/F3/263/359/533767/> (12.04.2025).

by another individual or entity²⁸. This often involves the filing of baseless or bad-faith complaints with dispute resolution bodies, typically by a trademark holder or someone claiming trademark rights, with the aim of coercing the rightful domain name owner into relinquishing the domain²⁹.

Such attempts are often characterized by the fact that the domain name in question predates the complainant's trademark registration. In many cases, the registrant has used the domain name for an extended period, without any malicious intent, and has derived either direct or indirect economic benefit from it. Given that the domain holder has a legitimate interest worthy of legal protection, these complaints are deemed bad faith attempts at reverse domain name hijacking.

A notable example of this type of case is the *healthwave.com* dispute between Personal Communication Systems, Inc. and CDN Properties Inc., resolved in 2014 by the World Intellectual Property Organization (WIPO). The complainant claimed to have registered the trademark "*Healthwave*" in 2012 and to be using it for cloud-based communication services. However, the respondent had registered the domain name in 2002 and was generating revenue through a pay-per-click (PPC) advertising model. The respondent also emphasized that the words "*health*" and "*wave*" were generic and that they held a legitimate right to the domain name. Despite the complainant proving that the domain name matched its trademark, the WIPO panel found no evidence of bad faith on the part of the respondent and dismissed the complaint, concluding that the complaint itself was filed in bad faith and constituted reverse domain name hijacking³⁰.

A similar case was brought in 2013 between M/s. Core Diagnostics and Herr Guenter Keul regarding the domain name *corediagnostics.com*. In that case, the complainant had registered the trademark in 2011, whereas the respondent had registered the domain in 2001. The respondent demonstrated long-term, legitimate use of the domain name and the absence of malicious intent. The panel rejected the complaint and found that the attempt amounted to reverse domain name hijacking³¹.

28 Reverse domain name hijacking is defined in Article 1, titled "*Definitions*," of the Rules for Uniform Domain Name Dispute Resolution Policy (RUDRP).

29 Sefer Oğuz, *İnternet Alan Adı (Domain Name) Haklarının Korunması*, 2. Bası, Seçkin Yayıncılık, Ankara, 2014, s. 318.

30 For details of the dispute, see: <https://www.wipo.int/amc/en/domains/search/case.jsp>; Case Number: D2014-0664 (10.04.2025).

31 For details of the dispute, see: <https://www.wipo.int/amc/en/domains/search/case.jsp>; Case Number: D2013-1238 (10.04.2025).

These rulings demonstrate that domain name dispute resolution mechanisms not only protect against bad-faith registrations but also serve to shield legitimate domain holders from vexatious or coercive legal tactics. Trademark holders should exercise caution when asserting rights over domain names that were registered prior to their own trademark registrations. Otherwise, even if acting under the pretense of trademark enforcement, they may be deemed to have acted in bad faith.

D. Disputes Between Legitimate Rights Holders

Domain name disputes are not limited to malicious registration attempts. They may also arise when each party involved holds a legally protectable interest or right over the same domain name. These types of conflicts differ from conventional cases of cybersquatting, as the registrant does not act in bad faith but rather relies on an objectively legitimate interest. At the core of these disputes lie conflicting claims by multiple parties to the same domain name.

In the real world, it is common for identical or similar names and identifiers to be used by different individuals or legal entities across various geographical regions or sectors. However, the requirement that every domain name be globally unique causes such overlapping rights to collide. In domain name systems governed by the “*first come, first served*” principle, priority is generally granted to the first applicant, which often leads to disputes even among legitimate rights holders³².

One representative example is the dispute over the domain name delta.com. Delta Air Lines Inc. operating in the airline industry, Delta Financial active in financial services, and DeltaComm, an internet service provider, each had valid interests in the name Delta. However, DeltaComm was the first to register for the domain. The domain was later transferred first to Delta Financial and subsequently to Delta Air Lines. This case typifies a priority conflict between equally legitimate parties³³.

A similar situation occurred in 1999 between Hasbro Inc. and Clue Computing Inc. Hasbro registered the Clue trademark for its board game and sought to acquire the domain name clue.com. However, the domain had already been legitimately registered and actively used by Clue Computing for many years. Hasbro filed a claim based on its trademark rights, requesting the domain’s transfer. The court rejected the claim, finding that the registrant’s long-standing use was

32 Lipton, *Book*, p. 1406; Bettinger, Waddell, p. 119.

33 Lipton, *Book*, p. 1406.

lawful, genuine, and free of bad faith. The court also noted that Hasbro failed to demonstrate that the domain created public confusion or misrepresentation³⁴.

In such cases, relying exclusively on the “*first come, first served*” principle may not always lead to fair and equitable outcomes. Therefore, the concept of a “*superior right*” should also be considered. While the first applicant may technically obtain registration, a more balanced assessment requires examining which party’s use better serves the public interest, as well as factors such as brand recognition, commercial reach, and societal visibility.

The Tea Rose Doctrine in United States law provides a helpful framework in this regard. Under this doctrine, a party who first uses a mark in good faith may have superior rights to a later trademark registrant³⁵. When both parties are acting in good faith, the resolution of the conflict should consider their business sectors, geographic markets, and the level of public awareness of their brands. Otherwise, simply prioritizing the first filer may result in outcomes that undermine fairness and justice.

In conclusion, domain name disputes between legitimate rights holders, although not involving bad faith, require careful legal evaluation and represent some of the most nuanced issues within internet law.

E. Disputes Involving Personal Names

The registration of personal names as domain names has led to various legal conflicts and constitutes a distinct category of disputes within domain name law. These conflicts typically arise when individuals’ names and surnames are registered as domain names by third parties, often without the knowledge or consent of the individuals concerned. Such practices may lead to infringements of personality rights, issues concerning the protection of public figures’ names, and disputes related to trademark law. Notably, these disputes are not confined to well-known public figures; they may also affect ordinary individuals³⁶.

There are diverse motivations behind the registration of domain names containing the names of famous individuals. These include registering the name for commercial purposes and offering it for sale at a high price, using the domain for parody or criticism, creating fan sites, or registering the domain

34 For details of the case, see: <https://law.justia.com/cases/federal/district-courts/FSupp2/66/117/2489238/> (12.04.2025).

35 Robert Nupp, “Concurrent Use of Trademarks on the Internet: Reconciling the Concept of Geographically Delimited Trademarks with the Reality of the Internet”, *Ohio State Law Journal*, Volume 64, Issue 2, p. 624.

36 For further information, see: Tamarah Belczyk, “Domain Names: The Special Case of Personal Names”, *Boston University Law Review*, Volume 82, Issue 25, 2002, pp. 485-523.

in good faith with the intent to attract attention or establish contact. While some instances of registration may be considered good faith use, in practice, registrations aimed at commercial gain and carried out in bad faith are more frequently encountered³⁷.

A classic example is the dispute over the domain name *juliaroberts.com*. The domain was registered in 1998 by a third party and subsequently became the subject of a dispute resolution proceeding before WIPO. The panel ruled in favor of Julia Roberts, concluding that the registrant held no legitimate right or interest in the domain name, which was then transferred to her³⁸.

A similar dispute occurred in 2016 between the globally known singer Lady Gaga (Stefani Germanotta) and Nancy Faralysz, the registrant of the domain name *ladygaga.mobi*. It was found that the registrant had registered not only Lady Gaga's name but also the names of several other celebrities, with the apparent intention of selling the domains for profit. The panel considered this clear evidence of bad faith and ordered the domain to be transferred to the complainant³⁹.

In Turkey, a comparable case involved the domain name *cemyilmaz.com*, associated with the well-known comedian Cem Yılmaz. The domain was registered in 1999 by Roman Club International, and the related website included images of Cem Yılmaz, giving the impression of an official website. In 2000, Cem Yılmaz applied for trademark registration of his name and initiated a WIPO dispute resolution proceeding. He argued that the registrant had no legitimate interest in the domain, that the domain name was confusingly similar to his name and trademark, and that it was registered in bad faith. The panel concluded that the domain should be transferred to Cem Yılmaz⁴⁰.

In disputes involving personal names, the core legal issue is the balance among personality rights, privacy, commercial reputation, and trademark protection. Key factors in resolving such disputes include the identity of the registrant, the purpose and manner of domain use, and the level of public recognition of the name in question. Particularly in cases where the name of a well-known person has been registered without consent and bad faith, panels may rule in favor of transferring the domain name to the rightful holder.

37 Belczyk, p. 522.

38 For details of the dispute, see: <https://www.wipo.int/amc/en/domains/search/case.jsp>; Case Number: D2000-0210 (10.04.2025).

39 For details of the dispute, see: <https://www.wipo.int/amc/en/domains/search/case.jsp>; Case Number: D2016-0298 (11.04.2025).

40 For details of the dispute, see: <https://www.wipo.int/amc/en/domains/search/case.jsp>; Case Number: D2000-1541 (11.04.2025).

F. Disputes Concerning Geographical Indications, Place Names, and Culturally Significant Names

Disputes regarding the registration of geographical indications, place names, and culturally meaningful names as domain names are generally more complex and ambiguous compared to other types of domain name disputes. The complexity arises from the fact that such names carry not only individual but also collective and public values. In the social, cultural, and historical context, it is not always clear which persons, institutions, or communities may legitimately claim rights over these names, which in turn makes the assessment of the legitimacy of domain name ownership more challenging.

One of the main sources of these disputes is the registration of well-known city names as domain names for the purpose of direct commercial gain, often leading to conflicts between local governments and private or commercial users. According to the “*first come, first served*” principle applied in the domain name system, many famous geographical names were registered early on by individuals or entities other than public authorities. As a result, governmental bodies have initiated legal proceedings or administrative dispute resolution mechanisms to reclaim such domain names.

Examples include domain names such as *berlin.com*, *madrid.com*, *dublin.com*, *london.com*, *munich.com*, and *paris.com*, which were registered by Easylink Services Corporation. These domains were used for providing tourism-related services such as hotel reservations, car rentals, and city guides, and therefore had a clear commercial purpose. In 2003, the Madrid City Council filed a complaint with the World Intellectual Property Organization (WIPO) regarding the domain name *madrid.com*. The complainant argued that “*Madrid*” was identical or confusingly similar to its registered trademarks and demanded the transfer of the domain name. The respondent countered that “*Madrid*” was a universal geographical term, incapable of trademark monopolization, and that no infringement had occurred. The WIPO panel agreed with the respondent and rejected the request for transfer, allowing the domain name to remain with the registrant⁴¹.

A similar case was seen in 2004 concerning the domain name *mexico.com*, where the decision also favored the domain name owner. These rulings demonstrate that the mere public nature of a place name does not grant absolute rights of use to public authorities, and that individual or

41 For details of the dispute, see: <https://www.wipo.int/amc/en/domains/search/case.jsp>; Case Number: D2002-1110 (11.04.2025).

commercial use of such names is legally protected as long as there is no evidence of bad faith⁴².

G. Typosquatting

Typosquatting refers to a widespread form of domain name abuse in which malicious actors register intentionally misspelled variations of domain names in anticipation of common typing errors made by internet users. These practices primarily target well-known brands or websites with high visitor traffic, diverting users to fraudulent websites and thereby posing serious threats to brand reputation and user security⁴³.

The methods employed by typosquatters typically include registering common misspellings of complex or frequently mistyped brand names (such as “*microsof.com*”), adding extra words or suffixes to legitimate domain names (like “*googleonline.com*”), removing or abbreviating parts of domain names (such as “*ytube.com*”), altering top-level domain extensions (e.g. replacing .com with .net), or creating visually deceptive lookalike domains (e.g. “*wwwgoogle.com*” instead of “*www.google.com*”) through the deliberate insertion or omission of punctuation marks or special characters⁴⁴.

The primary objective behind typosquatting is to redirect unsuspecting users to fake websites due to typographical errors, and to exploit the resulting web traffic for monetary gain through advertisements, data collection, or other malicious commercial activities. This not only harms users but also significantly undermines the commercial reputation, customer loyalty, and economic rights of legitimate brand owners⁴⁵.

A notable case related to this form of domain name abuse occurred in 2000 between Bargain Bid and Ubid Inc. While the plaintiff operated under the domain “*bargainbid.com*” the defendant registered “*barginbid.com*” differing by just one letter. The phonetic and visual similarities between the two domain names caused confusion among users, which the panel deemed an infringement of trademark rights, ultimately prohibiting the defendant from using the contested domain name⁴⁶.

42 For details of the dispute, see: <https://www.wipo.int/amc/en/domains/search/case.jsp>; Case Number: D2004-0242 (11.04.2025).

43 Bettinger, Waddell, p. 144.

44 Bettinger, Waddell, p. 144.

45 Bettinger, Waddell, p. 145.

46 For details of the case, see: https://itlaw.fandom.com/wiki/Bargain_Bid_v._uBid (12.04.2025).

Similar examples include variations of well-known trademarks such as “*phillipmorris.com*” and “*microsof.com*” derived from the established brands “*phillipmorris.com*” and “*microsoft.com*” respectively. These lookalike domains were used to siphon off traffic and generate unjust profits for the registrants. The prevalence of typosquatting has been empirically demonstrated in a 2010 study by Moore and Edelman. Their research found that an average of 281 typographical variants were registered for each of the popular websites examined, including “*google.com*” “*youtube.com*” “*myspace.com*” “*freecreditreport.com*” and “*hotels.com*” In total, over 938,000 domain names were identified as being used for typosquatting purposes. Remarkably, a single individual was found to own approximately 1.8 million domain names, of which 1,100 infringed upon the Dell trademark⁴⁷.

In Turkey, a similar dispute arose between the owner of the domain “*gecce.com*” and a registrant of “*egedegece.com*.” The plaintiff argued that “*gecce*” was a registered trademark under which it was well known, and the visual and phonetic similarities between the domain names were likely to mislead consumers. The court, recognizing the plaintiff’s prior rights, ruled in favor of cancelling the contested domain name registration and removing it from the registry⁴⁸.

In conclusion, typosquatting is recognized as one of the most common forms of trademark infringement and unfair competition both in national legal systems and at the international level. Combating such abuses requires both strategic diversification of brand owners’ domain name registrations and the education of internet users to raise awareness of deceptive domain practices.

H. Domain Name Parking

Domain name parking refers to a form of domain name usage in which domains with high potential for user visits are registered not for the purpose of creating content or offering services, but rather for generating indirect advertising revenue. Although it constitutes a passive use, domain name parking possesses significant commercial potential, and thus requires careful legal evaluation⁴⁹.

47 For further information, see: Tyler Moore, Benjamin Edelman, *Measuring the Perpetrators and Funders of Typosquatting*, 14th International Conference on Financial Cryptography and Data Security, Tenerife, Spain, <http://www.benedelman.org/typosquatting/> (12.04.2025).

48 11th Civil Chamber, Case No. 2015/5104, Decision No. 2015/12014, Date: 30.12.2014; <https://karararama.yargitay.gov.tr/> (11.04.2025).

49 For further information, see: Johannes Zirngibl, Steffen Deusch, Patrick Sattler, Juliane Aulbach, Georg Carle, Mattijs Jonker, “Domain Parking: Largely Present, Rarely Considered!”, *Proc. of Network Traffic Measurement and Analysis Conference*, (TMA. 22, 2022), IFIP.

In practice, the process typically begins with the registration of a domain name that is likely to attract traffic. This domain is then directed, usually via intermediary service providers offering domain parking services, to a website that contains no original content but only advertising links. When visitors are redirected to this parked page and click on these links, the advertising companies make payments to the parking service provider, who subsequently shares a portion of the revenue with the domain name holder.

When assessed in isolation, domain parking cannot be deemed unlawful *per se*. However, if the domain name incorporates third parties' trademarks, trade names, or other distinctive signs without authorization, this usage may result in legal consequences such as trademark infringement, unfair competition, or bad faith registration. Therefore, in evaluating the legality of such usage, not only the fact of parking itself but also whether the use interferes with the rights of others must be considered based on the specific circumstances of the case.

A significant example illustrating the potential misuse of domain name parking is the case of *Enterprise Holdings Inc. v. Domain Admin*, which was resolved in 2010 before the National Arbitration Forum (NAF). The dispute centered on the domain name “*enterprpise.com*” a typographical variant of the trademark “*Enterprise*”. The domain had been parked in a manner that redirected users to the claimant's direct competitors and to other parked pages containing advertisement-based content. It was established that revenue was generated from pay-per-click advertisements on these pages, and that such use had harmed the complainant's commercial reputation and economic interests. The panel concluded that the domain name had been registered in bad faith and ordered its transfer to Enterprise Holdings Inc⁵⁰.

In conclusion, although domain name parking in its essence is legally neutral, when it is carried out in a way that violates trademark rights or constitutes bad faith, it may lead to the cancellation of the domain registration or its transfer to the rightful holder. In each individual case, a careful assessment of how the domain name is used, the nature of the redirected content, and the existence of potential bad faith elements is essential.

I. Pay Per Click (PPC)

The Pay Per Click (PPC) model refers to the use of domain names not for the purpose of generating original content but rather for redirecting users to various commercial websites and earning income for each click made. In this

50 For details of the case, see: <https://www.adrforum.com/domaindecisions/1349808.htm> (12.04.2025).

model, domain names typically contain frequently searched keywords or bear a resemblance to well-known trademarks. The domain holder earns revenue whenever users click on advertisements displayed on the redirected pages⁵¹.

Legally, the PPC model is not considered inherently unlawful. However, when it is implemented by exploiting registered trademarks owned by third parties, it can lead to significant legal consequences. Such uses are generally evaluated within the scope of trademark infringement, bad faith registration, and unfair competition, and they pose risks of violating trademark owners' rights as well as misleading consumers.

A notable case that illustrates the legal implications of the PPC model is the 2010 dispute concerning the domain name "*googledoc.com*". The registrant, Ravi Mani, had acquired the domain and used it to redirect users to various commercial websites to generate revenue through PPC. Google Inc., the complainant, filed a complaint with the National Arbitration Forum (NAF), asserting that the domain name bore a high degree of similarity to its own trademark, was likely to cause confusion, and had been exploited to obtain unfair economic benefits through misuse of the brand. The panel found that the domain name "*googledoc.com*" indeed had a substantial resemblance to the Google Inc. trademark. It concluded that the registrant had used this similarity to generate commercial gain and that the domain had therefore been registered in bad faith. Consequently, the panel ordered the transfer of the domain name to Google Inc⁵².

In conclusion, although domain names operating under the PPC model are not always considered unlawful, if such usage infringes upon trademarks or commercial identifiers belonging to third parties, the domain holder may be deemed to have acted in bad faith. As a result, remedies such as cancellation of the registration or transfer of the domain to the rightful owner may be imposed. Therefore, the legitimacy of economic benefits obtained through PPC practices must be carefully evaluated in light of the specific facts and legal context of each case.

J. Domain Name Slamming

One of the common abuses encountered in the domain name system is known as "*domain name slamming*" a deceptive practice typically carried out by

51 For further information, see: Peter O'Connor, "Pay-per-Click Search Engine Advertising: Are Hotel Trademarks Being Abused?", *Cornell Hospitality Quarterly*, Volume 50, Issue 2, 2009, pp. 232-244.

52 For details of the case, see: <https://www.adrforum.com/domaindecisions/1349808.htm> (11.04.2025).

domain registrars or third parties acting on their behalf. In this form of fraud, trademark or domain name holders receive notifications that create a sense of urgency, suggesting that a specific domain name is about to be registered by another party. Such a registration request does not exist⁵³. Under pressure from the fabricated threat, the trademark owner is directed to a link where they are persuaded to initiate a domain name registration through a particular registrar, thereby falling into a scheme designed solely for financial gain.

The primary aim of this method is to induce the domain name holder to voluntarily complete the registration through a particular registrar and generate profit for the service provider. It is widely known that some registrars, particularly those based in China, frequently employ this tactic. In the event of such a situation, domain name holders generally have a few options. They may ignore the notification and refrain from taking any action⁵⁴. Alternatively, they may report the issue to the accredited registrar with which the domain is actually registered, or to the relevant authorities such as the Information and Communication Technologies Authority (ICTA). If necessary, legal proceedings may be initiated under the grounds of fraudulent activity.

These types of fraud schemes are often conducted through fake email notifications or correspondence designed to appear like official documents. Therefore, it is of utmost importance that domain name holders examine such communications with scrutiny and verify their authenticity.

A related tactic similar to domain name slamming is known as “*fake renewal reminders*” In this version of the fraud, domain name holders receive an email stating that their domain is about to expire, even though its registration period has not yet lapsed⁵⁵. The email includes a link prompting the user to extend their registration. If the domain name holder falls for the ruse and clicks the link, they may end up making an unnecessary payment or having their personal and financial data compromised.

In conclusion, domain name slamming and similar tactics are misleading and unlawful practices that exploit domain name holders’ lack of knowledge and unfamiliarity with digital procedures. In order to guard against such schemes, it is essential that all domain-related transactions are conducted only through accredited and trustworthy registrars. Additionally, any incoming communication should be carefully assessed with regard to its origin and content to ensure its legitimacy.

53 Bettinger, Waddell, p. 144.

54 Bettinger, Waddell, p. 144.

55 For further information, see: Wood, p. 28.

K. Domain Name Tasting

Domain name tasting refers to a practice that exploits the “*add grace period*” system within the domain name registration framework. This system allows for the cancellation of a domain name registration within a specific period, typically five days, following its initial registration, without any obligation to provide justification. The original intent of this grace period is to enable users to correct mistakes made during the registration process. However, this mechanism has been misused by malicious actors who exploit it as a means of commercial profit⁵⁶.

Within this framework, a large number of domain names with high traffic potential are registered temporarily at no cost. These domain names are then linked to advertising networks or pay-per-click (PPC) systems to generate revenue. Based on the performance data collected during the trial period, domain names with low-income potential are dropped before the grace period expires, while those that generate higher returns are registered permanently. As a result, the system transforms into a profit-driven testing strategy based on cost-benefit analysis.

Data on the prevalence of this practice reveals the extent to which domain name tasting has become a systematic activity. In an empirical study conducted by Coull and others, it was determined that approximately 66 percent of domain names registered in connection with current events were permanently retained after the five-day grace period, while the remaining were used solely for short-term testing. These findings indicate that domain name tasting has evolved from a purely technical adjustment mechanism into an economically motivated strategy⁵⁷.

In conclusion, although domain name tasting may initially appear as a convenient technical feature, it carries a significant risk of misuse. When such systemic gaps are used as instruments for commercial exploitation, the result can be the infringement of trademark rights and a broader erosion of trust in the domain name system as a whole. Therefore, legal measures should be taken to restrict domain name tasting against malicious use, in order to preserve the integrity of the system and ensure the effective protection of intellectual property rights. Following the analysis of the types and causes of domain name disputes, it is essential to evaluate the legal remedies available for resolving such disputes.

56 Scott Coull, Andrew White, Ting-Fang Yen, Fabian Monrose, Michael Reiter, “Understanding Domain Registration Abuses”, *Computers & Security*, Volume 31, Issue 7, 2012, p. 810.

57 Coull, White, Yen, Monrose, Reiter, p. 810.

Depending on the nature of the conflict, the legal standing of the parties, and the extent of protection sought, various legal and administrative avenues can be pursued. The primary dispute resolution methods available under Turkish law will be systematically addressed in the subsequent section.

IV. Legal Remedies Available under Turkish Law for Domain Name Disputes

Due to the inherently transnational nature of the internet, disputes arising in this sphere often extend beyond the traditional jurisdictional boundaries of nation-states. In this context, the need for a uniform, globally applicable framework for resolving domain name disputes has long been discussed at the international level. However, a universally binding consensus applicable to all states has yet to be achieved. Consequently, existing solutions and regulations have predominantly remained confined to national or regional domains.

At present, many countries around the world have developed and implemented their own mechanisms for resolving internet domain name disputes within the framework of their domestic legal systems. These mechanisms include judicial, administrative, and alternative dispute resolution (ADR) pathways. The applicability and implementation of such mechanisms depend largely on the specific legal system of each country and the type of domain name at issue.

This section focuses on the mechanisms adopted within the Turkish legal system for resolving internet domain name disputes. Under Turkish law, there are three primary methods available to resolve such disputes:

- 1. Resolution through Mutual Agreement:** The dispute may be resolved through negotiation and settlement between the parties involved.
- 2. Judicial Proceedings before National Courts:** Parties may initiate litigation before general courts and seek judicial adjudication of the dispute.
- 3. Application to Domain Name Dispute Resolution Service Providers (UÇHS):** Within the framework of the *Internet Domain Names Regulation* and the *Communiqué on Dispute Resolution Mechanisms*, an administrative ADR process may be initiated.

The following sections will provide a detailed analysis of these three mechanisms, examining their legal foundations and practical applications through illustrative case studies.

A. Resolution through Mutual Agreement

One of the fastest, most cost-effective, and practical methods available for resolving domain name disputes is for the parties to settle the conflict directly through negotiation and mutual agreement. This approach offers significant advantages, particularly in avoiding time delays, high litigation costs, and legal uncertainties commonly associated with judicial proceedings.

Technical access to information related to the disputed domain name is generally possible. Through the WHOIS database, which is part of the domain name registration system, the identity details of the individual or entity to whom the domain name is registered can be accessed. This allows the parties to establish direct communication, thereby increasing the possibility of reaching an amicable settlement⁵⁸.

A frequently encountered scenario in practice involves domain names being registered by malicious third parties who then offer to transfer the domain name to the rightful owner in exchange for a high payment. This situation typically arises during the registration of domain names that include registered trademarks or trade names, placing the actual rights holders in a difficult position. The rightful holder may choose to acquire the domain name at the proposed price, or alternatively, assert their rights through administrative dispute resolution mechanisms or by initiating judicial proceedings.

Although resolving a dispute through mutual agreement can expedite the process and save time for both parties, it also carries the risk of rewarding bad-faith registrations and speculative profit-seeking behaviors. Therefore, in our opinion, this method should only be regarded as a “*last resort*” to be considered when other legal remedies prove ineffective or when specific circumstances justify such a resolution.

B. Resolution through Judicial Proceedings

Although there is no uniform and domain name-specific regulation under Turkish law, such disputes can nevertheless be resolved before judicial

⁵⁸ The Whois database can be accessed at <http://www.whois.com/> (11.04.2025). It should be noted that the General Data Protection Regulation (GDPR) of the European Union has had a significant impact on the operation of the WHOIS system managed by ICANN. The GDPR's strict requirements concerning the processing of personal data have led to substantial changes in the public accessibility of domain name registrants' information. As a result, ICANN adopted interim measures to limit public WHOIS data in order to ensure compliance with data protection standards. While this issue falls somewhat outside the primary focus of this article, it is nevertheless an important dimension of the broader debate surrounding WHOIS and data privacy. See: ICANN, 'Approved Resolutions Special Meeting of the ICANN Board – 17 May 2018' (17 May 2018) <https://www.icann.org/en/board-activities-and-meetings/materials/approved-resolutions-special-meeting-of-the-icann-board-17-05-2018-en> (27.06.2025).

authorities within the framework of existing general and special legal provisions. In particular, cases involving trademark infringement, damage to commercial reputation, violation of personality rights, and bad-faith registrations constitute the primary types of disputes that may be brought before the courts⁵⁹.

Where domain names are used unlawfully, the rightful owner may bring a lawsuit before the competent court seeking the cancellation of the domain name, its transfer, the cessation of its use, and compensation for material and moral damages. This right of action applies both to generic top-level domains (*gTLDs*) and country-code top-level domains (*ccTLDs*), such as domain names ending in “.tr”.

Under Turkish law, the main legal grounds invoked in domain name disputes are as follows:

- **Trademark Law:** Domain name uses that create a likelihood of confusion with or infringe on registered trademarks are protected under the Industrial Property Code No. 6769.
- **Unfair Competition Law:** Pursuant to Articles 54 et seq. of the Turkish Commercial Code (*TCC*), domain name uses that violate the principle of good faith, are misleading, or damage the commercial reputation of third parties are considered acts of unfair competition.
- **Personality Rights:** In cases where real person names are registered as domain names without consent, legal action may be brought under Articles 24 and 25 of the Turkish Civil Code.
- **Limits of Freedom of Expression:** Domain names used for criticism or parody purposes are assessed within the scope of freedom of expression. However, this freedom does not extend to bad-faith uses.

Judicial authorities evaluate domain name disputes by considering all the circumstances of the case, including the parties’ good or bad faith, the manner of domain name usage, the trademark registration date, and the degree of public recognition of the mark.

The core legal grounds for initiating legal proceedings in domain name disputes under Turkish law include:

- **Industrial Property Code No. 6769** (notably Articles 7 and 150),
- **Turkish Commercial Code (TCC):** Articles 39 et seq. (trade names and business names), Articles 54 et seq. (unfair competition),

⁵⁹ Oğuz, p. 335.

- **Turkish Code of Obligations (TCO):** Article 57 (general provisions on tort liability),
- **Turkish Civil Code (TCC):** Article 26 (protection of names).

When a domain name is registered and misused in a way that coincides with or resembles another's trademark, trade name, business name, or personal name, it is possible to initiate judicial proceedings on the basis of the provisions listed above. In such cases, if a specific provision exists, it should be applied first; otherwise, general provisions shall apply.

1. Filing a Lawsuit Concerning Domain Names under Trademark Law

In cases where domain names conflict with registered trademarks, it is possible to initiate legal proceedings under the provisions of the Industrial Property Code No. 6769. In this context, the unauthorized or confusingly similar use of a registered trademark as a domain name may constitute trademark infringement, entitling the trademark holder to seek judicial protection against the violation⁶⁰.

According to the Industrial Property Code, a sign must be registered before the Turkish Patent and Trademark Office in order to be protected as a trademark, and such protection is effective as of the filing date. Trademark registration grants the holder the exclusive right to use the mark in connection with certain designated goods or services. If a domain name is used in a manner that is identical or confusingly similar to a registered trademark, particularly within the same category of goods or services, the trademark owner may have grounds for a legal claim.

The Code enumerates specific acts that constitute trademark infringement, including the use of a trademark or a confusingly similar sign as a domain name without the consent of the trademark owner. In such cases, the trademark holder may request the prohibition of the domain name's use, the cessation of the infringement, and compensation for material and moral damages.

Accordingly, the trademark provisions serve as one of the most effective judicial remedies against the misuse of domain names.

2. Filing a Lawsuit Concerning Domain Names under Unfair Competition Provisions

In cases where non-registered trademarks, trade names, business names or other distinctive identifiers are misused as domain names, one of the most

60 For further information, see: Tamer Soysal, *İnternet Alan Adı Hukuku (Domain Name Law)*, Adalet Yayınevi, Ankara, 2014, p. 779; Oğuz, p. 342, Okan, p. 98.

effective legal remedies is found in the provisions on unfair competition regulated under Articles 54 to 63 of the Turkish Commercial Code No 6102. Especially for enterprises operating in the digital environment, the fact that domain names serve a promotional function similar to trademarks makes these provisions directly applicable to domain name disputes⁶¹.

According to Article 54 of the Turkish Commercial Code, any commercial practice that contradicts the principle of good faith constitutes unfair competition. Within this scope, using a distinctive sign that belongs to another person, such as a trade name or business name, as a domain name may be considered an act of unfair competition if it causes confusion among consumers, exploits brand recognition for unjust gain, or diverts internet traffic⁶².

In such cases, the injured party may, pursuant to Articles 56 and subsequent articles of the Code, request the prohibition of the domain name's use, its cancellation or transfer, as well as claim compensation for both pecuniary and non-pecuniary damages. Furthermore, ancillary claims such as requests for preliminary injunctions and the publication of the judgment may also be submitted to the court.

Therefore, with the increasing commercial value of domain names, the provisions on unfair competition offer a wider scope of protection beyond trademark law, enabling legal recourse even for unregistered commercial signs.

3. Judicial Resolution of Domain Name Disputes Based on Trade Names under Article 52 of the Turkish Commercial Code

Disputes arising between domain names and trade names or business names have become increasingly common, particularly due to the growing importance of distinctive signs in the digital environment. According to Articles 39 et seq. of the Turkish Commercial Code No. 6102, trade names, business names, and other distinctive identifiers are afforded legal protection when they are likely to be confused with a domain name, and this protection is grounded in Article 52 of the Code.

Pursuant to Article 52, if a trade name is used unlawfully, the owner of that name may request the termination of such use. Depending on the specific nature of the dispute, the trade name holder may also seek the cancellation or judicial transfer of the domain name. This legal protection is significant not

61 For further information, see: Seniha Dal, “Türk Hukukunda İnternet Alan Adları (Domain Names) ve Bu Alandaki Son Gelişmeler”, *Marmara Üniversitesi İktisadi ve İdari Bilimler Dergisi*, Volume 28, Issue 1, 2010, pp. 479-497.

62 Okan, p. 100.

only for those who possess a registered commercial enterprise, but also for individuals who actively use a trade name yet have not secured it as a domain name.

Judicial authorities assess these disputes on a case-by-case basis, taking into account factors such as the trade name's recognition, duration of actual use, commercial activity sector, and the nature of the domain name usage. If a domain name closely resembles a trade name to the extent that it causes confusion and damages commercial reputation, courts generally afford broad protection to the trade name holder under Article 52 of the Turkish Commercial Code.

In this regard, the legal relationship between a trade name and a domain name extends beyond mere similarity of expression and directly impacts branding, customer acquisition, and competitive advantage in the digital sphere. Consequently, the misuse of a trade name as a domain name gives rise to a unique type of legal dispute that involves not only issues of unfair competition, but also the proprietary rights associated with the trade name.

4. Judicial Protection against the Use of Personal Names as Domain Names under Article 26 of the Turkish Civil Code

The registration of individuals' names and surnames as domain names by third parties in the digital environment can constitute a violation of personality rights protected under the Turkish Civil Code. The right to a person's name, as covered by Article 26 of the TCC, represents a reflection of the broader right to personality. Where a name is used unlawfully, the rightful holder may request the cessation of the violation and the elimination of its consequences⁶³.

The requirement for uniqueness in domain name systems means that the bad-faith registration of personal names may undermine individuals' rights to be recognized and represented online. Article 26 not only allows courts to prevent continued infringement but also permits claims for pecuniary and non-pecuniary damages if the violation was committed with fault.

The scope of name protection is not limited to official names and surnames but extends to nicknames, distinctive stage names, and names publicly associated with a specific individual. Similarly, trade or business names can be protected under the right to name where they are considered extensions of personal identity.

In this context, the unauthorized registration of a domain name containing someone else's name may not only violate data protection principles but

63 For further information, see: Hayr nnisa  zdemir, "T rk ve İsvi re Meden  Hukukunda Ad  zerindeki Hak ve Korunması", *Ankara  niversitesi Hukuk Fak ltesi Dergisi*, Volume 57, Issue 3, 2008, pp. 561-598.

also threaten the individual’s digital and social existence. In assessing such disputes, courts evaluate factors including the purpose of use, the level of public recognition, the public perception of the name, and the presence of bad faith⁶⁴.

It should be noted that legal protection in domain name disputes is not limited to specific provisions related to trademarks, unfair competition, trade names, or names. The dynamic and multilayered nature of the internet leads to disputes that often require broader legal approaches. Depending on the specific facts of a case, claims may also be based on general tort provisions under the Turkish Code of Obligations, the Law on Intellectual and Artistic Works in cases of copyright infringement, the Turkish Penal Code in cases involving cybercrime or fraud, or the Law on the Protection of Personal Data if personal information is disclosed through the domain name.

Accordingly, the resolution of domain name disputes should not rely solely on predetermined legal norms. Instead, the most suitable and comprehensive legal framework must be identified based on the nature and specifics of each individual dispute.

C. Application to the Domain Name Dispute Resolution Service Provider

The procedural and financial challenges associated with traditional litigation have increased the demand for faster and more cost-effective methods of dispute resolution. This development has led to the growing significance of alternative dispute resolution mechanisms, particularly in the context of domain name disputes. In this regard, online dispute resolution procedures specifically designed for domain name conflicts have gained prominence, particularly due to their arbitration-like structure.

At the international level, the most widely applied model is the system based on the Uniform Domain Name Dispute Resolution Policy (*UDRP*), developed by the Internet Corporation for Assigned Names and Numbers (*ICANN*). Commonly referred to as “*ICANN arbitration*” in practice, this model differs from conventional arbitration in several respects, yet offers a fast, online, and binding dispute resolution mechanism⁶⁵.

64 For further information, see: Soysal, p. 943; Oğuz, p. 338.

65 For further information, see: Paul Torremans, *Research Handbook on Cross-Border Enforcement of Intellectual Property Research Handbooks in Intellectual Property Series*, Edward Elgar Publishing, United Kingdom, 2014, p. 644; Savaş Bozbel, *İnternet Alan Adlarının (Domain Names) Korunmasında ICANN Tahkim Usulü*, Seçkin Yayıncılık, Ankara, 2006, p. 67; Badgley, p. 3-5; Lipton, p. 35.

Rather than directly adopting this model, Turkey has implemented a specific system tailored for country-code top-level domains (*ccTLDs*) under its national legislation. This mechanism has been established under the Internet Domain Names Regulation and the Communiqué on Internet Domain Names (Dispute Resolution Mechanism), published in the Official Gazette No. 28742 on 21 August 2013. Accordingly, domain name disputes related to “.tr” extensions are resolved through applications made to Dispute Resolution Service Providers (*DRSPs*), authorized by the Information and Communication Technologies Authority (*ICTA*).

This system applies exclusively to domain names with the “.tr” extension and does not cover generic top-level domains (*gTLDs*). The dispute resolution process is conducted online via the *DRSPs* authorized by *ICTA*. It provides right holders with an administrative, rapid, and cost-effective means of applying for remedies such as the cancellation or transfer of domain names.

Compared to traditional judicial proceedings, applications made to Dispute Resolution Service Providers offer a more accessible and efficient alternative. The process is entirely document-based, conducted online without hearings, and the appointed arbitrator is required to issue a decision within ten days from the date of appointment. The decisions rendered may result in the domain name being cancelled, transferred to the rightful owner, or remaining with its current holder. Due to its speed and simplicity, the mechanism has increasingly been accepted in practice as a user-friendly solution.

However, it must be emphasized that the authority of the Dispute Resolution Service Providers is limited to decisions concerning the legal status of the domain name. It does not extend to awarding pecuniary or non-pecuniary damages, which fall within the jurisdiction of judicial courts. This clearly demonstrates that the mechanism is administrative in nature and does not possess the full scope of judicial authority.

1. Application to a Dispute Resolution Service Provider under the Communiqué on the Domain Name Dispute Resolution Mechanism

A party wishing to initiate a domain name dispute resolution process may submit an application through the website of a Dispute Resolution Service Provider (*DRSP*) of their choice, provided that the conditions specified in the first paragraph of Article 25 of the Regulation are met simultaneously⁶⁶. The *DRSP* has the authority to assess the admissibility of the application and may

66 This section has been prepared with reference to the Communiqué on the Internet Domain Name Dispute Resolution Mechanism.

reject it on grounds such as lack of capacity. In such cases, a notice of acceptance or rejection is to be delivered to the complainant within one business day. Until the complainant receives a response regarding their application, they may not apply to another DRSP concerning the same dispute. Additionally, it is permissible to submit a single application covering multiple domain names registered under the same holder.

The complainant must clearly state in the application whether the dispute is to be resolved by a single arbitrator or by three-member arbitrators. The application must also include the following: contact details of the applicant and, if applicable, his representative; the disputed domain name (DND); a request for the cancellation or transfer of the DND; supporting information, evidence, and legal grounds not exceeding 5,000 words; any other documents required by the DRSP; information as to whether any prior application has been made to another DRSP or a court concerning the same matter, and if so, the outcome of such proceedings; and a declaration that the information provided is accurate and complete. After submission, the complainant may provide additional information or documents; however, whether these will be considered is at the discretion of the arbitrator or arbitrators.

If the DRSP detects any deficiency in the application, it must notify the complainant and grant five days to rectify it issue. Failure to correct the deficiency within this period shall cause the application to be deemed invalid; however, this does not preclude the complainant from submitting a new application. Upon acceptance of the application, the DRSP shall immediately notify TRABIS (the .tr Network Information System) and the relevant registrar. A public announcement concerning the disputed domain name is then made, and the domain name is temporarily suspended.

In domain name disputes involving “.tr” extensions, the resolution procedure proceeds in accordance with the following steps⁶⁷:

Filing an application with a Dispute Resolution Service Provider (DRSP), developed specifically for resolving domain name disputes, constitutes an alternative online dispute resolution method conducted by arbitrators, offering a faster, more cost-effective, and user-friendly option compared to traditional litigation.

Within the framework of an application to a DRSP, the average dispute resolution period is estimated to be approximately 45 days. However, the authority of the arbitrator is limited to deciding on the transfer or cancellation

⁶⁷ This chart has been prepared with reference to the Communiqué on the Internet Domain Name Dispute Resolution Mechanism.

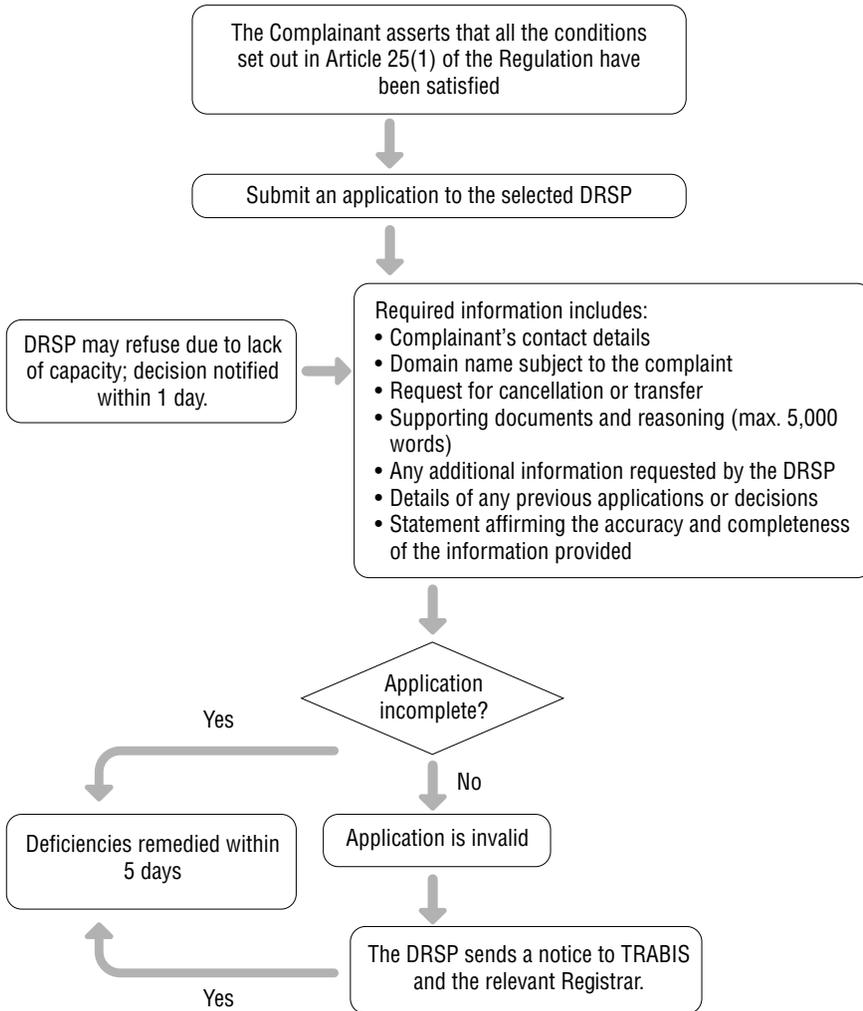


Figure 1. Application for Domain Dispute Resolution

of the domain name or rejecting the application. In contrast, judicial authorities have the power to issue broader and more enforceable remedies in cases involving the unlawful use of a domain name, including:

- Granting interim injunctions,
- Awarding pecuniary and non-pecuniary damages,
- Order for the recovery of attorney's fees,
- Publication of the judgment,
- Termination of the domain name's usage.

With the introduction of this new system, it is expected that domain name allocations based on the “*first come, first served*” principle will increase, which may lead to a rise in domain name disputes. In this context, inspired by international examples, the legislature has adopted the DRSP mechanism to ease the judiciary’s workload and provide parties with a more efficient, faster, and cost-effective remedy.

As a mechanism tailored specifically for country code top-level domains with the “.tr” extension, it is anticipated that this system will, in the near future, not only facilitate systematic dispute resolution but also significantly reduce the burden on judicial authorities. Furthermore, streamlining and accelerating the domain name allocation process is likely to contribute to the widespread use of “.tr” domain names, promote local digital production, and, indirectly, support the national economy.

D. Key Differences Between Judicial Proceedings and Application to Dispute Resolution Service Providers

Among the available avenues for resolving domain name disputes are judicial proceedings before courts and administrative resolution mechanisms provided by Dispute Resolution Service Providers (DRSPs). These two methods differ significantly in terms of procedural structure, scope of decision, procedural formalities, and legal consequences. The table below offers a comparative overview of the fundamental differences between these two resolution methods, serving as a guide to determine which option may be more appropriate in specific disputes.

Conclusion and Evaluation

Domain name law has emerged as a crucial field in the digital age, serving as a means of identity for individuals, corporations, and public institutions. With the increasing use of domain names, the legal disputes arising in this area have demonstrated that existing regulations are at times inadequate in addressing the realities of the digital world. In response to this need, the Turkish legal system has introduced both judicial and alternative dispute resolution mechanisms. Notably, the implementation of the DRSP procedure specifically for “.tr” domain names marks a significant advancement.

Nevertheless, to ensure the effective functioning of the domain name system and to promote fair, swift, and efficient resolution of disputes, the following recommendations should be considered:

Table 1.

Criteria	Judicial Route	Dispute Resolution Service Providers (DRSP)
Application Venue	Civil / Intellectual Property Courts	Authorized DRSPs (BTIDER, ISTAC, TOBB UYUM etc.)
Scope	Trademark rights, unfair competition, name protection, compensation claims, preliminary injunctions, etc.	Limited to cancellation, transfer, or reallocation of “.tr” domain names
Duration	Typically ranges from several months up to several years	Approximately 48 days on average; decisions usually issued within 10 days
Cost	Court fees, attorney fees, expert witness and discovery costs	Relatively low, fixed fees depending on the number of arbitrators
Jurisdiction / Outcome	Comprehensive rulings including compensation and other legal remedies	Binding decisions on domain name cancellation or transfer; no compensation awarded
Appeal / Review Possibility	Appeals, retrials, and other judicial review mechanisms available	Limited legal recourse: lawsuits can be filed against DRSP decisions, but no appeal mechanism
Decision-Making Process	Includes witness testimony, expert reports, discovery, and hearings	Based on evaluation of written documents only; no hearings conducted
Decision-Makers	Judge or panel of judges	Single arbitrator or three-member arbitration panel
Usage Scope	Applicable to all types of domain names and related legal disputes	Applicable only to “.tr” domain names
Legal Assurance	Full judicial review and extensive legal protections	Limited review; administrative and expedited dispute resolution process

- A specific legal framework for domain name disputes should be established, clearly defining the applicable rules in cases where domain names intersect with rights such as trademarks, trade names, and personal names.
- DRSP decisions should be standardized and aligned more closely with judicial precedents to enhance the system’s predictability.
- In dispute resolution procedures, the selection of arbitrators should be based on their technical and legal expertise, and decisions should be reasoned and transparently published.

- As the scope of domain name disputes expands, BTK should adopt a more proactive regulatory role and develop improved oversight and guidance mechanisms.
- Trademarks and distinctive signs should be registered as domain names at an early stage, and similar variations or combinations vulnerable to misuse should be proactively protected.
- Tools such as WIPO’s online trademark databases and alert systems should be used to detect potential infringements in advance, and legal consultation should be sought before domain name registration. However, in the context of Turkey, the practical use of such international tools remains limited due to low public awareness, absence of legal obligation, and the lack of integration with national systems like TRABIS. Therefore, strengthening local advisory mechanisms and increasing awareness among registrants and right holders are essential steps to prevent future disputes.

In light of these suggestions, it must be emphasized that the reform process in domain name law is not merely a technical issue but also a matter of protecting digital rights and ensuring digital security. The Turkish legal system must develop comprehensive, up-to-date, and practical solutions in this dynamic area, which is essential for strengthening international competitiveness and ensuring the sustainability of the digital economy. To achieve this, a multi-layered reform strategy should be adopted. This includes aligning TRABIS procedures with international best practices and ensuring their interoperability with WIPO mechanisms, introducing legal provisions that mandate pre-registration checks for potential trademark conflicts, expanding awareness and training programs and individual registrants, and establishing a centralized national watch system capable of detecting and preventing bad-faith domain name registrations in real time.

BIBLIOGRAPHY

- Badgley, Robert, *Domain Name Disputes*, Aspen Law and Business, New York, 2002.
- Bal, Nurullah, “İnternet Alan Adları ve İnternet Alan Adı Uyuşmazlıklarının Tahkim Yoluyla Çözümlemesi”, *Gazi Üniversitesi Hukuk Fakültesi Dergisi*, Volume 17, Issue 1-2, 2013, pp. 315-352.
- Bedord, Jean, *I’ve Got a Domain Name-Now What? A Practical Guide to Building a Website and Your Web Presence*, Happy About, Silicon Valley, 2008.
- Belczyk, Tamarah, “Domain Names: The Special Case of Personal Names”, *Boston University Law Review*, Volume 82, Issue 25, 2002, pp. 485-523.
- Bettinger, Torsten; Waddell, Allegra, *Domain Name Law and Practice-an International Handbook*, Second Edition, Oxford University Press, United Kingdom, 2015.
- Bozbel, Savaş, *İnternet Alan Adlarının (Domain Names) Korunmasında ICANN Tahkim Usulü*, Seçkin Yayıncılık, Ankara, 2006.
- Coull, Scott; White, Andrew; Yen, Ting-Fang; Monrose, Fabian; Reiter, Michael, “Understanding Domain Registration Abuses”, *Computers & Security*, Volume 31, Issue 7, 2012, pp. 806-815.
- Curtin, Thomas, “The Name Game: Cybersquatting and Trademark Infringement on Social Media Websites”, *Journal of Law and Policy*, Volume 19, Issue 1, 2011, pp. 353-394.
- Dal, Seniha, “Türk Hukukunda İnternet Alan Adları (Domain Names) ve Bu Alandaki Son Gelişmeler”, *Marmara Üniversitesi İktisadi ve İdari Bilimler Dergisi*, Volume 28, Issue 1, 2010, pp. 479-497.
- Faye, Fangfai Wang, “Domain Name Management and Legal Protection”, *International Journal of Information Management*, Volume 26, Issue 2, 2006, pp. 116-127.
- Levine, John; Baroudi, Carol; Young-Levine, Margaret, *The Internet for Dummies*, 6th Edition, IDG Books Worldwide, Foster City, 1999.
- Lindsay, David, *International Domain Name Law ICANN and the UDRP*, Hart Publishing, Oxford, 2007.
- Lipton, Jacqueline, “Beyond Cybersquatting: Taking Domain Name Disputes Past Trademark Policy”, *Wake Forest Law Review*, Volume 40, Issue 4, 2005, pp. 1-64.
- Lipton, Jacqueline, *Internet Domain Names, Trademarks and Free Speech*, Edward Elgar Publishing, Cheltenham, 2010.
- Moore, Tyler, Edelman, Benjamin, *Measuring the Perpetrators and Funders of Typosquatting*, 14th International Conference on Financial Cryptography and Data Security, Tenerife, Spain, <http://www.benedelman.org/typosquatting/> (12.04.2025).
- Nupp, Robert, “Concurrent Use of Trademarks on the Internet: Reconciling the Concept of Geographically Delimited Trademarks with the Reality of the Internet”, *Ohio State Law Journal*, Volume 64, Issue 2, 2003, pp. 617-658.
- O’Connor, Peter, “Pay-per-Click Search Engine Advertising: Are Hotel Trademarks Being Abused?”, *Cornell Hospitality Quarterly*, Volume 50, Issue 2, 2009, pp. 232-244.
- Oğuz, Sefer, *İnternet Alan Adı (Domain Name) Haklarının Korunması*, 2. Bası, Seçkin Yayıncılık, Ankara, 2014.
- Okan, Neval, *Ağ Reklamları ve Haksız Rekabet*, Seçkin Yayıncılık, Ankara, 2011.
- Özdemir, Hayrünnisa, “Türk ve İsviçre Medenî Hukukunda Ad Üzerindeki Hak ve Korunması”, *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, Volume 57, Issue 3, 2008, pp. 561-598.

- Soysal, Tamer, *İnternet Alan Adı Hukuku (Domain Name Law)*, Adalet Yayınevi, Ankara, 2014.
- Torremans, Paul, *Research Handbook on Cross-Border Enforcement of Intellectual Property Research Handbooks in Intellectual Property Series*, Edward Elgar Publishing, Cheltenham, 2014.
- Weidmann, Jeffrey, “Evolving Property Rights in Domain Names”, *Law School Student Scholarship*, Volume 86, Issue 1, 2010, pp. 1-29.
- Zirngibl, Johannes; Deusch, Steffen; Sattler, Patrick; Aulbach, Juliane; Carle, Georg; Jonker, Mattijs, “Domain Parking: Largely Present, Rarely Considered!”, Proc. of Network Traffic Measurement and Analysis Conference (TMA. 22, 2022), IFIP.