

		Science, Education and Innovations in the Context of Modern Problems Issue 9, Vol. 8, 2025	
		TITLE OF THE RESEARCH ARTICLE	
		Protection of the Electronic Address and Trademark in Electronic Commercial Transactions	
Tahraoui Soumia	Doctor of Philosophy in Philology Faculty of Law and Political Science, University of mscara Algeria E-mail: soumia.tahraoui@univ-mascara.dz		
	Faculty of Law and Political Science, University of mscara Algeria E-mail : souad.yahiaoui@univ-mascara.dz		
	Yahiaoui Souad		
	Faculty of Law and Political Science, University of mscara Algeria E-mail : souad.yahiaoui@univ-mascara.dz		
Issue web link		https://imcra-az.org/archive/383-science-education-and-innovations-in-the-context-of-modern-problems-issue-9-vol-8-2025.html	
Keywords		electronic address, trademark, electronic commercial transactions, infringement, priority of registration.	
Abstract			
Dealing via the Internet is considered one of the pillars of the digital economy, as most commercial companies have turned to adopting the method of electronic commerce in their dealings. This shift has provided them with the opportunity to promote goods and services in easier ways, at lower costs, and on an unlimited global scale. It has also enabled the electronic consumer to save time and effort through the diversity of offers and the ease of purchasing and payment via remote communication websites. Given the great importance represented by electronic websites, it became necessary to establish a means of access that connects the user or consumer with the company offering its products online. This means was embodied in the electronic address. Companies have chosen electronic addresses that bear their names or trademarks to distinguish their websites from those owned by competing companies. This situation has made the electronic address a target for many individuals and companies who rushed to register electronic addresses without having any legitimate right or interest in them, thereby infringing upon the rights of others. This has made it essential to explore the legal mechanisms established for their protection.			
Citation. Tahraoui S.; Yahiaoui S. (2025). Protection of the Electronic Address and Trademark in Electronic Commercial Transactions. <i>Science, Education and Innovations in the Context of Modern Problems</i> , 8(9), 1264–1281. https://doi.org/10.56334/sci/8.9.104			
Licensed © 2025 The Author(s). Published by Science, Education and Innovations in the context of modern problems (SEI) by IMCRA - International Meetings and Journals Research Association (Azerbaijan). This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).			
Received: 01.05.2025		Accepted: 12.08.2025	
		Publishing time: 22.09.2025	

Introduction

There is no doubt that conducting business over the Internet has become one of the main pillars of the digital economy. It is observed that most commercial companies are turning to adopt the method of electronic commerce, which has provided them with opportunities to promote goods and services in easier ways, at lower

costs, and on an unlimited global scale. It has also enabled electronic consumers to save time and effort through the diversity of offers and the ease of purchasing and payment via remote communication websites.

Given the great importance of electronic websites, it became necessary to establish a means of access that connects the user or consumer with the company offering its products online. At first, this access was represented by a set of numerical codes referring to the desired site. Thus, if a consumer wanted to access a particular company's website, they had to memorize the numbers indicating its address.

However, due to the difficulty of memorizing these numbers because of their length, complexity, and abundance, attention shifted to a new method — using a combination of letters that are easier for users to remember and use to reach the desired company's website. This method is known as the **electronic address (domain name)**. To make it easier for users to access their websites, companies and businesspeople have been keen to choose electronic addresses that carry their names or trademarks in order to distinguish their sites from those of competing companies. Given the crucial role played by the electronic address, it has become the company's representative on the Internet, symbolizing its trademark, name, or address.

This has made the electronic address an object of desire for many individuals and companies who hastened to register domain names without having any legitimate right or interest in them, thereby infringing upon the rights of others. Consequently, a legal issue arises concerning the mechanisms adopted to protect **electronic addresses and trademarks in electronic commercial transactions**. This paper seeks to answer this question using the **descriptive-analytical method**, guided by a **comparative approach**.

In fact, the infringement of electronic addresses and trademarks constitutes a form of **cybersquatting or piracy** of the rights of trademark owners on the Internet, leading to a **conflict between trademarks and electronic addresses (First Section)**. This situation calls for the **protection of the rights of domain name registrants and trademark owners (Second Section)**.

Section One: The Conflict Between the Trademark and the Electronic Address

The electronic address plays a distinctive role in identifying the existence of websites, which have become an essential element in the commercial companies' strategies for competition and for conducting business transactions over the Internet. (Dweidar, 2008, p. 14), As a new component of industrial and commercial property, infringement of the electronic address constitutes an infringement of the other elements of industrial and commercial property, particularly the trademark. The main causes of such infringements are closely linked to the system of electronic address registration. The most prominent forms of these violations are the unlawful appropriation of trademarks with the intent to sell them back to their rightful owners — a practice known as **cybersquatting** — and engaging in **unfair competition** involving trademarks in a way that harms their legitimate owners. (Al-Talahmeh, 2005, p. 75).

Accordingly, we will address the **causes of the conflict between the trademark and the electronic address (First Requirement)**, followed by the **forms of conflict between them (Second Requirement)**.

First Requirement: Causes of the Conflict Between the Trademark and the Electronic Address

The causes of disputes arising between trademarks and electronic addresses on the Internet are numerous; however, they generally stem from the rules governing the regulation of electronic addresses — whether related to the **registration of these addresses**, represented by the **principle of priority in registration (First Branch)**, or related to the **rules of using electronic addresses**, represented by the **absence of the principle of specialization on the Internet (Second Branch)**. (Ghanem, 2007, p. 11).

First Branch: The Principle of Priority in Registration

The registration of electronic addresses on the Internet is governed by a principle known as the **"first come, first served"** rule (*Premier arrivé, premier servi*). The application of this principle, combined with the lack of preventive measures by the authorities responsible for registration, has led to numerous disputes between trademark owners

and electronic address registrants. To clarify this issue, we will address the **meaning of the principle of priority in registration (1)** and the **impact of its application (2)**.

1. The Meaning of the Principle of Priority in Registration

The principle of priority means that any person may obtain an electronic address as long as they submit their registration request before any other company or individual, without objection from others. There are no specific conditions required to acquire an electronic address, except that it must not have been previously registered by another person. Thus, when registering electronic addresses, what matters most is **the chronological priority of the registration request** over other applications. (Nasreddine, 2008, p. 102), Despite the similarity between the registration of an electronic address and that of a trademark – as both are based on the principle of priority or precedence in registration – there are differences between them concerning the registration procedures. The registration of a trademark goes through several stages: **filing the application, examination, and finally registration and publication** (Rachidi, 2012, p. 232), In contrast, the registration of an electronic address is carried out directly, without being preceded by the filing of a registration application. The person wishing to register simply fills out the registration form available on the website of the competent authority—whether for general or national electronic addresses—and then pays the required fees. If the domain has not been previously registered, the authority will approve the request without examining the submitted applications, unlike the procedure followed for trademark registration. Hence, the registration of an electronic address does **not** go through a preliminary application stage.

Furthermore, trademark registration requires the competent authority to **verify the identity of the applicant** and allows it to request all necessary documents to prove the applicant's right to file the registration. This ensures that the application does not infringe upon any **pre-existing rights of others** (Mubarak, n a, p. 50), While the situation differs in the case of registering an electronic address, the competent registration authorities do **not** verify the identity of the applicant. It is sufficient that the address has not been previously registered for the request to be approved without any further conditions. Therefore, most registration companies always include in their **domain name registration agreements** a clause stating that they are not responsible for conducting any prior search regarding the existence of third-party rights before registration. The burden of performing such a search falls entirely on the applicant, who becomes liable if the registration infringes upon others' rights.

An example of this is the **naming agreement** governing electronic addresses within the French domain ending in ".fr," issued by the company **AFNIC** and implemented on **January 26, 2001**. This agreement explicitly states that AFNIC does not conduct any search for the prior existence of domain names and that the applicant must ensure that their chosen electronic address does not infringe upon any legitimate rights of others.

2. The Effect of Applying the Principle of Priority in Registration

When an electronic address is granted according to the **principle of priority in registration**, numerous disputes arise between domain name registrants and trademark owners. The application of this principle often results in depriving the trademark owner of registering an electronic address representing their trademark on the Internet because it has already been registered by another party. This situation constitutes an infringement upon the **legitimate rights and commercial interests** of the trademark owner, particularly concerning their ability to use an electronic address bearing their trademark name to represent their business online.

The effects of this principle can be illustrated as follows:

2.1 Preventing the Trademark Owner from Using Their Trademark on the Internet

The registration of an electronic address grants its holder the **exclusive right** to use it, without any interference from others. This is explicitly stated in most domain registration agreements. Consequently, the registered electronic address cannot be used by anyone other than its registrant, and others are prevented from benefiting from it to promote their products or services through the corresponding website, which functions as an **electronic commercial outlet**.

In such cases, the registration of the electronic address causes harm to the trademark and constitutes an infringement of the legitimate rights of the trademark owner by a person who has no rightful claim to it.

To illustrate this negative effect of the **principle of priority in registration**, there are numerous judicial precedents, the most notable being the **French “Alice” case**.

The facts of this case are as follows: **SNC ALICE**, a company operating in the field of advertising and publicity, sought to register an electronic address on the Internet under the name **“Alice.fr”**. However, the French registration authority **AFNIC** responded that this electronic address was **unavailable**, as it had already been registered by another company, **Alice SA**, which worked in the field of computer software.

Both the **Court of First Instance** and the **Court of Appeal** confirmed that the registration of the electronic address **“Alice.fr”**, granted to **Alice SA**, was consistent with the registration rules established by **AFNIC**, particularly the **principle of priority in registration**. Therefore, no infringement was found on the legitimate rights of **SNC ALICE**.

Hence, it can be concluded that, **even when the registrant of the electronic address acts in good faith, no legal protection** is granted to the legitimate trademark owners who are unable to register electronic addresses corresponding to their trademarks on the Internet (Kapferer, 1988, p. 146).

2.2 Infringement of the Legitimate Rights of Others

The impact of the **principle of priority in registration** is not limited to preventing the legitimate owners of trademarks from registering electronic addresses that represent their marks; it also extends to **violations of legitimate rights**. This principle has encouraged many individuals to exploit it as a means of financial gain, given the **low cost** and **speed** of registering an electronic address. Consequently, many rushed to register **trademarks as domain names** with the intent of reselling them later to their rightful owners at **exorbitant and unrealistic prices**, which ultimately constitutes what is known as **cybersquatting** or **cyber piracy**.

Some individuals even register domain names containing **famous or globally recognized trademarks** such as *La Coste* or *Rolux*, with the goal of forcing the rightful owners to pay large sums of money in exchange for relinquishing the domain name that bears their well-known trademark. The **wide popularity of such trademarks among consumers** and their **high financial value** for the companies that own them make them tempting targets for misuse and exploitation as a tool for **illegitimate profit**—by registering them quickly as domain names at minimal cost and then reselling them at inflated prices to their lawful owners.

The **Generic Top-Level Domain (gTLD)** system has greatly contributed to the **increase and spread of trademark infringements**, since domain names ending with “.com” are among the most widely used on the Internet. The majority of commercial companies prefer this extension to promote their products and services. However, because the **principle of priority in registration** allows a domain name to be registered **only once by the first applicant**, some people register famous trademarks within the **gTLD system** to give the domain a high commercial value, which they later resell at enormous prices to the actual trademark owners.

To address such infringements that represent clear **violations of trademark ownership rights** through domain name registration, the **U.S. Congress** intervened by enacting the **Anticybersquatting Consumer Protection Act (ACPA)** in 1999, which came into effect in **January 2000**. This law aimed to combat acts of **cybersquatting** and the **unauthorized registration of trademarks as domain names**. It also classified such practices as **illegal acts**, including the **imitation of famous or protected trademarks** under trademark law.

Under the **ACPA**, a **trademark owner** is granted the right to file a **civil lawsuit** against any person who engages in cybersquatting or uses a domain name with **bad faith intent to profit** from such conduct.

Among the **remedies** that a court may order under this law are:

- **Cancellation** of the cybersquatter’s domain name registration;
- **Transfer** of the domain name to the legitimate trademark owner; and
- **Monetary compensation** for damages and profits obtained through the wrongful exploitation of the domain name.

In some cases, the **compensation** awarded can reach up to **\$100,000 (USD)** per infringed domain name. (Fernan, 2001, p. 56).

Second Branch: The Principle of Specialization on the Internet

The registration and use of trademarks are governed by the **principle of specialization**, which determines the scope of legal protection granted to a trademark within the limits of the goods or services it represents. In principle, **electronic addresses (domain names)** are also subject to this rule; however, applying it on the Internet proves to be particularly complex and distinctive. This complexity has led to numerous disputes between trademark owners and domain name registrants. The issue can be better understood by examining **the meaning of the principle of specialization (1)** and **its application to electronic addresses (2)**.

1. The Meaning of the Principle of Specialization

The registration of trademarks is governed by the principle of specialization, which means that a trademark is used and legally protected **only within the scope of the goods and services it represents**. Therefore, protection does not extend to other goods or services that are dissimilar or unrelated to those specified in the registration application.

In other words, there is a **specific designation of products and services** that the trademark covers, and legal protection applies **only within that scope**. For goods or services outside this scope, the **general rule is freedom of use**—that is, the use of a similar trademark is not prohibited as long as it concerns different types of goods or services.

The **objective of the principle of specialization** is to **protect consumers** from confusion or deception that might occur if the same trademark were used to identify unrelated products or services. (Al-Qalyoubi, 2007, p. 38).

Although the principle of specialization is considered the core of trademark law and applies to other elements of industrial and commercial property, there is no explicit provision that establishes it. However, legal scholars infer this principle from the various provisions governing trademark protection. In French law, for instance, the principle of specialization can be derived from Article 713, paragraphs 1, 2, and 3, of the French Intellectual Property Code. This article restricts the right to a trademark to the goods and services represented by that trademark, excluding other products. The third paragraph reinforces this by prohibiting any use of the trademark that could cause confusion in the minds of the public without the owner's consent, whether for the same goods and services or similar ones. Furthermore, international conventions concerning trademarks also adopt this principle — for example, the Nice Agreement on the International Classification of Goods and Services, concluded on June 15, 1957, to which most countries have acceded. (Abdallah, 2008, p. 288).

2- Application of the Principle of Specialization to Domain Names

Applying the principle of specialization to domain names is characterized by a certain difficulty and peculiarity, which often leads to disputes between domain name registrants and trademark owners. The reason for this lies in the fact that, from a technical standpoint, a domain name can only be granted once, in accordance with the principle of registration priority. Thus, the person who registers the domain name first acquires the legal right to it.

Consequently, in cases where two trademarks represent different products belonging to two different companies, if one of them registers a domain name incorporating its trademark under the international domain “.com,” that same domain name becomes unavailable to the other company—even though its trademark represents products entirely different from those of the first company that registered the domain.

An illustrative example is the trademark **“Vichy,”** owned by three different commercial companies: the first specializes in cosmetics and perfumes, the second in sparkling water, and the third in pharmaceuticals. Although the trademark is identical, each company owns it within a specific and distinct product category. Under normal circumstances, this raises no legal issue. However, when it comes to domain name registration, there can only be one domain name—**“Vichy.com”**—and it can belong to only one company, namely the one that registered it first within the international or global “.com” domain. This situation may give rise to disputes with the other companies seeking to benefit from the same domain name within this general commercial domain.

The issue becomes even more problematic when the person registering the domain name does **not** own the corresponding trademark, resulting in the legitimate owner being deprived of registering the domain name and thus prevented from representing their trademark on the internet due to its prior registration by another party.

Section Two: Forms of Conflict Between Trademarks and Domain Names

The conflict between domain names and trademarks can take several forms. The domain name holder may intentionally register a domain name with the aim of reselling it later at an exaggerated price to the original trademark owner or to one of their competitors—this constitutes a form of **cybersquatting** or **electronic piracy** of trademarks owned by others (First Branch). Another form of infringement may occur through **unfair competition** involving the use of trademarks on the internet (Second Branch).

First Branch: Electronic Piracy (Cybersquatting)

The emergence of electronic piracy — that is, the imitation or unauthorized use of trademarks on the Internet — coincided with the rise of the Internet itself as a fast and global means of communication. It was also linked to the widespread belief among many that the Internet is a space beyond the reach of legal regulation. (Laakab, 1999, p. 55).

Accordingly, this section will first explain the **concept of electronic piracy (1)** and then outline its **various forms (2)**.

1- The Meaning of Cybersquatting

Cybersquatting, or electronic piracy, refers to the act of a person who has no legal right to a trademark registering that mark as a domain name on the internet. This is done with the intent of harming the rightful owner of the trademark or reselling the domain name to that owner at an exaggerated price for profit, or selling it to one of the owner's competitors. (Al-Hefnawi, 2000, p. 109).

The hacker relies, in selling the electronic domain names he has registered, on the confusion and misunderstanding that occur in the minds of the public, as he deliberately chooses famous trademarks to register electronic addresses representing them. Consequently, the owner of the well-known trademark — in order to protect the reputation of his mark — has no choice but to negotiate with the hacker to recover the address at whatever price he demands. Among the factors that have encouraged the emergence of cybersquatting are the following:

1.1 The principle of priority in registration:

As previously explained, this principle governs the registration of electronic domain names, allowing anyone to register a domain name for a website based on the first application not previously registered. The registration authorities do not impose any conditions for obtaining it. This has encouraged many individuals to rush into registering numerous domain names that represent famous trademarks and then reselling them at exorbitant prices to their legitimate owners.

1.2 The fame of the trademark:

Many judicial rulings condemning cybersquatting have been issued in connection with infringements on globally renowned trademarks that are well-known among a large audience of consumers. Examples include the trademarks *McDonald's* and *Guy Laroche*.

1.3 The type of domain in which electronic addresses are registered:

Cybersquatting tends to increase in relation to general domain names ending with “.com” or “.net” more than national domain names. This is due to two reasons: first, these domains are more famous and widely recognized among internet users, which leads most commercial companies to seek to own general electronic addresses because of their popularity, thereby helping to spread their trademarks and market their products more effectively. The second reason lies in the limited prior supervision over the granting of general electronic addresses, as the American company *NSI* responsible for registering such domains does not require any certificate or document for registration, unlike national domain names belonging to specific countries. For example, in France, domain names

ending with “.fr” require, for valid registration, that the registrant present a certificate proving ownership of the trademark he wishes to register as a domain name. (Mohamed Saeed, 2009, p. 438).

2. Forms of Cyber Piracy

While trademarks are exposed to infringement in the real world, the likelihood of such infringements increases significantly on the Internet, particularly by domain name registrants. These infringements may take two forms: **infringement of the trademark by the domain name**, or **reverse infringement of the domain name by the trademark**.

2.1 Infringement of the Trademark by the Domain Name

In this case, it is assumed that the trademark has been duly registered in accordance with legal procedures. The holder of the domain name then registers a domain that infringes upon this trademark. Courts generally consider that the domain name holder has violated the rights of the trademark's lawful owner, granting the latter the right to file a claim for infringement in order to transfer or cancel the domain name and to obtain compensation for the damages sustained.

2.2 Infringement of the Domain Name by the Trademark

In this situation, the domain name is registered prior to the registration of the trademark. Thus, when the trademark owner later seeks to register it as a domain name, they find that it has already been registered by another party who acted in good faith, since the trademark was not yet registered at the time of the domain registration.

In this case, courts regard the domain name as a legitimate intangible asset protected by law against infringement, just like a trademark. The judiciary acknowledges the registrant's right to the domain name and considers that registering a similar trademark after the domain has been used constitutes an infringement of that registrant's right.

Section Two: Unfair Competition of Trademarks on the Internet

Trademark infringements on the Internet are not limited to acts of cyber piracy; they also extend to **unfair competition**. The concept and regulation of unfair competition on the Internet do not differ substantially from the general rules established under national laws. However, the online environment has introduced particular characteristics in the conditions for its application—especially with respect to the notions of **competition** and **damage**.

This becomes evident when examining the **concept of competition between the domain name and the trademark (1)** and the **concept of fault in unfair competition on the Internet (2)**.

1. The Concept of Competition Between the Domain Name and the Trademark

The Algerian legislator has not explicitly regulated unfair competition lawsuits nor specified their legal basis or conditions, merely mentioning certain practices considered unfair. In the context of trademarks, the legislator deems the imitation of distinctive marks, products, services, or advertisements of a competing economic operator—with the intention of attracting that operator's clients through deception or confusion—as acts of unfair competition.

The scope of unfair competition has extended to electronic commercial transactions. Thus, unfair competition claims also apply to online dealings conducted over the Internet. These claims are governed by the general principles of tort liability but acquire certain specific features related to their online application. Judicial practice shows that, for an unfair competition claim to be valid, there must be competition between the domain name registrant and the trademark owner, while taking into account the peculiarities of Internet-based commerce.

1.1 Similarity of Activities as a General Condition for Unfair Competition

As a general rule, for an unfair competition claim to be admissible, competition must exist between traders engaged in identical or similar activities. If the activities differ, competition cannot be presumed. The same

condition applies to unfair competition on the Internet, as judicial applications have adopted the criterion of similarity of goods and services to determine whether competition exists in electronic transactions and whether such similarity could lead to consumer confusion or deception. Consequently, in the absence of such similarity, no competition can be said to exist between a trademark and a domain name.

1.2 Application of Unfair Competition in the Absence of Similarity – An Exception to the General Rule

Although courts generally require the existence of similarity or identity of goods and services to establish competition, they have expanded this concept in certain cases to protect trademarks from online infringements. Courts have applied unfair competition rules even when the products or services differ, recognizing that merely registering a domain name identical or similar to a trademark may indicate bad faith and an intent to prevent the trademark owner from using their mark on the Internet or to resell the domain for profit.

An example of this is the **1999 decision of the Paris Court of Appeal**, where the defendant company was convicted under the rules of unfair competition for using the trademark **“Champagne”** to attract customers to its website dealing in perfumes and fragrances. The court dismissed the defendant’s argument that its business activities differed from those associated with the trademark (wines), ruling that the company had engaged in unfair competition by exploiting the mark’s reputation.

Thus, recent judicial trends regarding online trademark infringements no longer require similarity or identity of goods and services as a condition for protection. Instead, they rely on the **criterion of confusion and deception among consumers** as the decisive factor in establishing unfair competition.

2. Fault in Unfair Competition

In cases of unfair competition between trademarks and domain names on the Internet, **confusion and deception** represent the most common forms of fault. The registration of a domain name identical or similar to a trademark can mislead consumers, directing them to a competing website and generating unjust profit while harming the trademark owner.

A clear example is the **“Guy Laroche” case**, in which the court found that Internet users attempting to access the disputed domain name were redirected to a competitor’s website rather than the official **“Guy Laroche”** site, resulting in a significant loss of clients.

Moreover, the **Uniform Domain Name Dispute Resolution Policy (UDRP)** issued by ICANN on **October 24, 1999**, explicitly recognizes the registration of domain names with the intent to obstruct or harm commercial competition as an act of **bad faith**, justifying the cancellation or transfer of the domain name. The UDRP expressly provides that attracting Internet users away from trademark owners by creating confusion among consumers constitutes bad faith registration and use.

Section Two: Manifestations of Trademark and Domain Name Protection in E-Commerce Transactions

The expansion of the Internet and the proliferation of e-commerce activities have led to an increase in the number of websites, accompanied by new forms of infringement against trademarks and domain names. This has made it necessary to protect legitimate rights holders by enabling them to bring legal actions before courts.

However, in order to strengthen protection for trademarks and domain names in cyberspace, significant efforts have been made by various organizations and entities involved in Internet regulation and intellectual property protection. These efforts culminated in the adoption of **amicable settlement mechanisms (First Requirement)** through the **Uniform Domain Name Dispute Resolution Policy (UDRP)** as an additional means of protection designed to mitigate the limitations of judicial protection (**Second Requirement**).

First Requirement: Amicable Settlement

Electronic transactions, by their very nature, transcend the geographical boundaries of states due to the global nature of the Internet. This gives such transactions a unique character, as they are based fundamentally on borderless communication. Consequently, the idea emerged to make the protection of rights conducted over the Internet **global in scope**.

This development has prompted numerous institutions and organizations concerned with online transactions to pay close attention to **intellectual property rights** as they are exercised and traded via the Internet, ultimately serving the interests of all parties engaged in **electronic commerce**. (Ahmed , 2006, pp. 66 - 67).

Credit is due to the distinguished efforts of the **World Intellectual Property Organization (WIPO)**, which recognized the importance of protecting trademarks in their relationship with domain names, especially with the evolution of commercial transactions from traditional to electronic forms. These efforts culminated in the response of the **Internet Corporation for Assigned Names and Numbers (ICANN)** to the recommendations of WIPO's first report in 1999, through the adoption of new rules for resolving disputes related to domain names. These are known as the **Uniform Domain Name Dispute Resolution Policy (UDRP)**.

To provide a comprehensive understanding of these rules as an additional means of protection, this section will examine the **legal nature and scope of application** of these rules (Section One), followed by an analysis of the **conditions and procedures** for their implementation (Section Two).

Section One: The Legal Nature and Scope of Application of the Uniform Dispute Resolution Policy

The **Uniform Domain Name Dispute Resolution Policy (UDRP)** refers to the set of rules issued by **ICANN** as a friendly and optional mechanism for resolving disputes arising from the registration of domain names, particularly those involving infringements of trademarks. It represents a new form of **alternative dispute resolution** specifically designed for e-commerce conflicts.

1. The Legal Nature of the UDRP Rules

These rules differ from traditional court litigation, as dispute resolution is handled by **international arbitration panels** rather than national courts. These panels examine disputes through **administrative committees** and issue **non-binding decisions** for the parties involved.

Recourse to the UDRP mechanism is based on a **clause included in the domain name registration contract**, imposed by the domain registrar on the registrant. This clause requires that any future dispute concerning the domain name be resolved through the UDRP mechanism. Since the contract exists between the domain name registrant and the registration authority, the **trademark owner** is usually unaware of this clause, as they are **not a party to the contract**.

It is worth noting that the presence of a clause subjecting domain name disputes to the UDRP does **not prevent** the parties from resorting to **judicial proceedings**, either before or after the UDRP decision. If judicial proceedings are initiated, the administrative panel handling the dispute may either **suspend** or **terminate** the UDRP procedure. Likewise, a court may issue a judgment that **contradicts** the decision made under the UDRP, as such decisions are **not binding** on judicial authorities.

The enforcement of a UDRP decision is **not carried out by the disputing parties themselves**, but rather by a **third party**—namely, the **domain name registrar** that registered the disputed domain name. The registrar is responsible for executing the decision by **canceling**, **transferring**, or **retaining** the domain name as determined by the panel. Thus, the decision is directed only to the **registration authority**, even though it is **not a party** to the dispute, since the actual parties are the **domain name registrant** and the **trademark owner**.

2. The Scope of Application of the UDRP Rules

The **Uniform Domain Name Dispute Resolution Policy (UDRP)** constitutes the **legal framework** for resolving disputes arising between **domain names** and **trademarks**. However, it does **not** address all such disputes; it applies

only in cases where a **domain name has been registered in bad faith**, unlawfully, and **without any legitimate right**, with the intent to harm the **lawful rights of a trademark owner** or to **gain financial profit** from such registration.

Any person who has suffered harm due to the registration of a domain name incorporating their trademark may file a **complaint** against any **natural or legal person** who carried out the registration—**with the exception** of **ICANN itself** and the **domain name registration authorities**, as these entities are **not subject to the UDRP** and may instead be sued before **ordinary courts of law**. (Faroun, 1997, p. 34).

The **UDRP rules** have jurisdiction to resolve disputes under a clause included in the **domain name registration agreement**, by which the registrant agrees to be bound by these rules in the event of a dispute concerning the domain name. The **ICANN** organization has required the inclusion of this clause for all domain name registrants since **December 1, 1999**. As for registration contracts concluded before that date, the parties may choose to resort to the **Uniform Domain Name Dispute Resolution Policy (UDRP)** on a **voluntary basis**. (Marie-Christine , Alexandre, & Emmanuel, 2007, p. 75).

In principle, the Uniform Domain Name Dispute Resolution Policy (UDRP) applies to generic or international domain names such as those ending with **.com**, **.org**, or **.net**. These unified rules therefore apply to domain names registered under these generic extensions when they involve an infringement of trademarks. The **UDRP** may also apply to national or local domain names if adopted by the authorities responsible for registering such domains. (Dretta, 2003, p. 85).

Section Two: The Administrative Procedure for Dispute Resolution under UDRP Rules

The **Internet Corporation for Assigned Names and Numbers (ICANN)** has sought to provide a fast and efficient solution for domain name disputes. To achieve this, the **UDRP** (Uniform Domain-Name Dispute-Resolution Policy) established an *optional administrative procedure* that individuals and companies may resort to as an amicable means of settling their disputes. The rules govern both the conditions for initiating this procedure and its method of operation. To fully understand this mechanism and its role in resolving intellectual property disputes related to domain names, we will examine the **concept of the administrative procedure (1)** and then its **implementation and termination (2)**.

1. The Concept of the Administrative Procedure

The concept of the administrative procedure established by **ICANN** for amicable settlement of domain name disputes is defined by its **characteristics** and **conditions**.

1.1 Characteristics

The main characteristics of this procedure are as follows:

1.1.1 A Low-Cost Procedure

Parties who choose this procedure do not incur the heavy expenses typically associated with ordinary courts or arbitration proceedings. The cost of the administrative procedure ranges between **USD 750 and USD 2,000**, when the dispute concerns a single domain name. (DREFUS, 2000, p. 110).

1-1-2. A Fast Procedure

The administrative procedure is characterized by its speed in resolving disputes. *ICANN* sought to shorten the duration of the process to ensure its effectiveness and compatibility with the nature of commercial relations on the Internet and the seriousness of cybersquatting, which causes significant losses to trademark owners. The total period required to issue a final decision in the dispute under this administrative procedure ranges between **40 and 60 days**, a much shorter timeframe than that required before ordinary courts.

1-1-3. An Amicable and Optional Procedure

The administrative procedure is both **amicable** and **optional**. It is amicable in the sense that, by choosing this route to settle their dispute, the parties avoid litigation before courts or arbitration tribunals. The dispute is presented to a **neutral administrative panel** that applies specific rules established by *ICANN*, which relate exclusively to domain names. The panel ultimately issues an **administrative decision** that the parties voluntarily comply with, without coercion.

From another perspective, it is **optional**, since although *ICANN* recommended including a clause in all domain name registration contracts obliging parties to resort to this procedure, the parties still enjoy broad freedom. They may **withdraw from the process at any time**, whether before it begins or during its course, and may **turn to ordinary courts** instead. Likewise, they are **not bound** by the panel's final decision and may still bring the case before the judiciary even after a decision has been issued, to have the dispute reconsidered. (DREFUS, 2000, p. 114).

1-2. Conditions for Applying the Administrative Procedure

For a dispute concerning a domain name to fall under the **UDRP rules**, three conditions must be met. The burden of proving these conditions lies with the **complainant**, i.e., the owner of the trademark. These conditions are as follows:

1-2-1. Existence of an Identical or Confusingly Similar Domain Name

According to this condition, the complainant (the trademark owner) must prove that the disputed domain name is **identical or confusingly similar** to their trademark in a way that is likely to mislead or confuse the public.

It is not required that the domain name be *identical* to the trademark; it is sufficient that there exists a **degree of similarity** that creates confusion in the minds of the public, considering the overall impression of both. The **assessment of similarity or identity** is left to the administrative panel handling the dispute, based on an **objective standard** — that of the *ordinary person*.

Thus, the administrative procedure provides protection under **UDRP rules** for both **registered and unregistered trademarks**. The conditions for applying the procedure require the complainant to prove the existence of identity or similarity between the domain name and the trademark, but **do not require** the complainant to prove **actual registration** of the trademark in question. Consequently, a trademark owner who has used their mark for a long time — sufficient to establish ownership — may file a complaint if their mark is registered as a domain name by another party, **even if the mark is not officially registered**.

1-2-2. Absence of Rights or Legitimate Interests of the Domain Name Holder

The trademark owner must also prove that the domain name registrant **has no rights or legitimate interests** in the domain name in order for the complaint to be accepted. A domain name registrant is considered to have a legitimate right if they also own a trademark identical to that of the complainant. In such a case, both parties are entitled to register a domain name incorporating that trademark to represent their respective goods and services online.

As for **legitimate interests**, the **UDRP** specifically defines them through a set of limited cases, which are detailed in the following sections.

- **The domain name registrant must prove** that, **before becoming aware of any dispute** regarding the domain name, they had **already used it in good faith** to offer goods or services, or had made demonstrable preparations to use it for such purposes.
- **The domain name registrant must prove** that they are **commonly known by the name** corresponding to the disputed domain name.
- **The domain name registrant must prove** that they have **used the domain name for legitimate, noncommercial purposes**, without the intent to profit, divert customers from the trademark owner, or tarnish or damage the reputation of the trademark or its owner.

1-2-3. Bad Faith Registration and Use of the Domain Name

Under the **UDRP rules**, the trademark owner must demonstrate that the domain name registrant **acted in bad faith** when registering or using the domain name. Bad faith can be inferred from various factors, such as:

- The **fame and recognition** of the infringed trademark;
- The **failure of the registrant to respond** to the complainant's allegations;
- The **pattern of conduct** in which the registrant registers multiple domain names to sell them for profit.

Bad faith may also be established **even if the registrant has not used the domain name commercially** — that is, even if no business activities were conducted through it. The mere **offer to sell the domain name**, without actual use, is sufficient to prove bad faith.

2. The Administrative Procedure: Commencement and Termination

The **UDRP rules** provide a clear framework outlining the **steps of the administrative procedure**, beginning with the filing of a complaint by the complainant and ending with a final decision to **transfer or cancel** the domain name.

2-1. Commencement of the Administrative Procedure

Alongside the UDRP itself, **ICANN** has issued **procedural rules** that must be followed by the **authorized dispute-resolution providers** when handling such cases. These providers may also establish **supplemental rules** to address procedural aspects **not covered by the general UDRP rules**, provided that these supplemental provisions **do not conflict** with the main **UDRP framework**. (DECANDE, 2000, p. 541).

The procedures followed before the competent authorities to examine the dispute can be summarized as follows:

2-1-1 Filing a Complaint by the Trademark Owner:

To address the dispute, the affected party—the owner of the trademark (the complainant)—must file a complaint with one of the competent authorities, claiming that the domain name registrant has infringed upon their trademark by registering a domain name identical or confusingly similar to it.

The procedural rules require that the complaint include the following information:

- Personal information about the owner of the infringed trademark, as well as the personal details of the domain name registrant.
- Identification of the disputed domain name and the infringed trademark, along with the products and services represented by that mark.
- Proof of the complainant's ownership of the infringed trademark.
- The competent court that may have jurisdiction over the dispute in case the committee's decision is not accepted.
- A statement from the complainant expressing readiness to comply with any supplementary procedure required by the competent authority until the dispute is resolved.
- Evidence that the dispute falls under the scope of the **UDRP rules** by proving that the registered domain name is identical or confusingly similar to the complainant's trademark and that the respondent has no legitimate rights or interests in the registered domain.

The committee then examines the complaint to ensure that all required information has been provided. If any information is missing, the complainant is notified and given five (5) days to correct the deficiency; failure to do so is considered a withdrawal of the complaint. If the complaint is accepted, the complainant must pay the required legal fees within ten (10) days from the date the complaint was received by the competent dispute-resolution

authority. Failure to pay the fees is treated as a withdrawal of the complaint, and the authority will not proceed with any further action until payment is made. The amount of these fees is determined by the accredited authority handling the dispute in accordance with its supplementary procedural rules.

2-1-2 Notifying the Respondent and Forming a Panel to Examine the Dispute:

After the complaint is filed, reviewed, and the fees paid, the dispute-resolution authority must notify the respondent of the complaint within three (3) days from the date the fees are received. The authority then grants the respondent twenty (20) days to respond to the allegations in the complaint. Once this period expires, the authority forms a panel—called an “Administrative Panel”—which begins examining the dispute within five (5) days after the expiry of the respondent’s response period. The panel may proceed with the case even if no response is received from the respondent, basing its decision solely on the contents of the complaint. (Gomai & Samir, 2000, p. 12).

2-2 Considering the Dispute by the Committee:

The Administrative Committee decides on the dispute based on the documents submitted by the parties. It may also request that the parties provide any additional or necessary documents needed to resolve the case.

As a general rule, the Administrative Committee examines the dispute without oral hearings; its decision is based solely on the written submissions and evidence provided by the parties. The Committee applies the *Uniform Domain Name Dispute Resolution Policy (UDRP)*, the *UDRP Rules*, and any legal principles or rules it deems relevant to the case.

Regarding the language of the proceedings, it is determined by the agreement of the parties. In the absence of such an agreement, the language used in the domain name registration process is adopted according to the registration rules.

During the proceedings, the respondent is prohibited from transferring or otherwise disposing of the disputed domain name—for instance, by selling or re-registering it with another registrar. If the respondent violates this prohibition, *ICANN* notifies the relevant registration authority to cancel any transactions made concerning the domain name during this period.

After reviewing the dispute, the Committee issues its decision within 14 days from the date of its appointment. The decisions generally fall into two categories:

First type: The Committee confirms the validity of the complainant’s claims and determines that the domain name registration by the respondent constitutes an infringement of the complainant’s trademark. In this case, the Committee orders the suspension of the respondent’s use of the domain name and its transfer to the complainant (the trademark owner). The Committee also notifies the relevant registration authority, which must implement the decision within 10 days of its issuance.

Second Type:

In this case, the Administrative Committee rejects the complainant’s arguments and upholds the respondent’s legitimate rights and interests, confirming that the domain name was not registered in bad faith. Consequently, the Committee dismisses the complaint filed by the trademark owner.

Despite the availability of this amicable and expedited mechanism for resolving domain name disputes provided by *ICANN*, the jurisdiction of national courts remains unaffected. If no amicable settlement is reached between the parties, they may resort to ordinary judicial proceedings. This will be discussed as follows:

Section Two: Judicial Settlement

This aspect of protection, established by law, is embodied in judicial proceedings through which any person with a legitimate right may request judicial protection for that right and bring action against any infringement upon it.

The types of lawsuits available to a trademark owner vary depending on their legal basis. Among these are actions based on tort liability—particularly the **unfair competition claim**, which is considered one of the most important forms of **civil protection for trademarks**. (Bakr & Khater, 2001, p. 177), Trademark owners may also resort to specific legal actions to combat cyber piracy. Accordingly, we will first address general judicial actions (Section One), then move on to the special judicial actions that deal with cyber piracy (Section Two).

Section One: General Judicial Actions

These actions available to the trademark owner differ in their legal basis. Some are grounded in intellectual property law—such as an action for trademark counterfeiting or imitation (1)—while others are based on tort liability principles, namely the action for unfair competition (2).

1. Action for Trademark Counterfeiting or Imitation

The Algerian legislator addressed this in Article 26 of Ordinance No. 03/06, which states:

“The owner of a registered trademark has the right to bring a legal action against any person who has committed or is committing an act of imitation of the registered trademark.”

However, for a trademark to enjoy legal protection, it must be registered. This is confirmed by Article 28 of the same Ordinance:

“Subject to the provisions of Article 10 above, any act infringing the exclusive rights of a registered trademark committed by another person constitutes the offense of counterfeiting. Counterfeiting is considered a criminal act punishable under Articles 27 to 33 below.”

Regarding the imitation of a trademark on the Internet, the purpose of a counterfeiting action in disputes between a trademark owner and a domain name holder is not to impose a criminal penalty on the perpetrator of counterfeiting or imitation, but rather to remedy the infringement committed against the trademark. This remedy takes the form of canceling the registration of the domain name, transferring it to the original trademark owner, and obtaining compensation for the damage caused by the infringement.

For such an action to be admissible, the trademark owner must prove ownership of the trademark. The trademark must also be distinctive, new, lawful, and duly registered and used by its owner. Proof of ownership may be provided through a certificate of national or international registration of the trademark. (BUCKI, 2000, p. 9).

It is also required, for the admissibility of a forgery or imitation claim, that the owner of the trademark proves that the use of the domain name by another party on the Internet has created a likelihood of confusion in the minds of the public between the trademark and the domain name. This confusion depends on the degree of similarity between the goods or services represented by the trademark and those represented by the domain name, and is assessed according to the specific circumstances of each case as determined by the trial judge.

2. The Unfair Competition Claim

The unfair competition claim is considered one of the most important means of protecting trademarks against domain name registrants. However, the Algerian legislator did not regulate this type of action in terms of the procedure for filing it or the conditions for its admissibility, leaving this issue to legal doctrine. At the international level, however, Article 10 (2) of the Paris Convention for the Protection of Industrial Property defines unfair competition as:

“Any act of competition contrary to honest practices in industrial or commercial matters.” (Sedqi, 2004, p. 15).

The admissibility of an **unfair competition claim on the Internet** is subject to the same conditions as those applied in the physical world, as defined by national laws, while taking into account the specific features imposed by the online environment. To initiate such a claim, there must be **unfair competition** between the trademark and the domain name. This requires the existence of a competitive relationship, meaning that the activities carried out by

the competitors must be identical or at least similar. Moreover, the acts of competition must be capable of **causing confusion or deception** among consumers regarding the products or services. Thus, the mere registration of a domain name that is identical or similar to a trademark and capable of misleading or confusing consumers is sufficient to hold the domain name registrant liable and to grant the trademark owner compensation for damages resulting from this infringement, which diminishes the value of the trademark.

In addition, **damage** must be established as a prerequisite for awarding compensation, since there is no liability unless the unfair competition directly causes harm to the competitor whether **material damage**, such as loss of profits, or **moral damage**, such as harm to the reputation of the trademark owner. Furthermore, there must be a **causal link** between the wrongful act (the unfair competition) and the harm suffered in order to justify compensation.

Section Two: Special Legal Actions

With the growing phenomenon of **cybersquatting** and the continuous infringement of famous trademarks through their registration as domain names on the Internet, several legislators have adopted specific rules to combat this issue. The **United States** was the first to recognize the seriousness of cybersquatting and the need to protect trademark owners against it. Consequently, the first special law addressing this issue was the “**Anti-Cybersquatting Consumer Protection Act (ACPA)**.”

Accordingly, we will examine (1) the **adoption and scope** of this law and then (2) the **forms of protection** provided under the Anti-Cybersquatting Consumer Protection Act.

1. Adoption and Scope of the Anti-Cybersquatting Consumer Protection Act

The U.S. judiciary sought to protect trademarks from infringement by domain name registrants through the application of the **Trademark Act**, attempting to extend its principles to the Internet. It treated **domain names as trademarks**, applying the same legal standards to disputes between a domain name and a trademark as those applied between two competing trademarks. As a result, trademark owners were allowed to file **lawsuits for forgery or imitation** of trademarks against domain name registrants using identical or similar names and to obtain **compensation** under civil liability principles. (CABELL, 2007, p. 7).

Under these circumstances, the U.S. **Consumer Protection Against Cybersquatting Act** was enacted on **November 29, 1999**, and entered into force in **January 2000**. The most significant provisions of this law include:

1-1 The provisions of this law base the conviction of cybersquatting on the **bad faith** of the domain name registrant, regardless of any similarity or identity between the goods or services represented by the domain name and those represented by the trademark. The law identifies cases of bad faith on the part of the registrant **by way of example, not limitation**, and proof of any one of these cases is sufficient to apply the provisions that require **cancellation or transfer** of the domain name registration to the trademark owner and may also entitle the latter to **compensation**. Examples of bad faith include registering a domain name with the intent to prevent the trademark owner from registering it, or with the intent to sell, offer for sale, or rent it.

1-2 The law enables trademark owners to bring what is called an **in rem action** against the domain name itself, when it infringes on their trademark, with the aim of canceling or reclaiming the registration. In addition to the *in rem* action, a **compensation claim** may also be filed against domain name registrants to remedy the harm suffered by the trademark owner.

2- Forms of protection provided by the Consumer Protection Against Cybersquatting Act
The Act provides trademark owners with **two main legal remedies** to protect their legitimate rights against cybersquatting: the **in rem action** and the **compensation claim**.

2-1 The in rem action

This is a lawsuit filed directly by the owner of the infringed trademark **against the domain name itself** that constitutes an infringement. The court's authority in such a case is limited to ordering either the **cancellation** or

transfer of the domain name to the trademark owner. To have this action admitted, the plaintiff must prove that an infringement has occurred against a legally owned and registered trademark, and that this infringement is linked to a domain name already registered on the Internet. The plaintiff must also demonstrate that it was **impossible to obtain the domain name** from the registrant despite reasonable efforts to do so.

2-2 The compensation claim

The U.S. Consumer Protection Against Cybersquatting Act also allows the injured party to seek **monetary compensation** from the infringer, in addition to requesting the **transfer or cancellation** of the domain name, in order to repair the damage caused by cybersquatting. However, according to the Act, the plaintiff – the trademark owner – **cannot request compensation** while the court is still considering the *in rem* action. (CEISTAL & GREEN, n a, p. 5), This is because the court's ruling is limited solely to the transfer or cancellation of the domain name. If the trademark owner wishes to obtain compensation, they must file a new lawsuit either before the same court that heard the *in rem* action or before another competent court.

Furthermore, this law established two types of compensation that the plaintiff must choose between prior to filing the lawsuit. The first is the **actual compensation**, defined by general legal principles, which covers all elements of damage, including both loss of profit and actual harm suffered. The second type is **statutory compensation**, in which the law determines both the minimum and maximum limits of the compensation, allowing the judge to award an amount within these limits without necessarily linking it to the actual extent of the damage.

However, what is criticized about this statutory compensation established under the U.S. *Consumer Protection Against Cybersquatting Act*—as noted by some legal scholars—is that it may lead to an abuse of rights by trademark owners. Even though the purpose of this law is to combat cybersquatting by all possible means, there must still be a balance between protecting trademark owners and the actual harm they have suffered as a result of the infringement.

Conclusion:

The rapid expansion of the commercial use of the Internet has led companies to reserve domain names in order to distinguish their products and services online. Consequently, e-commerce has used websites as a means of displaying trademarks, providing companies with a new gateway to global markets – accessible only through domain names that facilitate communication via the Internet. As a result, domain names have gained great importance for both consumers and businesses alike. They enable consumers to easily access the websites of commercial enterprises they wish to reach, thereby simplifying online transactions. Furthermore, domain names have become a vital tool for advertising, marketing goods and products, and introducing services offered by individuals and companies to an unlimited global audience.

At the conclusion of our study on this topic, we have formulated several recommendations as follows:

1. **We propose the introduction of prior control** over the granting of domain names by registration authorities. This could be achieved by requiring applicants to provide documents and certificates proving ownership of the name they wish to register as a domain name. Imposing such a requirement would significantly limit the activity of cybersquatters who unlawfully register trademarks owned by others.
2. **We also propose the creation of a new international domain space** dedicated specifically to trademarks, in which all domain names representing internationally registered trademarks would be recorded. Ideally, this international space should be divided into national subdomains where domain names representing national trademarks would be registered. The benefit of this specialized trademark domain and its national divisions lies in its role as a large database containing comprehensive information on international and national trademarks – including the trademark name, owner, registration date, corresponding domain name, registrar's name and details, and the registration date.
3. **Judges should be given the opportunity** to attend workshops and seminars organized by the World Intellectual Property Organization (WIPO Arbitration and Mediation Center) and the International Trademark Association. Such programs would enable them to better understand technical issues related to the Internet and e-commerce, particularly the technical aspects of domain names.

4. **Finally, we suggest that the Algerian legislator** take measures to address the phenomenon of cybersquatting through a specific law regulating the registration and use of domain names within the Algerian domain (.dz). The law should also amend the Trademark Act by adding provisions stating that:

“Registering a domain name identical or similar to a trademark constitutes an infringement of that trademark.”

Additionally, new provisions should be added to the unfair competition laws explicitly stating that: *“Acts of cybersquatting are considered forms of unfair competition.”*

Methodology

This research adopts a descriptive-analytical method supported by a comparative legal approach. The descriptive approach is employed to examine the concepts of electronic addresses (domain names), trademarks, and electronic commercial transactions, as well as to identify the nature and forms of infringement associated with them in the digital environment. The analytical aspect focuses on interpreting relevant legal texts, judicial decisions, and international regulations governing the protection of domain names and trademarks, particularly in light of the procedures established by the Internet Corporation for Assigned Names and Numbers (ICANN) and the Uniform Domain-Name Dispute-Resolution Policy (UDRP). Furthermore, a comparative examination is conducted between the legal frameworks applied in selected international jurisdictions and Algerian legislation, in order to highlight similarities, identify gaps, and propose recommendations for strengthening legal protection mechanisms in electronic commercial practices.

Ethical Considerations

This study is based exclusively on publicly available legal sources, academic references, and international regulatory frameworks. No human participants, surveys, or personal data were involved. Therefore, the research did not require formal ethics approval. All sources and references have been cited appropriately to ensure academic integrity and avoid plagiarism. The authors affirm that this study complies fully with ethical standards applicable to legal and academic research.

Acknowledgements

The authors would like to express their sincere appreciation to the Faculty of Law and Political Science at the University of Mascara for providing academic guidance and a supportive research environment. Gratitude is also extended to colleagues and specialists in commercial and cyber law whose insights and discussions contributed to enhancing the quality and depth of this study.

Author Contributions

- Tahraoui Soumia: Conception and design of the study, theoretical framework development, analysis of international legal approaches, and drafting of primary sections.
- Yahiaoui Souad: Comparative analysis of national legislation, review of literature, refinement of legal arguments, and final editing and proofreading.

Both authors have read and approved the final version of the manuscript.

Funding

This research received no external funding. It was conducted as part of academic research activities affiliated with the University of Mascara.

Conflict of Interest

The authors declare no conflict of interest. The research was conducted independently and without any financial or institutional influence that could affect the objectivity or integrity of the findings.

References

1. Abdallah, A. (2008). The legal protection of intellectual property rights on the Internet. New University House.

2. Ahmed, A.-D. (2006). The legal aspects of electronic commerce and the mechanisms for settling its disputes. Dar Al-Nahda Al-Arabiya.
3. Al-Hefnawi, F. (2000). Law of software: Encyclopedia of computers and information systems. Dar Al-Kitab Al-Hadith.
4. Al-Qalyoubi, S. (2007). The concise guide to industrial legislation (Vol. 2). Dar Al-Nahda Al-Arabiya.
5. Al-Talahmeh, K. (2005). Conflicts between trademarks and domain names on the Internet. *An-Najah University Journal for Research*, 2, 75.
6. Bakr, I. A.-M., & Khater, S. H. (2001). Legal protection of intellectual property. Bayt Al-Hukm Publications.
7. Bucki, J. (2000). The conflict between trademarks and domain names. *Review of Intellectual Property Law*, 9.
8. Cabell, D. (2007). Forging domain name disputes. Mam-Tech. <http://www.mam-tech.com>
9. Ceistal, L., & Green, R. (n.d.). Trademark law and the Internet. International Trademark Association. <https://www.inta.org>
10. Decande, P. (2000). Conflict between domain names and trademarks: The first judicial decision under the UDRP. *Chronicle: Recueil Dalloz*.
11. Dreyfus, W. (2000). Protection of trademarks on the Internet: Toward conflict-resolution procedures. *Les Échos*.
12. Dretta, A. (2003). Internet and electronic commerce in international business law. Brylant.
13. Dweidar, H. (2008). Reflections on the legal regulation of electronic commerce. New University House.
14. Faroun, S. A. (1997). Protection of intellectual property rights on the Internet. *Intellectual Property Protection Journal*, 53, 34.
15. Fernan, B. S. (2001). Issues of commercial, industrial, and intellectual piracy (Vol. 1). Al-Halabi Legal Publications.
16. Ghanem, M. S. (2007). Protection of trademarks on the Internet in their relation to the electronic address. New University House.
17. Gomai, H. A., & Samir, H. (2000, November 20-22). The legal protection of websites and domain names [Conference presentation]. E-Commerce and Cross-Border Insolvency Conference, Cairo Regional Centre for International Commercial Arbitration, Cairo.
18. Kapferer, J.-N. (1988). Trademarks: The capital of the enterprise and the organization.
19. Laakab, M. (1999). Internet and the age of the information revolution. Houma Publishing and Distribution House.
20. Marie-Christine, J., Alexandre, C., & Emmanuel, C. (2007). The protection of trademarks on the Internet (Notebook of the Center for Research in Computer Science and Law). Bruylant.
21. Mohamed Saeed, A. (2009). Legal protection methods for e-commerce transactions. Al-Halabi Legal Publications.
22. Mubarak, M. A. (n.d.). The trademark and the means of its protection (Master's thesis). An-Najah National University.
23. Nasreddine, H. A. (2008). Internet site addresses (their registration, protection, and conflict with trademarks). Zein Legal Publications.
24. Rachidi, S. (2012). Protection of trademarks in Algerian law. *Academic Journal of Legal Research*, 1, 232.
25. Sedqi, M. A. (2004). Temporary protection of intellectual property rights. Dar Al-Nahda Al-Arabiya.