

Technical Protection of Digital Intellectual Works



Received: 06/05/2025; Accepted: 18/09/2025

Hajar KERMECHE ¹, Rawia YAHIA ^{2*}

¹ Banta 01 University Algeria, hajar.kermecche@univ-batna.dz

² Batna 01 University Algeria, rawia.yahia@univ-batna.dz

Abstract

Digital piracy protection fundamentally relies on technological measures that enable authors to control and safeguard their digital works. This study examines the effectiveness of such technical mechanisms in ensuring adequate protection against piracy. Adopting a descriptive-analytical approach, the research methodically explores solutions to the problem and poses the central question: to what extent do these measures effectively secure intellectual digital creations? Key proposals from the study include the rapid imposition of strict, deterrent penalties on piracy offenders, the enhancement of existing mitigation mechanisms, and the development of a global legal framework. Such a framework, forged in cooperation with the international community, is envisioned to serve as a benchmark for countries seeking to implement anti-piracy legislation. Overall, the study underscores the critical role of combining advanced technological measures with robust legal strategies to combat digital piracy effectively.

Keywords

Digital Intellectual Works;
Piracy;
Technical Protection.

الكلمات المفتاحية

المصنفات الفكرية الرقمية؛
القرصنة؛
الحماية التقنية.

الحماية التقنية للمصنف الفكري الرقمي

ملخص

تعتبر التدابير التكنولوجية آلية حمائية يمكن للمؤلف من خلالها السيطرة على مصنفه الرقمي وحمايته من جريمة القرصنة الإلكترونية، من هذا المنطلق نطرح الإشكالية التالية: ما مدى فعالية الآليات التقنية في تقرير حماية فعالة للمصنف الفكري الرقمي ضد جريمة القرصنة؟. للتحقيق الأهداف المبتغاة من خلال البحث كان لابد من الاعتماد على مناهج معينة في هذه الدراسة حيث اعتمدنا على " المنهج الوصفي التحليلي " الذي ساهم في تقديم حلول ملائمة لمشكلة محل بحث ودراسة.

من أهم المقترحات التي خرجنا بها في هذه الدراسة هو التعجيل بتشديد العقوبات الردعية الصارمة ضد مرتكبي جريمة القرصنة خاصة وأنها كثيرة الانتشار، مع تطوير جميع الآليات للحد منها، وكذا العمل على سن تنظيم قانوني عالمي لمكافحة القرصنة بالتعاون مع المجتمع الدولي بهدف جعله كمرجع للدول التي ترغب بإصدار قانون لمكافحة القرصنة على شبكة الأنترنت.

* Corresponding author. E-mail: hajar.kermecche@univ-batna.dz

Doi:

I- Introduction:

Digital intellectual works are defined as all that the human mind creates in literature, the arts, or sciences, regardless of the mode of expression—be it through writing, sound, drawing, photography, or any other physically embodied form. With the rapid technological progress, the advent of computers, and the emergence of the Internet, the dissemination, publication, and distribution of these works have become remarkably fast, easy, and cost-effective. Unfortunately, this convenience has engendered a new realm of digital crime in the form of cyber piracy—a phenomenon that has adversely affected the integrity of intellectual property rights and now poses a significant, real-world challenge to copyright law.

The importance of this study is underscored by the transformation of digital intellectual works from mere vehicles for the dissemination of knowledge and science into major economic assets and valuable commercial investments. Despite the vast array of digital tools and platforms that now provide authors with opportunities to capitalize on and widely disseminate their creations, many creators live in constant fear that their works will be pirated and exploited without any corresponding material or even moral compensation. This situation inevitably stifles their creative and innovative impulses.

In light of these factors, we pose the following research question:

To what extent are technological mechanisms effective in ensuring robust protection for digital intellectual works against the crime of piracy?

To answer this question, our study is divided into two main sections:

Section One: The Concept of Digital Intellectual Work Piracy

Section Two: Technological Measures as a Mechanism to Mitigate the Piracy of Digital Intellectual Works

Previous Studies.

It is noted that there are few studies on the subject of digital works due to its novelty, and those available focus only on one aspect among the several dimensions that this subject raises. Among the most important studies we relied upon are:

- A PhD Dissertation by the student Fatiha Hawas, which addressed the protection of digital works and domain names on the Internet. This study, discussed during the academic year 2016–2017 at the Faculty of Law and Political Sciences, University of Algiers [1]

The researcher aimed to delineate the scope of legal, technical, and administrative protection for digital works and domain names on the Internet by examining the concept, types, legal nature, international protection, and the legal mechanisms enacted by the Algerian legislator, as well as the extent to which copyright law and related rights keep pace with these developments.

This study intersects with our research by addressing technological measures for protecting digital works from piracy; however, the difference lies in that the researcher covered all types of protection provided for digital works, including both national legal protection and international protection.

- A PhD Dissertation by the student Linda Haj Sadouq, which dealt with the legal system of website names—a comparative study discussed during the academic year 2019–2020 at the Faculty of Law and Political Sciences, University of Algiers 1.

In her study, the researcher examined website names, or "domain names," in terms of the concept, protection requirements, types, legal nature, and the national and international mechanisms to protect them from infringements and the methods for their resolution.

This study intersects with our research in addressing digital works and their technical protection, since domain names are a type of digital work; however, our research extends to technological measures for protecting digital works in all their forms, including domain names.

I.1. The Concept of Digital Intellectual Work Piracy:

Establishing a clear concept for the crime of digital intellectual work piracy necessitates defining the term "piracy" as well as outlining its historical development, various forms, and the resulting consequences.

I. 2. The Historical Evolution of Piracy

The phenomenon of piracy began with the advent of the computer and expanded significantly with the use of Internet technology. The world's first recorded incident of piracy dates back to the early months of 1903. At that time, the physicist John Ambrose Fleming was preparing to demonstrate one of the era's revolutionary technological marvels—

a long-range wireless telegraph system invented by the Italian Guglielmo Marconi—before a large audience in the renowned lecture hall of the Royal Institute in London.

Just before the demonstration commenced, the device inexplicably began to click out a message. What started as a single word quickly transformed into an inappropriately satirical poem accusing Marconi of deceiving the audience. This incident, essentially a hacking of Marconi's presentation, was orchestrated by the British illusionist and inventor Neville Maskelyne, who later told *The Times* that his goal was to expose security weaknesses for the public good¹.

More than a quarter of a century after that wireless telegraph episode, in 1932, the issue of piracy evolved further. Polish cryptography experts Marian Rejewski, Henry Zygalski, and Jerzy Rozycki managed to crack the cipher of the Enigma machine—an apparatus exclusively used by the Germans during World War II to send and receive secret messages.

In the 1970s, piracy took on an even more complex dimension under the aegis of the renowned American programmer John Draper. He successfully manipulated telephone systems and their operational characteristics to control call routing and place long-distance free calls. This breakthrough played a role in the emergence of one of the world's most successful computer companies, later founded by Steve Wozniak and Steve Jobs.

The 1980s marked a further turning point in the history of software piracy. Personal computers, once the preserve of prestigious companies and universities, became accessible to the general public. This democratization of technology led to a rapid increase in the number of hackers and digital pirates².

During this period, numerous high-profile cases emerged—among them that of Roberto Soto, a Colombian national who, in 1986, infiltrated a government telex line to send messages to banks in the United Kingdom and other countries. This breach resulted in the illicit transfer of 13.5 million dollars from Colombian government funds. Subsequent years witnessed a succession of cyber-attacks targeting individuals and both public and private institutions³.

These developments spurred both domestic legislatures and the international community over recent decades to implement exceptional measures to combat piracy. A myriad of agreements, conferences, and protocols have since been established to protect individuals and institutions from the risks associated with this crime.

1.3 Defining the Crime of Digital Intellectual Work Piracy

The term "pirate" is an Arabized adaptation from the Medieval Latin word *cursarius*, which itself derives from the classical Latin *cursus*—meaning "course" or "path" from the verb *currere* (to run), a root that also appears in Arabic. Over time, the meaning in Medieval Latin evolved from "course" to denote a journey or campaign, eventually coming to signify an attack aimed at plunder. It is believed that the original Arabization of *cursarius* was rendered as "qarsār," which, over time, saw its final consonant shift from an "r" to an "n," possibly under the influence of the word for "captain."

The English word "pirate" is derived from the Latin term "pirata" (meaning "seafarer, sea thief") and its origin can be traced back to the Greek word "πειρατής," which means pirate. The literal meaning of *peiratēs* in Greek is "the person who attacks ships⁴."

The term "piracy" denotes an act committed by an individual called the pirate, and pirates are the robbers of the sea. Both "piracy" and "pirates" are used to describe the acts of plunder and robbery that were traditionally carried out at sea and along its shores, and which continue to exist today; piracy involves intercepting the passage of ships and boats, seizing their cargo and contents, and looting them. However, the advent of the computer and the evolution of its technologies and networks enabled free navigation and movement through cyberspace, thereby providing these modern pirates with clear opportunities for aggression through intercepting and seizing flowing information. This has introduced a new technical usage of the term "piracy," which is now applied to a subset of cybercrimes targeting intellectual property rights⁵.

In this context, WIPO and UNESCO have provided a similar definition of intellectual property piracy as: "any irresponsible use of materials protected under copyright law," which includes reproduction and distribution with the aim of achieving financial profit. Pirates often employ various methods and forms to reproduce the original printed edition, and to carry out unauthorized modifications with the intent of expropriating creative and intellectual works for use without authorization, such as by duplicating a work without paying the author's royalties, exploiting it, and clandestinely selling it through fraud and deception.

The selection of the term piracy to denote the violation of intellectual property rights is based on the similarity with traditional acts of piracy. When sea pirates attack ships out in the middle of the ocean and seize the entire vessel or its cargo, this scenario is analogous to the way digital pirates "attack" an author's work at the moment of its publication—with the intention of selling and profiting from it by expropriating its intellectual content, reproducing it, and distributing it. This offense bears a resemblance, to some extent, to the actions of traditional sea pirates⁷.

The TRIPS Agreement, in its preamble, defines piracy as: "pirated goods; that is, a product that constitutes a copy made without the consent of the rights holder or a person duly authorized by the rights holder in the country of production,

whether this copying is performed directly or indirectly from one of the items, thereby constituting a violation of the author's or neighboring rights under the laws in force in the importing country."

It can be said that the piracy of digital works is the unlawful appropriation of a digitally protected work stored within a computer system, with the aim of copying, reproducing, and distributing it for the purpose of achieving financial profit.

1.4 Forms of the Crime of Digital Work Piracy.

Digital work piracy manifests in the following ways: piracy of works originating from computer science—primarily the computer—and piracy of digital works resulting from the convergence of computer science and information technology—chief among them, domain names.

1.5 Piracy of Works Originating from Computer Science.

Piracy of computer programs takes many forms, but can generally be categorized into seven types; namely: copying; where computer software is pirated by creating several copies of the same program within one institution. Some organizations purchase a particular program with a license granted for use by one user on one computer only, yet they proceed to copy the program for all their employees, thereby enabling each employee to use the same software even though their license restricts them to a single user on one device. Alternatively, a purchaser may duplicate the program and distribute it among acquaintances—a practice some have referred to as actual theft⁸.

Piracy can also occur by loading the program onto a hard drive, where a computer distributor copies and installs the program onto the disk as a promotional and marketing tool to facilitate the sale of more computers.

Or through counterfeiting; which entails the unauthorized reproduction and sale of software protected by copyright law, often reproduced to appear as the original program—with the aim of achieving a high profit from marketing these non-genuine programs by selling them at a reasonable price, thereby allowing the perpetrator to achieve significant profit without any restraint or cost.

Or through piracy via media boards, whereby the protected program—as mandated by copyright law—is loaded onto media boards operated by a computer via a modem.

Or through the renting out of computer software via a specialized retail outlet that sells and displays the program, or even through some individuals who deliver these programs either in person or by mail, thereby generating financial benefit for the renter (as paid by video rental services and similar). This form of piracy has become quite widespread in recent times, especially in the realm of entertainment and gaming software.

Also, when the digital work is displayed on the Internet, then prepared in an isolated computer environment separate from the network or physical surroundings, it can be downloaded onto a computer connected to the network, transferred to a website, webpage, or email, or by any other means that allows Internet users to access and view it.

As in the case where someone processes and stores a copy of an article, book, artwork, or audiovisual work and uploads the copy onto the Internet; or accesses a website containing an electronic work, copies it, and then uploads this copy to their own website or webpage, making it available to the public either for a fee or free of charge.

Downloading and uploading, which represent technical systems used to transfer files from one computer to another over the Internet; the term "downloading" refers to the technical system that enables the reception of data and information from one computer to another via a server or modem linking them.

Meanwhile, the term "uploading" refers to a technical system that permits the transmission of a set of digital files from one computer to another connected to it via data networking, as these systems have made it possible to send and receive copies of intellectual works over the Internet, and consequently, to pirate these works⁹.

1.6 Piracy of Digital Works Between Computer Science and Information Technology.

Electronic piracy emerged from the realm of cybercrime that revolves around the digital space. The phenomenon of domain name piracy did not arise from the establishment of organizations such as ICANN, but rather surfaced with the growth of the Internet and the advent of e-commerce. In the early days, when commercial enterprises were not fully aware of the importance of having a presence in cyberspace and the commercial opportunities that could be reaped by acquiring domain names, they were faced with an extremely serious problem: that of electronic piracy of domain names.

It is meant by the piracy of domain names that an individual or legal entity registers a trademark or trade name belonging to another as a domain name, and then proceeds to lease it or offer it for sale—or even to a competitor. Studies indicate that the first act of electronic domain name piracy occurred in 1878 by one of the local American telephone companies.

The period between 1980 and 1989 is considered the golden age of electronic piracy, and the United States Senate defined domain name piracy as: "the willful, bad-faith, and abusive registration of domain names on the Internet, which violates the rights of trademark holders."

The process of domain name piracy is carried out through a variety of illicit practices; for example: registering a certain domain name for the purpose of sale or lease; transferring the registration of a domain name to the previous registrant, to the owner of the trademark, service mark or trade name, or to one of the aforementioned rights holders' competitors in exchange for substantial financial compensation—far exceeding the registration costs directly linked to that domain name; or registering a domain name to prevent the owner of a trademark, service mark, or trade name from using the mark in a similar domain name. This latter practice implicates the domain name registrar in such conduct, or involves registering a domain name with the aim of misleading Internet users who are, one way or another, seeking to access a person's or project's trademark, service mark, or trade name on the Internet.

The aggrieved party has several options: either purchase the domain name that encompasses their violated rights at the price offered, or resort to the courts to reclaim the domain name and prevent its use by its registrant—given that such use inflicts both material and moral damages—or resort to the Uniform Domain-Name Dispute-Resolution Policy¹⁰ overseen by ICANN¹¹.

1.7 The Effects of Digital Work Piracy

Digital work piracy results in a range of negative effects that can be summarized as follows: moral effects and economic effects.

1.8 The Moral Effects of Digital Work Piracy.

They are manifested in the assassination of the spirit of creativity and intellectual innovation, with the loss of authenticity of the intellectual product on display and a decline in its protection levels, as pirated and unauthorized works supplant the original creations. This, in turn, adversely affects the productivity of authors, given the increasing prevalence of piracy and cybercrime against their works, as well as the weakening of legal deterrents against such violations.

1.9 The Economic Effects of Digital Work Piracy.

The world loses billions of dollars annually due to violations of intellectual property rights, despite the tremendous efforts made to protect regional economies from this nightmare, which hinders economic and social development and contributes to the decline of intellectual and creative output. This occurs in the face of counterefforts that actively seize programs, inventions, and products created by others.

Intellectual property rights violations concern authors, writers, and creators around the world both internationally and regionally, as piracy increasingly poses a global threat to most literary, artistic, and technical works. This, in turn, leads to annual losses amounting to billions of dollars—especially after the Internet has become the broadest free commercial space known worldwide and has greatly contributed to the creation of new forms of publishing, transferring, copying, and preserving literary, artistic, or technical products; a development that necessitates the review and improvement of the current legislation in this area.

Piracy has a profound impact on authors, publishers, and both protected and global economies due to the ever-increasing assaults. Some statistics illustrate the losses incurred by many countries worldwide as a result of these illicit activities;

for instance, Algerian statistics from the "National Office of Copyright and Related Rights" indicate that the number of software, programs, and compact discs seized annually in Algeria has recently exceeded 600,000 discs, compared to no more than 80,000 discs at the end of the 1990s. This dangerous phenomenon has intensified due to the widespread use of the Internet across the country and a significant increase in youth participation in training courses in this field, which has led to the establishment of Algerian hacker associations that meddle in cyberspace corruptly. Their activities have spread to various countries around the world, resulting in the emergence of professionals in this field who have turned the world of information technology and the Internet into an opportunity to amass vast fortunes through the sale of discs and software containing various content—such as music, films, games, and programs for different administrations and research offices—with a modest sum of 100 Algerian dinars being sufficient to purchase the necessary software, whereas in developed countries, buyers pay hundreds of times more for IT products¹².

II. Technological Measures as a Mechanism to Limit Digital Work Piracy.

Due to the growing phenomenon of digital work piracy and the inability of national laws to provide adequate protection for it—along with the absence of specific measures aimed at safeguarding these works—it became necessary to devise a special form of protection, the goal of which is to safeguard the digital work and prevent its infringement by relying on

technological means and measures. However, new challenges soon emerged in this regard, particularly with the appearance of counter-technological methods that undermine the effectiveness of such protections¹³.

2.1 Definition of Technological Measures.

Technological measures, which can also be referred to as technological safeguards, are modern technical mechanisms aimed at combating digital criminal behavior using tools and methods based on contemporary digital technologies; these measures protect the digital work from any infringement, ensuring that it can only be accessed with the author's permission.

On the other hand, after reviewing Order No. 03-05 dated 19 July 2003 concerning copyright and related rights, it becomes evident that the Algerian legislator did not remain passive in the face of the technological developments taking place and the concomitant dissemination and distribution of digital works. Although the legislator did not specifically regulate protective measures for copyright on the Internet, he did employ new terms imposed by modern technology, such as "computer programs," "databases," and also the term "information processing system." In paragraph (a) of Article 4 of Order No. 03-05, the legislator specified the works covered by protection, among which "computer programs" are included—even though Algeria is a party to the first and second Internet treaties.

Technological protection measures play an important role in preventing access to a protected digital work, which is only possible with the permission and authorization of the copyright or related rights holder, especially when various types of data encryption techniques are used.

Moreover, these measures enable the author or their representative to establish a system for collecting a fee each time a user wishes to benefit from a protected digital work—whether by viewing or copying it.

These measures are also valuable in that they facilitate control over the number of copies made of the work. They allow for the identification of the specific work being copied, the determination of the author or rights holders of the work, as well as the specification of the forms and methods of copying being executed—all with the aim of easing the management of rights related to the work¹⁴.

It has also become entirely feasible, through these measures, to determine the number of times a work can be copied via the digital platform, to specify the number of times the work may be read through this platform, and even to set the duration during which the work can be accessed¹⁵.

2.2 Types of Technological Measures.

Protection through technical means is the prevailing method in most countries worldwide. These means rely on establishing technical barriers that prevent or hinder usage, with the aim of restricting access to the digital work and its exploitation only to those holding a license from the rights holder. These methods are varied and diverse—to the extent that it is extremely difficult to compile a comprehensive list of them; however, they all share the objective of providing the author and rights holders with the proper tools to ensure such protection¹⁶.

2.3 Effective Technological Measures to Protect the Digital Work.

Effective technological measures for protecting digital works can be divided as follows:

2.4 Technological Measures That Control Access to the Works ("Control Access"):

This type of technological measure aims to prevent access to the protected digital work and its exploitation except by those holding a license from the rights holders. These measures provide strict monitoring that prevents the work from being copied, using various technologies that play a preventive role to hinder access to the works¹⁷.

Among these technological measures and access controllers to the work are the following:

- **Password Systems:** The traditional and straightforward method for enabling access to protected digital works is to distribute passwords to users. These passwords are chosen by the user themselves and are formulated either randomly or through derivation—bearing in mind that the derivation of the password is based on a secret word or number known only to the user.

The passwords chosen by the user may be embodied in the form of security questions and answers stored by the system, where the system automatically poses questions to assist in forming the password, which can be changed at each connection.

- **Electronic Payment Methods:** This method of protecting copyright involves requiring an Internet user, who decides to view and use copies of the work, to make an advance electronic payment; either by instructing their bank to transfer the amount to the rights holder's account or by making an online electronic payment¹⁸.
- **Encryption:** Encryption involves introducing modifications intended to block or prevent access to information when transmitted to a specific party, or to convert the information into codes that are meaningless. When such encrypted data reaches others who cannot understand or utilize it, it effectively serves as a means to transform clear, ordinary texts into encrypted, unintelligible texts. In this way, encryption acts as a means to render the protected works published on the Internet invisible and inaccessible except to those who possess the encryption key.

Encryption is currently regarded as the only method to secure messages transmitted over the Internet, so that they contain clear information or signals between the two parties while remaining obscure to others.

The encrypted work published on the Internet could originally be an image, sound, or text... For instance, the music a user listens to on a website cannot be recorded on their computer's hard drive unless they obtain the key or a functional application that permits them to exercise their usage rights¹⁹.

- **Electronic Signature:** By electronic signature is meant "those unique letters, numbers, symbols, or signals that allow for the identification of the signatory and distinguish them from others, and that are certified by the competent authority." It is one of the modern techniques used to maintain strong security levels, ensure privacy, and protect information, data, and messages exchanged over the network. The electronic signature prevents unauthorized parties from viewing, modifying, or altering the contents, by determining the sender's and recipient's identities and detecting any alterations made to any program or file; since it resembles the sender's handwritten signature and cannot be forged, it provides enhanced protection for the information and works published on the Internet, thereby saving many from the burdens of online theft and cyber-attacks committed through the misuse of the network for exchanging and disseminating information²⁰.
- **Firewall:** A firewall is an insulating barrier composed of a series of programs and electronic devices that isolate important devices from one another's information systems, as well as from the communication network; all communications pass through this firewall, which permits only legitimate connections and prevents any unauthorized usage.
- **Website Filtering Technology on the Internet:** This refers to a set of media and specific computer programs that, according to commonly recognized standard specifications of the network's structure, allow for blocking, halting, or impeding access to certain websites.

The method employed by these programs for filtering is mostly at the level of website addresses—that is, access to a specific website on the network is blocked by restricting access to its particular address.

Internet network operators—especially those of public and private telecommunication networks controlled by states as a whole or by agencies allocating website addresses, as well as network service providers or certain specialized sites—can carry out this filtering, all the way to ordinary network users accessing the Internet via their personal computers.

However, the filtering system on the Internet that operates at the level of website addresses faces a number of problems and obstacles: some stem from the technical nature of the Internet, and others from its global nature. Therefore, filtering cannot rely solely on the address or even on the name of the service provided to achieve complete oversight over websites and the information exchanged on the Internet.

The only method remaining for effective website filtering is known as semantic filtering; that is, filtering based on meaning, so that instead of blocking access to entire websites, only the specific page or pages that should be restricted are identified within these various websites connected to the network²¹.

2.5 Technological Measures That Control the Usage of the Digital Work ("Use Control"):

Typically, the rights holder resorts to technological measures aimed at limiting the usage of a work that a user can access. This is usually done by preventing the user from obtaining any copy of the work or by specifying the number of copies a user is allowed to obtain; for this reason, these measures are sometimes called anti-copy measures—although this term is not entirely accurate since these measures, in addition to protecting the right of reproduction, may also include other rights such as the right of transmission²².

For example, multimedia products—also known as "multimedia" products such as compact discs—can be protected by technological measures that not only prevent the copying of the disc but also inhibit its use over the Internet.

Thus, there are types of technological measures which, when applied to an audio or visual work, have the capability to prevent the work from being streamed continuously ("streaming") on the Internet; this type of streaming does not reproduce the work onto the user's hard drive but merely allows them to listen to or watch it²³.

2.6 Essential Information for Rights Management.

Every piece of information provided by the creator of the digital work or by rights holders, intended to define the digital work and specify its terms and methods of use—and any number or code used to express all or part of this information. Consequently, the work may be "watermarked," for example, with a code or number to advertise its owner's details and the terms and conditions for its use. Such information, as applied to works, is akin to the metal license plate on a vehicle²⁴.

Essential information for rights management directly or indirectly facilitates the identification of the rights holders, aims to simplify the administration and exploitation of the related licenses, and also serves to track the duplicated copies on the Internet. In the digital environment where the circulation of works is effortless, marking them—whether the watermark is visible or not—indirectly encourages the respect of intellectual property rights.

Direct information refers to those details that allow for the identification of the protected digital work or its rights holders, such as the title of the work, the year of production, the name of the author or performing artist, the identity of the producer or distributor, etc²⁵.

Indirect information, on the other hand, comprises any numbers or codes that symbolize the aforementioned data; examples include those used in the realm of audio recordings and audiovisual materials.

A common method is also the electronic watermarking technique, known as "Watermarking1"; this technique permanently links the information to the work by adding data related to the work into its digital copies—either in a hidden or visible form, although the watermark is usually hidden.

It is noteworthy that digital watermarking has been increasingly used in cinematic works lately, where a film copy is watermarked with information such as the screening location, copy number, screening start date, and other details. Thus, if someone installs video cameras in screening halls for the purpose of piracy and online distribution, then by using the invisible electronic watermark—readable by special devices—the rights holders can identify the duplicated copy, its source, and location. Consequently, the screening hall owner may be held accountable for failing in their duty by not preventing the entry of cameras into the screening room.

Accordingly, this system enables the rights holder to track and distinguish copies made from the original work, so that unauthorized copies can be detected through reviews conducted by specialists on websites. In the event unlicensed copies are found, the author may request that the Internet service provider hosting these copies remove them or suspend the service for the infringer²⁶.

However, the system of essential information for rights management may infringe upon individual freedoms and the sanctity of private life, as it can be used to monitor users, verify the legitimacy of their possession of various programs, identify the person downloading the works by communicating with the service provider's website—even to the extent of attacking the personal computer using viruses. Therefore, the use of this technology must not transform from protecting the author's rights into an invasion of others' privacy or a breach of personal sanctity.

Although these measures have evolved, counter-technological methods quickly emerged with the aim of nullifying their effect and circumventing them—thus enabling the acquisition and exploitation of digital works without compensation. This has led most national legislations to treat such circumvention as an infringement of the author's rights and, consequently, as a criminal offense warranting punishment.

2.7 Circumvention of Technological Measures.

After the rights holders devised technical means to protect their digital works, counter-technological methods rapidly appeared with the purpose of nullifying these technological measures and circumventing them, in order to access and exploit the digital work without paying any compensation to the rights holders.

For example, devices that rely on code recognition and decryption technology effectively override the technological measures—the codes—that rights holders use to protect their works; such as the device used to decrypt television signals, which enables its user to view encrypted television programs without any payment to the rights holders²⁷.

Comparative legislations have turned to the protection of technological measures to prevent infringements on digital works by various means. The levels of protection provided in comparative legislations can be divided into three levels:

- a. Prohibition of acts that nullify or circumvent technological measures when such acts are conducted with the intent to obtain a legally protected work. (Level One)**

This level of protection is based on actions conducted with the intent to obtain a digital work legally protected under copyright and related rights law. This means that if the work is not enjoying the legally prescribed protection under copyright law, or if the protection period has expired and the work has entered the public domain, or if the work is not eligible for protection under the applicable copyright law, then acts that nullify or circumvent technological measures are considered legitimate and are not punishable by law.

b. Prohibition of acts that nullify or circumvent technological measures regardless of whether the work is protected or not. (Level Two)

This level is higher than Level One in terms of the degree of protection it provides to the technological measures, as it entails an absolute prohibition on any act that nullifies or circumvents these technological measures, without any distinction—whether the digital work is protected under copyright law or not, and regardless of whether the purpose of disabling or circumventing these measures is for fair use of the protected work or otherwise.

c. Prohibition of acts that nullify or circumvent technological measures, in addition to a ban on the manufacture, sale, or distribution of devices used to nullify or circumvent such technological measures. (Level Three)

This is the highest level of protection, because the prohibition here is not limited to the acts that nullify or circumvent the technological measures; it extends to the manufacturing, sale, or distribution of any devices used for that purpose. In other words, it prohibits the production or distribution of any tool designed to overcome access restrictions to the protected work, and to control its usage or exploitation. Therefore, protection at this level reaches its peak.

III. Conclusion:

In conclusion, it can be said that technological measures are technical mechanisms through which an author can control and protect their digital work from the crime of cyber piracy, by preventing access to the protected digital work except with their approval or the authorization of the rights holders.

The aim of technical protection is to employ methods based on modern digital technologies to safeguard the digital work from attacks, making it an effective means compared to the legal protection provided by international agreements and copyright and related rights laws. The greater the effectiveness, the greater the importance of technical protection at the expense of legal protection.

Key Recommendations

- 1- Expedite the imposition of strict, deterrent penalties against piracy offenders, especially given its widespread prevalence, while developing all mechanisms to reduce it.
- 2- Work towards enacting a global legal framework to combat piracy in cooperation with relevant international organizations and bodies, aiming to establish it as a reference for countries wishing to enact legislation against Internet piracy.

Referrals and References:

-
- [1]. Article published on the website <https://www.ta3allamdz.com/2017/02/history-of-Electronic-piracy.html>
 - [2]. Ahmed Fawzi Salem, "Digital Piracy: An Ancient History, 'Robin Hood' Motives, and Losses in the Billions", an article published on the website <https://www.noonpost.com/content/37624>.
 - [3]. Article published on the website <https://www.bankygate.com/7551>
 - [4]. Article published on the website ar.m.wikipedia.org.
 - [5]. Mohammad Abu Al-Hijaa Ibrahim, *E-Commerce Contracts*, First Edition, Dar Al-Thaqafa Publishing and Distribution, Amman, 2005, p. 215.
 - [6]. United Nations Educational, Scientific and Cultural Organization (UNESCO). Established under the London Convention of 1945 and headquartered in Paris, France, UNESCO is a specialized agency of the United Nations. Its primary objective is to contribute to the establishment of peace and security by enhancing cooperation among countries in the fields of education, science, and culture, thereby promoting global respect for justice, the rule of law, human rights, and fundamental freedoms. It is considered one of the key organizations that has significantly contributed to the international protection of copyright, either through its independent efforts or through its collaboration with WIPO and other international organizations operating in this field.

- [7]. Sameer Medhat Saeed, "Intellectual Property Piracy: An Analytical Perspective", Al-Farahid Literature Journal, Kuwait University, Issue 34, 2018, p. 45.
- [8]. Nassima Sabiq Issa Boulekh, "The Crime of Imitation and Its Impact on Intellectual Property Rights in Algeria", International Conference held at Batna 1 University, Faculty of Law and Political Sciences, on Imitation and Piracy of Industrial Property Rights, 20–21 October 2020, p. 8.
- [9]. Flavia Scarpellini, "The Various Forms of Intellectual Property Crimes", in the Proceedings of the Regional Symposium on Intellectual Property Crimes, in cooperation between the Public Prosecution of the Kingdom of Bahrain and the United Nations Development Programme – Governance Management Programme in Arab States, Kingdom of Bahrain, 13–14 April 2008, p. 56.
- [10]. The Uniform Domain-Name Dispute-Resolution (UDR) Procedures are legal measures adopted by the Internet Corporation for Assigned Names and Numbers (ICANN) aimed at resolving all disputes related to domain names registered for illegitimate purposes between domain name registrants and the holders of the infringed trademarks in top-level domains, as well as in country-code domains that have voluntarily adopted this policy.
- [11]. Case No. 96-3284 DDP (JRx), dated 19 September 1996, California, published on the website www.justia.com.
- [12]. Jamal Al-'Aifa, "Software Piracy in Contemporary Algeria and Its Challenges", Al-Risalah Journal for Human and Social Studies, University of Larbi Tebessi, Tebessa, Vol. 1, Issue 3, 2017, p. 310.
- [13]. Samia Kassal, "The Legal Protection of Digital Works (A Comparative Study)", Journal of Judicial Jurisprudence, University of Biskra, Issue 16, March 2018, p. 44.
- [14]. Osama Abu Al-Hassan Mujahid, *Misuse of Technological Protection Measures for Digital Works*, Dar Al-Nahda Al-Arabiyya, 2009, p. 2.
- [15]. Shamama Boutor'ah, "International Protection of Copyright", Journal of Human Sciences, University of Mohamed Khider, Biskra, Issue 46, 2016, p. 64.
- [16]. Ibrahim Al-Dusuqi Abu Al-Layl, "E-Publishing and Intellectual Property Rights", a paper presented at the Conference on Electronic Transactions (E-Commerce – E-Government), United Arab Emirates University, 2009, p. 19.
- [17]. Osama Faraj Allah Mahmoud Al-Subaagh, *Criminal Protection of Electronic Works*, New University Press, Alexandria, 2016, p. 88.
- [18]. Shamama Boutor'ah, same reference, p. 72.
- [19]. Fatiha Houdaas, *Protection of Digital Works and Domain Names on the Internet*, First Edition, Al-Wafa Legal Library, Alexandria, 2017, p. 194.
- [20]. Ayyub Antonius Polyos, *The Legal Protection of Personal Privacy in the Field of Informatics*, First Edition, Al-Halabi Legal Publications, Lebanon, 2009, p. 232.
- [21]. Ayyub Antonius Polyos, same reference, p. 234.
- [22]. Shamama Boutor'ah, same reference, p. 74.
- [23]. Suhail Haitham Haddadin, "Technical Protection of Copyright and Related Rights in the Digital Environment", The Jordanian Journal of Law and Political Sciences, Vol. 4, No. 4, 2013, p. 198.
- [24]. Ayyub Antonius Polyos, same reference, p. 236.
- [25]. Suhail Haitham Haddadin, same reference, p. 202.
- [26]. Ayyub Antonius Polyos, same reference, p. 237.
- [27]. Shamama Boutor'ah, same reference, p. 79.

