



Criminal Protection of Automated Data Processing Systems Against Illegal Access and Unlawful Remaining: A Study in Light of Algerian Law



Received: 16/02/2026; Accepted: 20/04/2026

Brahim BELHOUT*

Akli Mohand Oulhadj University of Bouira, ALGERIA i.belhout@univ-bouira.dz

Abstract

This research aims to highlight the framework for the crime of unauthorized access and persistence in information systems amid the proliferation of electronic transactions, considering it the primary gateway to other cybercrimes—thus rendering its criminalization a proactive measure to protect both the system and the data stored therein, particularly personal data. The study employs an analytical methodology focusing on Algerian law provisions under Article 394 bis of the Penal Code, while outlining prominent doctrinal trends in interpreting the elements and forms of this crime. It concludes that the Algerian legislator has adopted a flexible criminalization model based on penalizing mere unauthorized access or persistence, with aggravated forms whenever the act impairs data integrity or system functionality.

Keywords

Criminal Protection;
Data Processing Systems;
Illegal Access;
Unlawful Remaining;
Article 394 bis of the Penal Code.

الكلمات المفتاحية

حماية جزائية؛
معالجة آلية؛
دخول غير مشروع؛
بقاء غير مشروع؛
المادة 394 مكرر قانون العقوبات.

الحماية الجنائية لنظم المعالجة الآلية للمعطيات في مواجهة الدخول والبقاء غير المشروعين: دراسة في ضوء التشريع الجزائري

ملخ ص

يهدف البحث إلى إبراز إطار جريمة الدخول والبقاء غير المشروعين إلى النظام المعلوماتي، وسط تنامي المعاملات الإلكترونية، باعتبارها مدخلا رئيسيا للجرائم المعلوماتية الأخرى، بما يجعل تجريمها خطوة استباقية لحماية كل من النظام والمعطيات المخزنة فيه، ولا سيما البيانات ذات الطبيعة الشخصية. وتعتمد الدراسة منهجا تحليليا يركز على أحكام القانون الجزائري في ضوء المادة 394 مكرر من قانون العقوبات، مع بيان الاتجاهات الفقهية البارزة في تفسير عناصر هذه الجريمة وصورها. وتنتهي الدراسة إلى أن المشرع الجزائري تبني نموذجا تجريميا يتسم بالمرونة ويقوم على تجريم مجرد فعل الدخول أو البقاء غير المشروعين، مع تقرير صورة مشددة كلما ترتب على

* Corresponding author. E-mail: i.belhout@univ-bouira.dz

Doi:

I- Introduction :

The digital revolution and the spread of electronic commerce have brought about a profound transformation in the environment of legal and economic transactions, where automated data processing systems have become the technical framework through which contracts are concluded and by means of which advertising, offer and acceptance, and data exchange operations are carried out.

As a result, these systems have become a main repository for data of a personal and economic nature, which has made them a target for various types of technical attacks that pose serious risks to the confidentiality, integrity and availability of information. At the forefront of these attacks stands the offence of illegal access to, or unlawful remaining in, an information system, which doctrine has considered the natural gateway to the commission of other computer crimes, given that any interference with data or with the functioning of the system is preceded – in most cases – by an act of access to, or presence within, that system.

In view of this danger, a number of legislators have hastened to enact specific provisions criminalizing such conduct^[1], either in standalone cybercrime laws or by incorporating them into criminal codes, as is the case in France, Algeria, Morocco, Qatar and others, in addition to their treatment in the 2001 Budapest Convention^[2]. In Algeria, the legislator drew on the French model when it introduced provisions on attacks against automated data processing systems into the Criminal Code by virtue of Law N°. 24-06 of 2024. the Algerian legislator criminalizes the act itself under the provision of Article 394 bis of the amended and supplemented Penal Code, which was introduced by Law N°. 04-15 dated November 10, 2004, and further amended and supplemented—specifically regarding the penalty—by Article 60 of Law N°. 06-23 dated December 20, 2006.

This study starts from a central question: To what extent is the criminalization model adopted by the Algerian legislator sufficient to protect automated data processing systems against the offences of illegal access or unlawful remaining, in comparison with relevant legislation and conventions? To answer this question, the study examines the material element of the offence in its different forms, then the mental element, before addressing the criminal policy and penalties prescribed for it.

Importance of the Research and Posed Problematic

The significance of this research lies in illuminating the practical application of Algerian legal provisions concerning information systems protection, particularly the crime of unauthorized access and persistence. As cybercrimes evolve continuously in methods and techniques, the legislator faces an ongoing challenge to pursue this evolution and ensure legal texts' effectiveness.

Subject Scope and Methodological Boundaries

This study focuses on analyzing the crime of unauthorized access and persistence in automated data processing systems as criminalized by the Algerian legislator under Article 394 bis of the Penal Code. It employs an analytical method to examine legal texts, supplemented by a comparative approach contrasting Algerian provisions with French law and selected Arab laws to identify similarities and differences in legislative techniques.

II. The material element of the offence of illegal access to, or unlawful remaining in, an information system

An automated data processing system means any composite set of physical and software units operating integrally to process data via input, storage, processing, output, retrieval, and transfer operations. The Budapest Convention on Cybercrime (2001) defines it as "any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data."^[3]

1. Scope of criminalization and forms of conduct

Most legal systems that have addressed the criminal protection of information systems tend to criminalize the act of accessing or remaining in an automated data processing system whenever this is done without legal basis or without the authorization of the person entitled to the system. Article 323-1 of the French Criminal Code criminalizes illegal access to, or unlawful remaining in, an automated data processing system, and provides for a more severe penalty when the act is accompanied by erasure or alteration of data or impairment of the operation of the system^[4]. The Algerian legislator followed the same approach in Article 394 bis, where it criminalizes access to, or remaining in, all or part of an information system "by fraudulent means", and extends the scope of criminalization to cover mere attempt, while increasing the penalty where the act results in the deletion or alteration of system data or in damaging the operation of the system^[5].

Other laws adopt a similar approach. The Moroccan law punishes access to, or remaining in, an automated data processing system by means of fraud, and doubles the penalty in the event of deletion or alteration of data or the creation of a disturbance in the functioning of the system^[6], while Qatari law provides for a harsher penalty where the act of access or remaining results in the erasure or modification of information, or the damage to or disruption of the operation of the

system^[7]. The Dubai Law on Combating Information Technology Crimes considers any intentional unauthorized access to a website or information system as punishable conduct, and increases the penalty when the act is accompanied by deletion, destruction, alteration, disclosure or re-publication of data.

From these provisions, it is clear that the material element of the offence takes two main forms:

The simple form: based on the mere act of illegal access to, or unlawful remaining in, the system or part of it, without requiring any harmful result.

The aggravated form: arising when the access or remaining is accompanied by certain results, most notably the deletion, alteration or erasure of data, or the impairment, disruption or destruction of the way the system operates.

2. The meaning of illegal access

Unauthorized access is deliberate entry—total or partial—into an automated data processing system without right, whether breaching security barriers (hacking), impersonating legitimate users, or exploiting software vulnerabilities. Physical transfer is unnecessary; logical connection enabling data viewing or system control suffices^[8].

In this context, “access” does not mean physical entry to the place where the computer is located, but rather virtual access to the information system itself, that is, connecting to the system or gaining control over the information or services it provides, even if this is done remotely via networks. Some legislations expressly define the act of “access”. The Saudi Anti-Cybercrime Law, for example, defines it as the intentional access by a person to a computer, website, information system or computer network without authorization, while the law of the State of Kansas (United States) broadens the concept to include approaching, giving instructions, and storing or retrieving data from a computer system or network.

In doctrine, computer access is seen as any act that allows entry into the system and becoming aware of the information it contains or controlling the services it provides. In this sense, it is an intangible phenomenon similar – metaphorically – to entering a person’s memory^[9]. For this reason, some legislations have preferred to use terms such as “access” (in the sense of connection or login) instead of “entry”, in order to avoid the narrow physical connotations of the latter, whereas other systems use the term “hacking” to denote penetration of systems protected by technical measures.

The law does not restrict the means by which illegal access may be committed. The offence is constituted whenever access is obtained by fraud, deception or trickery, whatever the technical means used; such as using a valid password without authorization, employing specialized programs to break security, or exploiting “back doors” that allow bypassing security systems.

3. The meaning of unlawful remaining

The French legislator – followed by the Algerian legislator and a number of Arab laws – included the act of “unlawful remaining” in the system among the punishable acts, in order to address situations where access is initially made by mistake or accident and the person then continues to remain within the system after realizing the illegality of his presence^[10]. In this form, the conduct consists of two interrelated elements: an access – even if unintentional – followed by a failure to disconnect despite knowledge of the lack of authorization, or an overstepping of the limits of authorization in terms of place, time or purpose^[11].

Some scholars regard remaining as a positive activity represented by the continued control over the connection to the system, while others consider it a negative act consisting in refraining from exiting when this is required, which makes the offence one of the continuing omissions-type crimes. In any event, it is impossible to conceive of the offence of unlawful remaining without prior access to the system, even if such access was lawful at the outset and then turned into unlawful remaining when the limits of authorization are exceeded in terms of scope, duration or purpose.

III. Legal characterization of the offence and its forms in comparative legislation and international conventions

1. Between conduct offence and result offence

Most legislators – including the Algerian, French and Moroccan legislators – consider the offence of illegal access to, or unlawful remaining in, an information system to be a conduct (formal) offence in its simple form, as the commission of the criminalized conduct – access or remaining – is sufficient for the offence to be constituted, without the need for actual damage to the system or the data. This is justified by the fact that the act represents a danger-type offence, since mere unauthorized access to the system exposes the confidentiality of data and the integrity of the system to risk, even if the harm has not materialized.

However, the offence becomes a result-type offence in its aggravated form, when the law links aggravation to the occurrence of specific results, such as the deletion, alteration or erasure of data, or the impairment, disruption or destruction of the system, or the serious hindering of its operation as expressed in the Budapest Convention. In this case, a causal link must exist between the act of access or remaining and the resulting harm, so that the act is the direct cause of the interference with the data or the functioning of the system.

2. The Budapest Convention and the model of “serious hindering”

The 2001 Budapest Convention attaches particular importance to the protection of data and information systems^[12]. It provides in Article 2 for the offence of illegal access, in Article 3 for the illegal interception of data, in Article 4 for the offence of data interference, and in Article 5 for the offence of “system interference”. The latter is constituted where there is serious hindering of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

It follows that the Convention does not require the complete destruction of the system or the total loss of its function; rather, it is sufficient to cause serious interference with its operation^[13]. This approach expands the protection afforded to systems compared with some legislation that associates aggravation with the loss by the system of its ability to perform its function or with its complete destruction. However, the use of the expression “serious hindering” raises concern from the standpoint of precision, since it is a relative criterion whose assessment may vary between legal systems, although the guiding nature of the Convention leaves States a wide margin in its definition.

3. The debate on requiring technical security measures

Scholars have debated whether the criminalization of illegal access or unlawful remaining presupposes that the information system is protected by technical measures (passwords, firewalls, encryption), such that the offence is constituted only when these protections are breached. One view requires the existence of a security system, on the basis that fraud can only be realized by breaching existing protection, and that fairness does not call for protecting those who neglect to take the necessary precautions to secure their information.

Another view rejects this condition on the grounds that it unduly limits the scope of protection, undermines the principle of equality, and imposes on the legal text a requirement that it does not contain, especially where the legislator has remained silent on the necessity of a specific security measure^[14].

This study leans towards supporting the view that does not require the prior existence of technical protection for the offence to be constituted, in line with the principle of legality and with the preventive function of criminal law in protecting individuals and entities that may not possess adequate technical means to secure their systems. Linking criminalization to the existence of technical protection would leave the majority of individual users outside the scope of protection, at a time when internet-connected devices and smartphones themselves have become automated data processing systems that merit protection^[15].

IV. The mental element of the offence of illegal access or unlawful remaining

This is an intentional crime requiring “criminal intent”: perpetrator’s knowledge of entering an unauthorized system or persisting without permission, with free will directed to the act, aware of illegality. Unintentional erroneous entry does not constitute crime unless followed by deliberate persistence post-discovery.

1. General criminal intent

The offence of illegal access to, or unlawful remaining in, an information system is an intentional offence based on general criminal intent with its two elements: knowledge and will. Knowledge consists in the offender’s awareness that he is accessing or remaining in an information system to which he has no right of access^[16], or that he is exceeding the spatial, temporal or functional limits of the authorization granted to him, and of the implications this has for the privacy of the system and the confidentiality and integrity of the data. General intent is negated where the offender believes – for reasonable reasons – that the system is open to access, or that he has valid authorization, or where access occurs by mistake, oversight or accident, provided that he hastens to disconnect upon learning of the illegality; otherwise his conduct turns into unlawful remaining if he deliberately continues to stay within the system^[17].

The element of will is represented by the direction of the offender’s will towards committing the act of access or remaining, so that the conduct emanates from him consciously and voluntarily, without coercion or lack of discernment. This is realized as soon as he chooses to log into the system or refrains from exiting it after knowing the illegality of his

presence. Motive is irrelevant in this respect; thus, a person who accesses out of curiosity, desire to explore, or to test his technical ability is not exempted from liability as long as general intent is present.

In the aggravated form of the offence, it is further required that the offender's knowledge and will extend to the consequences of his conduct – such as deleting or altering data or damaging or disabling the system – so that he foresees and accepts or seeks these results; otherwise, criminalization is limited to the simple form.

2. The debate on special intent

There has been a doctrinal disagreement as to whether this offence requires, in addition to general intent, a special criminal intent, such as the intention to obtain unlawful gain or to commit another offence (theft, fraud, extortion, etc.). One trend in French doctrine has inferred a special intent from the legislator's use of the term "fraud", whereas another trend considers that the provision requires only general intent and that the reference to "fraud" or "deception" is merely a reiteration of the element of knowledge of illegality.

Some legislations have in fact required a special intent. The English Computer Misuse Act, for example, requires that access be made with the intent to commit a further offence, the Portuguese law requires an intent to obtain unlawful profit or benefit^[18], and the UAE Cybercrime Law stipulates special intent in certain cases, such as accessing confidential government data^[19]. By contrast, neither the Algerian nor the French legislator requires such special intent, which is the position favored by this study, on the basis that requiring a special purpose narrows the scope of criminalization, makes proof more difficult in practice, and opens the door for many offenders to escape liability by arguing the absence of a specific ulterior aim.

Consistently with this, the Budapest Convention allows States Parties – in paragraph 2 of Article 2 – to require special intent if they so wish, but does not oblige them to do so, in recognition of differences in legal, social and technical circumstances between countries. It appears that confining the requirement to general intent is more consistent with the nature of the offence as a pure conduct crime and with the preventive aim of criminalization, which is to deter unauthorized intrusion into information systems from the outset.

V. Criminal policy and prescribed penalties

Penalties vary by legislation, typically principal (imprisonment/fines) and complementary. Subject to attempt and complicity rules, moral person liability.

The Algerian legislator classifies the offence of illegal access to, or unlawful remaining in, an automated data processing system as a misdemeanor, and provides in its simple form for imprisonment from three months to one year and a fine ranging from 50,000 to 200,000 dinars, with harsher penalties in the aggravated form where the act is associated with the deletion or alteration of data or the damaging of the functioning of the system. The legislator doubles the penalty in certain cases, particularly when the targeted information system belongs to sensitive entities such as national defense, public security or certain public-law legal persons, and distinguishes between penalties applicable to natural persons and those applied to legal entities.

Other legislations tend towards a combination of custodial and financial penalties, with aggravating circumstances linked to the nature of the system owner or of the data targeted. The Moroccan law, for instance, provides for imprisonment and a fine with doubled penalties in case of deletion or alteration of data or disturbance of the functioning of the system, while the Dubai law increases penalties when the data is of a personal nature, in recognition of the seriousness of attacks on personal data in the digital environment^[20].

Aggravation occurs for government/banking targets or data deletion/system disruption, escalating from simple to aggravated misdemeanor in cases: data integrity breach (deletion/modification/distortion); system disruption (DDoS); during duty performance, organized crime, cyberterrorism aim; targeting sovereign systems like national defense or national security

This gradation of penalties, and the differentiation between simple and aggravated forms and between ordinary systems and those of particular importance, reflects an attempt to strike a balance between general and specific deterrence and to avoid excessive criminalization and punishment in cases of minor or low-impact intrusions. Nevertheless, the study argues for greater precision in defining the scope of some aggravating circumstances and for the harmonization of terminology ("damage", "disruption", "destruction", "impairment", etc.) so as to reduce opportunities to exploit textual ambiguity to evade punishment.

VI. Proof and Judicial Pursuit Challenges

Justice systems face key hurdles:

- Detection difficulty: Breaches often leave no tangible traces; perpetrators use log-erasing software.
- Digital evidence volatility: Easily altered/deleted, requiring high expertise and swift preservation.
- Concealment techniques: VPNs or Tor networks hide IP addresses.

-Cross-border nature complicates jurisdiction: Where did it occur (perpetrator's location or server)? Perpetrator in one country, server in another, victim in third—yielding international jurisdictional conflicts and extradition issues.

VII- Results and discussion :

The analysis shows that the Algerian legislator – drawing on the French model and guided by international conventions and certain Arab legislations – has adopted a criminal policy based on criminalizing the mere act of illegal access to, or unlawful remaining in, automated data processing systems, with an aggravated form where there is interference with data or with the operation of the system. This model reflects an awareness that this offence constitutes the “gateway” through which various other computer crimes are committed, which justifies granting it a central position within the system of criminalization.

Strengthening the criminal protection of automated data processing systems remains a prerequisite for consolidating trust in electronic commerce and digital transactions more generally, which requires the Algerian legislator – like comparative legal systems – to continue updating its provisions to keep pace with rapid technological change, and to support them with effective procedural tools and with institutional structures capable of investigation and technical expertise in complex computer crimes.

VIII- Conclusion:

The study affirms that confining the requirement to general criminal intent, without requiring prior technical protection of the system or a special intent, is consistent with the principle of legality and affords broader protection to users of information systems, individuals and institutions alike, especially in an environment in which opportunities for technical attacks increase as tools available to offenders evolve. It also highlights the importance of legislative precision in defining aggravating results and distinguishing between degrees of interference with the functioning of the system, in a way that ensures the alignment of applicable provisions with the guiding standards laid down by the Budapest Convention and other relevant international instruments.

Unauthorized access/persistence in automated data systems is no longer mere technical mischief but a grave national/economic security threat. The study shows effective confrontation demands integrated procedural, technical, international cooperation beyond deterrent laws. Protecting cyberspace safeguards modern society; upholding "sanctity" of digital life rivals physical home inviolability.

IV-Recommendations

The study concludes with technical/legislative recommendations:

- Continuous legislative updates to refine definitions/terms, precisely defining "system" (including cloud servers), clarifying "persistence" legally, distinguishing data types (personal, sensitive, public).
- Periodic penal text reviews to match evolving hacking/cyberattack methods, specifying tools, addressing social engineering.
- Judicial training: Specialized courses for judges, prosecutors, judicial police on digital evidence/investigations per international standards.
- Enhance international cooperation: Activate mutual legal assistance/extradition treaties, simplify info-sharing on cross-border attacks; joint training/expertise exchange, expanded global initiatives.
- Security awareness: Promote cybersecurity culture among institutions/individuals to reduce unauthorized access success.

X- Referrals and References :

1. د. علي عبد القادر القهوجي: "الجرائم المتعلقة باستخدام البطاقات المغنطة"، الجديد في أعمال المصارف من الوجهتين القانونية والاقتصادية (بحث) مقدّم في أعمال المؤتمر السنوي لكلية الحقوق لجامعة بيروت العربية)، الجزء الثالث، الجرائم المتعلقة بأعمال المصارف، منشورات الحلبي الحقوقية، بيروت، لبنان، ط2002.
 2. د. جميل عبد الباقي الصغير: "الإنترنت والقانون الجنائي: الأحكام الموضوعية للجرائم المتعلقة بالإنترنت"، دار النهضة العربية، القاهرة، مصر، 2002.
 3. د. عبد الفتاح بيومي حجازي: "الأحداث والإنترنت" دار الفكر الجامعي، الإسكندرية، مصر، 2002.
 4. د. أحمد حسام طه تمام: الحماية الجنائية لتكنولوجيا الاتصالات، دراسة مقارنة"، دار النهضة العربية، القاهرة، مصر، 2002.
 5. د. محمد عبيد الكعبي: "الحماية الجنائية للتجارة الإلكترونية – دراسة مقارنة"، رسالة دكتوراه، كلية الحقوق، القاهرة، مصر، 2009.
 6. مروة زين العابدين سعد صالح: "الحماية القانونية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني"، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، مصر، 2014.
 7. د. دلخاز صلاح بوتاني فرحان: "الحماية الجنائية الموضوعية للمعلوماتية في القانون العراقي- دراسة مقارنة"، رسالة ماجستير، كلية الحقوق، جامعة الإسكندرية، 2015.
1. QUEMENER Myriam Et CHARPENEL Yves ; *Cybercriminalité : Droit pénal appliqué* ; Economica, Paris 2010.
 2. R. GASSIN, *Informatique (fraude informatique)*, DALLOZ, Paris 1988.
 3. HALLABI, A. (2026) Cybercrime in Algerian law and Islamic Shari'ah. art law and accounting reporter, 45(1), 18-29. <https://journalar.org/index.PHP/online/article/view/30> p.20.
 4. UNESCO, Global Perspectives on Cybercrime Prevention, (2023), Paris : UNESCO Press, pp. 234-267.
 5. Olivier Douzou, *Droit Pénal et Infractions Informatiques*, 3ème éd., (2022), Paris : Éditions Dalloz, pp. 456-498.
 6. Jean-Pierre Baud, *Criminalité Numérique et Justice Pénale*, 4ème éd., (2023), Paris : Éditions LexisNexis, pp. 567-612.
 7. International Telecommunications Union (ITU), *Global Cybercrime Statistics*, (2023), Geneva: ITU Publications, pp. 89-124.
 8. UNODC, The Convention on Cybercrime (Budapest Convention, 2001), <https://www.unodc.org/unodc/en/organized-crime/cybercrime/>
- Budapest Convention on Cybercrime, Council of Europe, <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>
-
- [1] - HALLABI, A. (2026) Cybercrime in Algerian law and Islamic Shari'ah. Art law and accounting reporter, 45(1), 18-29. <https://journalar.org/index.PHP/online/article/view/30> p.20
- [2] - UNODC, The Convention on Cybercrime (Budapest Convention, 2001), <https://www.unodc.org/unodc/en/organized-crime/cybercrime/>
- [3] - Budapest Convention on Cybercrime, Council of Europe, <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>
- [4] - QUEMENER Myriam Et CHARPENEL Yves ; *Cybercriminalité : Droit pénal appliqué* ; Economica, Paris 2010. p. 55.
- [5] - د. علي عبد القادر القهوجي: "الجرائم المتعلقة باستخدام البطاقات المغنطة"، الجديد في أعمال المصارف من الوجهتين القانونية والاقتصادية (بحث) مقدّم في أعمال المؤتمر السنوي لكلية الحقوق لجامعة بيروت العربية)، الجزء الثالث، الجرائم المتعلقة بأعمال المصارف، منشورات الحلبي الحقوقية، بيروت، لبنان، ط2002، ص: 49
- [6] - Moroccan Code of Criminal Procedure, Article 607-3, (2009 amendments)
- [7] - Qatari Criminal Code, Article 372, (2004 amendements).
- [8] - UNESCO, Global Perspectives on Cybercrime Prevention, (2023), Paris: UNESCO Press, p. 250.
- [9] - Olivier Douzou, *Droit Pénal et Infractions Informatiques*, 3ème éd., (2022), Paris : Éditions Dalloz, pp. 459.
- [10] - جميل عبد الباقي الصغير: "الإنترنت والقانون الجنائي: الأحكام الموضوعية للجرائم المتعلقة بالإنترنت"، دار النهضة العربية، القاهرة، مصر، 2002، ص: 3.

- [11] - Jean-Pierre Baud, *Criminalité Numérique et Justice Pénale*, 4ème éd., (2023), Paris : Éditions LexisNexis, p. 599.
- [12] - د. عبد الفتاح بيومي حجازي: "الأحداث والإنترنت" دار الفكر الجامعي، الإسكندرية، مصر، 2002، ص:37
- [13] - International Telecommunications Union (ITU), *Global Cybercrime Statistics*, (2023), Geneva: ITU Publications, p. 122.
- [14] - د. أحمد حسام طه تمام: الحماية الجنائية لتكنولوجيا الاتصالات، دراسة مقارنة، دار النهضة العربية، القاهرة، مصر، 2002، ص 266.
- [15] - دلخاز صلاح بوتاني فرحان: "الحماية الجنائية الموضوعية للمعلوماتية في القانون العراقي- دراسة مقارنة"، رسالة ماجستير، كلية الحقوق، جامعة الإسكندرية، 2015. ص 201.
- [16] - جميل عيد الباقي صغير، القانون الجنائي والتكنولوجيا الحديثة – الكتاب الأول-الجرائم الناشئة عن استخدام الحاسب الآلي"، مرجع سابق 1992، ص20
- [17] - عبد الفتاح بيومي حجازي، مرجع سابق، ص37.
- [18] - R. GASSIN, *Informatique (fraude informatique)*, DALLOZ, Paris 1988, p 13.
- [19] - محمد عبيد الكعبي: "الحماية الجنائية للتجارة الإلكترونية – دراسة مقارنة"، رسالة دكتوراه، كلية الحقوق، القاهرة، مصر، 2009، ص34.
- [20] - مروة زين العابدين سعد صالح: "الحماية القانونية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني"، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، مصر، 2014، ص 200.