

The difficulty of determining the legal characterization of emerging cybercrimes**PhD Student: Brik Soumia****University of alshahid Sheikh Larbi Tebessi- Tebessa-****asmabrik29@yahoo.com****Supervisor: Dr. Mounir Bouras****mounir.bouras@univ-tebessa.dz**

Received: 06/07/2025

Accepted: 16/07/2025

Published: 04/11/2025

Abstract:

Modern legal systems are increasingly challenged by the difficulty of legally qualifying emerging cybercrimes due to their rapid evolution and complex technological nature. This paper aims to highlight the shortcomings of traditional legal frameworks and examine the problematic nature of the legal classification of novel cyber-offenses, such as digital extortion, cyber fraud, and privacy violations. Adopting both a theoretical approach—through the analysis of definitions and legal elements—and a practical one—by comparing legislative and judicial experiences—the article proposes conceptual and normative criteria to guide the legal qualification of these emerging crimes, in line with recent developments in legislation and legal scholarship.

Keywords: Cybercrime, legislative innovation, criminal law, digital extortion, digital privacy.

الملخص:

تواجه المنظومات القانونية في العالم اليوم تحديًا متزايدًا يتمثل في صعوبة التكييف القانوني للجرائم الإلكترونية المستحدثة، نظرًا لتطورها المتسارع وخصائصها التقنية المعقدة. يهدف هذا المقال إلى تسليط الضوء على مواطن القصور في الأطر التشريعية التقليدية، وإبراز الإشكالات التي يطرحها الوصف القانوني للأفعال الإلكترونية المستحدثة، مثل الابتزاز الرقمي، والاحتيال السيبراني، وانتهاك الخصوصية. ويجمع المقال بين المقاربة النظرية، من خلال تحليل المفاهيم والأركان، والمقاربة التطبيقية من خلال مقارنة نماذج تشريعية وتجارب قضائية. كما يقترح المقال معايير مرجعية تساعد في ضبط التوصيف القانوني لهذه الجرائم المستحدثة، استنادًا إلى تطورات الفقه والتشريع.

الكلمات المفتاحية: الجرائم الإلكترونية، التوصيف القانوني، الابتكار التشريعي، التكييف، القانون الجزائي، الابتزاز الرقمي، الخصوصية الرقمية.

Introduction

In recent decades, the world has witnessed rapid transformations driven by the digital revolution, which has impacted all sectors of life—including the realm of crime. This revolution has given rise to new types of offenses that differ fundamentally from traditional crimes in terms of methods, perpetrators, and the nature of harm caused. These developments have revealed the limitations of traditional legal frameworks in dealing with such crimes, particularly regarding their legal characterization. Judges and public prosecutors often find themselves faced with novel situations that are difficult to classify under existing criminal laws, opening the door to conflicting interpretations or legal gaps that may allow offenders to escape punishment.

Research Problem

This study is guided by the following central research question:

To what extent do emerging cybercrimes present a challenge in terms of legal classification? Are existing legal provisions sufficient to accurately characterize such offenses, or is there an urgent need to develop new legislative tools that reflect their specific nature?

Study Objectives

This paper aims to:

1. Analyze the concept of legal classification of crimes and its importance within the criminal justice system.
2. Diagnose the challenges posed by cybercrimes with respect to legal characterization.
3. Highlight the shortcomings of traditional legislation in light of digital advancements.
4. Propose criteria for developing improved legal classification mechanisms for digital offenses.
5. Present a comparative analysis of legislative models from both Arab and Western legal systems.

Methodology

This study adopts a dual-method approach:

- **Theoretical Method:** To examine the legal concepts related to classification and cybercrimes, and to review contemporary legal literature
- **Comparative and Analytical Method:** By comparing various legislative and judicial experiences—both Arab and Western—and highlighting the solutions adopted to address the challenges of legal characterization.

1.1.1 The Criterion of the Technological Means Used in the Commission of the Crime

One of the most prominent criteria for distinguishing cybercrimes from conventional crimes lies in the technological means employed in their commission. In the digital age, crime no longer relies solely on traditional criminal behavior; rather, digital tools have become an integral part of the criminal act itself. Consequently, whether the means used are software-based or hardware-based, they play a decisive role in determining the legal classification (qualification) of the offense.

When lawmakers define a criminal act, significant importance is placed on the material element, i.e., the act or conduct constituting the offense. However, in the context of cybercrime, this act fundamentally changes, becoming intrinsically linked to the type of medium employed: Is it a spyware application? A hacking tool? A fraudulent website? This diversity of means lends independent legal significance to the technological instrument used.

The French legal system has adopted this approach in Article 323-1 of the Penal Code, which explicitly criminalizes "unauthorized access or continued presence in an automated data processing system," even in the absence of any resulting damage. This illustrates that the use of a technological means, when employed unlawfully, is sufficient to establish the legal characterization of the act (Boukhris, 2019, p. 134).

It is worth noting that some legal systems have begun to differentiate between acts that target information systems as an end in themselves and those that merely utilize technology as a means. For example, under Tunisian law, the mere "attempt to access a protected information system" constitutes a punishable offense—even if no data was obtained—pursuant to Law No. 5 of 2004. This indicates that the technological tool itself can legally define the nature of the act (Tarifi, 2022, p. 87).

In judicial practice, the Rabat Court of First Instance issued a ruling in 2018 concerning a defendant who had sent malicious links to victims with the intent of harvesting login credentials for their bank accounts. Although the act did not result in the theft of funds, the court held that the use of "malicious software" constituted an attempt to commit an information fraud offense and accordingly qualified it as such (Naciri, 2020, p. 241).

Comparative legal experiences demonstrate that the criterion of technological means goes beyond merely describing the tool used; it helps classify the nature of the act and distinguish it from similar behaviors conducted by traditional means. For instance, blackmail via email differs in legal qualification from blackmail committed through verbal or written threats, as the digital medium adds a specific technological dimension that necessitates a precise criminal description.

Therefore, adopting the criterion of technological means helps clarify the unique nature of cybercrimes and provides legislators with a framework to modernize legal systems in line with the evolving tools and methods of criminal activity.

1.1.2 The Criterion of Criminal Intent and the Extent of Specific Intent

Criminal intent constitutes one of the fundamental elements of an offense. It is not sufficient for an individual to commit a prohibited material act to be deemed a criminal; the act must also be accompanied by a conscious and deliberate criminal will. However, due to the technical nature of cybercrimes, this element poses significant challenges, as it is often difficult to determine whether the act was intentional or the result of an unintentional error in navigating the digital environment.

According to criminal jurisprudence, criminal intent requires that the perpetrator commits the act knowing its unlawful nature and desiring to achieve the criminal outcome. In the case of cybercrimes, actions may occur indirectly or through tools that can be used for both lawful and unlawful purposes. This complicates the judge's task in distinguishing between legitimate use and criminal misuse, thereby increasing the risk of misclassification.

In this context, some scholars have proposed the notion of “*specific cyber intent*”, which relies on technical indicators to infer criminal intent. These indicators include the use of advanced tools that are not easily accessed accidentally, the execution of actions requiring specialized skills beyond those of an ordinary user, or the employment of digital obfuscation techniques such as IP spoofing or the use of the dark web. This approach appears suitable for legally characterizing emerging crimes without resorting to excessive criminalization or arbitrary interpretation.

Ben Makhlouf, in his work on computer crimes, points out that criminal intent in cyber offenses can be inferred from the technical and temporal context of the act—especially in cases involving repeated behavior or the use of tools designed exclusively for unlawful purposes, such as spyware or malicious encryption software (Ben Makhlouf, 2021, p. 112).

In judicial practice, the Criminal Court of Algiers issued a ruling in 2021 against a defendant who had hacked the email account of an administrative official. The court held that unauthorized access alone was insufficient for conviction. However, the defendant's retention of message copies and his attempt to transmit them to a third party clearly demonstrated the presence of *specific criminal intent*—namely, an intent to harm and extort—which allowed the act to be legally qualified as an “infringement of informational privacy with intent to harm” (Akhder, 2022, p. 149).

From a comparative legal perspective, German law has developed the concept of “*technical intent*” in cybercrime. The use of tools such as keyloggers or rootkits is considered a clear indicator of criminal intent, even if the intended result is not achieved. This reflects an expanded conception of the *mens rea* element, adapted to the non-traditional nature of digital crime (Jamal Eddine, 2020, p. 78).

In conclusion, the criterion of criminal intent—if reinterpreted within the digital context—can serve as an effective entry point for determining the legal classification of cybercrimes. However, this should be done cautiously, ensuring that the principle of legality in

criminalization is not undermined by overextension, nor should it be so narrowly applied as to hinder the protection of sensitive digital interests.

1.1.3 The Criterion of the Legal Interest Infringed

Determining the nature of the legal interest affected by a criminal act is one of the most prominent criteria that can assist in the legal classification of emerging cybercrimes. This is particularly relevant given that such crimes often target multiple and diverse interests—ranging from individual freedoms and privacy to digital property, and even extending to national security or a state's digital sovereignty.

This criterion originates from traditional criminal jurisprudence, which classifies crimes according to the violated right: crimes against persons, property, or the state. However, the digital realm introduces a new complexity, wherein a single offense may simultaneously affect multiple legal interests, or may target immaterial interests such as data confidentiality or trust in information systems.

For example, the hacking of a medical institution's database not only constitutes a breach of data confidentiality but also directly threatens individual privacy and public health. Therefore, legal classification should not be limited to a technical description of the act, but must also consider the specific legal value being violated.

Some legislations have explicitly adopted this approach. Notably, French Law No. 2004-575 on confidence in the digital economy distinguishes between crimes that affect data confidentiality, those that affect data integrity, and those that threaten availability. Each legal interest, therefore, is associated with a distinct legal description that necessitates a differentiated classification of the act (Zouaoui, 2020, p. 203).

In Algerian judicial practice, a 2022 ruling from the Sidi M'hamed Court convicted a defendant who had published private photos of a young woman via a fake social media account. Although the photos were neither altered nor published under threat, the court ruled that the mere act of dissemination constituted an infringement of the right to privacy. Accordingly, the act was legally classified as a violation of *digital privacy*, rather than merely “unlawful use of media” (Bouamama, 2023, p. 174).

Legal scholars have further argued that this criterion helps avoid legislative confusion in cases involving multifaceted actions. For instance, the theft of banking data infringes upon *digital property*, whereas the publication of personal messages violates *privacy*. Each act requires a legal classification aligned with the particular interest affected—even if the technological methods are similar or repetitive.

Researcher Leila Razouki, in her comparative study between Algerian and Moroccan legislation, observed that applying the legal interest criterion allows judges to reinterpret traditional legal texts to encompass cybercrimes, without the need to constantly introduce

new laws. This approach enhances the flexibility and efficiency of the legal system (Razouki, 2021, p. 97).

In light of the above, it can be concluded that the criterion of legal interest not only supports the proper legal classification of cybercrimes, but also guides penal policy more precisely. It allows for crimes to be ranked based on their actual severity, according to the type of protected values they threaten. This ensures a more balanced protection of rights within the digital environment.

1.1.4 The Criterion of Comparative Judicial Precedent

Comparative judicial precedent is considered one of the key methodological tools for understanding and legally classifying emerging cybercrimes—particularly in light of the slow pace of national legislation in keeping up with rapid technological advancements. While legal texts may lag in defining newly emerging acts within the digital environment, courts in certain legal systems may already have addressed such acts through foundational rulings that serve as references in the absence of explicit statutory provisions.

This criterion grants national judges a degree of interpretive flexibility, enabling them to draw on the precedents established by high courts in legally advanced jurisdictions such as France, Germany, or Canada. These precedents may involve the legal characterization of highly specific digital offenses such as identity forgery, the misuse of artificial intelligence, or transnational cyber extortion. Despite differences in legal systems, the general principles underpinning such case law are often aligned with the overarching doctrines of criminal law, making them adaptable to local contexts.

For instance, Algerian courts have referenced French judicial precedent in classifying cyber extortion cases, particularly when national legislation lacks clear provisions. In a 2021 ruling by the Algiers Court of Appeal, the judge cited a decision by the French Court of Cassation, which held that sending sexually explicit images for the purpose of extorting money from the victim constitutes “digital threat with intent to profit”—even if the images were neither altered nor fabricated. This interpretation supported the classification of the act as a felony rather than a mere misdemeanor (Kherfi, 2022, p. 109).

Similarly, Moroccan judges have relied on Canadian precedent when interpreting criminal intent in digital forgery cases. They referred to a ruling by the Supreme Court of Canada in *R. v. Vu*, which held that merely creating a digital file containing false data was sufficient to constitute the offense, without the need to prove subsequent use. This interpretation reinforced the notion that the intent to commit digital forgery is manifested in the technical preparation of the act itself, not in its eventual outcomes (Zitouni, 2020, p. 144).

Researcher Rania Ben Turkî emphasizes that comparative judicial precedent should not be understood as the literal transplantation of foreign rulings. Rather, it is a tool of legal analysis that helps overcome the rigidity of domestic legal texts—especially given that digital environments across jurisdictions often present similar challenges, such as

anonymity techniques, digital fingerprints, and distributed cyber offenses (Ben Turkî, 2021, p. 63).

Ultimately, incorporating comparative judicial precedent into the legal classification of cybercrimes fosters the development of transnational legal thought. It also enhances the capacity of national legal systems to address technological developments, without undermining the principle of legality or compromising local legal particularities.

5. Le critère de la flexibilité législative à travers des formulations juridiques non fermées

L'un des défis majeurs posés par les infractions cybernétiques émergentes aux systèmes juridiques contemporains réside dans la capacité des textes législatifs à suivre le rythme effréné des évolutions technologiques. Le droit pénal repose, par essence, sur le principe de légalité, selon lequel il ne peut y avoir ni crime ni peine sans texte. Ce principe confère souvent au droit un caractère rigide, alors que la cybercriminalité évolue et se diversifie en temps réel, dépassant fréquemment les capacités des textes en vigueur.

Dans ce contexte, il devient impératif d'adopter des formulations juridiques souples, susceptibles d'interprétation en fonction des faits et des évolutions technologiques, tout en conservant la rigueur et la précision juridique nécessaires. Il n'est pas raisonnable que le législateur intervienne à chaque apparition d'un nouveau type de crime. Il serait plus judicieux de prévoir des dispositions législatives capables de s'adapter continuellement.

Le législateur français a suivi cette orientation en recourant, dans l'article 323 du Code pénal, à des expressions ouvertes telles que « l'accès frauduleux », « l'atteinte à un système d'information » ou encore « la conservation illicite de données ». Ces formulations permettent au juge d'englober une diversité d'actes sous un même cadre juridique, sans porter atteinte au principe de légalité (Taya, 2019, p. 122).

En Algérie, bien que la réforme du Code pénal de 2004 n'ait pas totalement répondu à l'évolution de la cybercriminalité, certaines dispositions à portée générale telles que « l'accès illicite » ou « la fraude informatique » ont permis aux juridictions de sanctionner des actes non expressément visés par la loi, comme les arnaques via des applications intelligentes ou la diffusion de liens malveillants. Ces décisions se sont appuyées sur la souplesse des textes plutôt que sur une incrimination spécifique de chaque acte (Bouزيد, 2021, p. 215).

Une étude traduite menée par la Faculté de droit de l'Université de Milan montre que les législations les plus efficaces dans la qualification des infractions cybernétiques sont celles qui utilisent des « normes souples encadrées », c'est-à-dire des concepts généraux assortis de limites précises d'application. À titre d'exemple, considérer que « tout acte causant une perturbation dans un système d'information sans autorisation préalable » constitue en soi une infraction, permet d'englober une multitude de comportements techniques sous cette disposition (Khaled, 2022, p. 98).

Ce critère met en évidence l'importance d'un équilibre législatif entre la nécessité d'encadrer les comportements nouveaux et la garantie des droits constitutionnels, notamment le principe de légalité des délits et des peines. Plus la formulation est souple mais encadrée, plus elle permet d'anticiper les réalités numériques sans sombrer dans l'arbitraire ou la violation des libertés individuelles.

Ainsi, le critère de flexibilité législative constitue un fondement essentiel dans la qualification juridique des cybercrimes, en particulier dans un environnement où apparaissent chaque jour de nouvelles formes d'infractions inédites, telles que l'usurpation d'identité par intelligence artificielle ou les techniques de piratage via les réseaux blockchain.

Conclusion :

Il ressort de cette étude que la difficulté de la qualification juridique des cybercrimes émergents ne réside pas uniquement dans la complexité de l'environnement technologique, mais également dans les limites des outils de qualification traditionnels utilisés en droit pénal. Cette interaction entre la nature technique de l'acte et le vide juridique a parfois conduit à une confusion dans la description des faits, que ce soit au niveau du ministère public ou du pouvoir judiciaire, ce qui peut engendrer soit une insuffisance dans l'incrimination, soit un excès dans la qualification.

Le recours à des critères interprétatifs précis — tels que le moyen technique utilisé, l'intention criminelle spécifique, la nature de l'intérêt juridique lésé, la jurisprudence comparée, et enfin la flexibilité législative — peut contribuer à dépasser cette problématique, à condition de respecter les exigences du principe de légalité pénale, les droits fondamentaux des individus, et d'éviter toute extension arbitraire du champ d'application de la sanction pénale.

Par ailleurs, la comparaison avec les expériences étrangères a montré que les législations qui adoptent des concepts juridiques souples mais encadrés, et qui prennent en compte l'environnement numérique à travers des lois spécifiques ou des codes pénaux modernisés, parviennent mieux à qualifier les actes nouveaux sans compromettre les principes fondamentaux de la justice pénale.

Recommandations :

1. **Réviser les textes pénaux nationaux** pour y inclure des définitions précises et flexibles des infractions numériques, notamment les actes non traditionnels tels que le vol de données, la falsification numérique, et les atteintes aux systèmes.
2. **Créer une instance technique et juridique spécialisée**, chargée de surveiller les évolutions numériques et de proposer des interprétations normatives pouvant servir de jurisprudence consultative.

3. **Renforcer la formation spécialisée des magistrats et procureurs** dans le domaine de la criminalité informatique, notamment en ce qui concerne les techniques d'enquête numérique et les éléments de preuve de l'intention criminelle.
4. **Valoriser les jurisprudences comparées**, en particulier celles émanant des juridictions supérieures en France, au Canada ou en Allemagne, tout en respectant les spécificités constitutionnelles nationales.
5. **Développer la coopération judiciaire et législative internationale** pour faire face aux infractions transfrontalières, par le biais d'accords bilatéraux ou régionaux.

Referrals and references:

Books:

- الأخضر، ع. (2022). التطبيقات القضائية للجرائم المعلوماتية في الجزائر. الجزائر: منشورات المجد.
- بن تركي، ر. (2021). التكيف القضائي للجرائم الإلكترونية: دراسة في النظم المقارنة. تونس: مركز الدراسات القانونية الرقمية.
- بن مخلوف، ن. (2021). الجرائم الإلكترونية: دراسة تحليلية مقارنة. الجزائر: دار الخلدونية.
- بوخريص، ع. (2019). الجريمة المعلوماتية في التشريع المغربي والمقارن. الرباط: مطبعة النجاح.
- بوزيد، ع. (2021). الجريمة الإلكترونية في ضوء التعديلات التشريعية الجزائرية. الجزائر: دار الفقيه.
- بوعمامة، ي. (2023). التطبيقات القضائية للجرائم الإلكترونية في المحاكم الجزائرية. قسنطينة: دار الإشعاع.
- جمال الدين، ي. (2020). التكيف القانوني للجريمة الرقمية: قراءة في التشريع الألماني والمقارن. بيروت: منشورات الحلبي الحقوقية.
- خالد، س. (2022). المرونة التشريعية في القانون الجنائي الرقمي: دراسة مقارنة بين أوروبا والمغرب العربي. الجزائر: ترجمة منشورات جامعة ميلانو.
- رزوقي، ل. (2021). حماية المعطيات الشخصية في القانونين الجزائري والمغربي: دراسة تحليلية. الرباط: المركز المغربي للبحوث القانونية.
- الزواوي، ع. (2020). الجريمة الإلكترونية: دراسة مقارنة بين القانون الفرنسي والجزائري. الجزائر: دار الكلمة.
- زيتوني، ف. (2020). التزوير الإلكتروني: قراءة تحليلية مقارنة. الرباط: دار النشر الجامعي المغربي.
- الطابع، ج. (2019). التشريع الجنائي وتحديات الجرائم الرقمية: قراءة تحليلية. بيروت: مركز النهضة القانونية.
- الطريفي، س. (2022). الجرائم الإلكترونية في القانون التونسي والمقارن. تونس: دار الميزان.
- قرفي، م. (2022). الجرائم المعلوماتية في ضوء الاجتهاد القضائي المقارن. الجزائر: دار الأكاديميون.
- الناصر، أ. (2020). الإثبات في الجرائم المعلوماتية: دراسة تطبيقية. الدار البيضاء: دار الأمان.