An Analytical Study of the Departures from General Criminal Policy in the Jordanian Cybercrime Law of 2023

Mohamad Shible Abdulmajeed Alshible

mshible@jadara.edu.jo

Department of Law, Faculty of Law, Jadara University, Irbid, Jordan

Received: November 28, 2025 Accepted: June 10, 2026 Online Published: June 29, 2026

URL: https://journal.aut.edu.jo/index.php/aut

Abstract

In the digital era, cybercrime legislation has become a central concern for criminal justice systems worldwide. This study examines the approach adopted by the Jordanian legislator in the Cybercrime Law No. 17 of 2023 and evaluates its consistency with the general principles of traditional criminal law. The law reflects a preventive and deterrent orientation, evident in the expansion of criminalization and the imposition of harsher penalties. While this orientation aims to strengthen protection against cyber threats, it has sparked significant legal and doctrinal debate regarding its compatibility with the principle of legality, the safeguarding of rights and freedoms, and its departure from established rules of criminal liability. The analysis focuses on two main aspects: the legal structure of cybercrimes and the substantive provisions governing criminal participation and aggravating circumstances. Findings reveal that the law employs vague terminology that risks undermining the principle of legality, criminalizes preparatory acts without adequate safeguards, and imposes penalties disproportionate to the seriousness of certain offenses. Moreover, it equates principal offenders with accomplices, contradicting fundamental principles of liability. The study concludes with recommendations to revise ambiguous provisions, restrict the criminalization of preparatory acts to narrowly defined cases, leave the regulation of attempts to the Penal Code, adopt a more proportionate approach to penalties, and reinstate the distinction between different forms of participation. These reforms would enhance the coherence of the Cybercrime Law with general criminal law principles while ensuring a more balanced protection of rights and freedoms.

Keywords: Cybercrime; Criminal Policy; Preparatory Acts; Attempt; Proportionality; Criminal Participation

دراسة تحليلية لأوجه الخروج عن السياسة الجنائية العامة في قانون الجرائم الإلكترونية الأردني لسنة 2023

محمد شبلي عبد المجيد الشبلي

mshible@jadara.edu.jo

قسم القانون، كلية الحقوق، جامعة جدارا، اربد، الأردن

تاريخ الاستلام: 28 تشرين الثاني 2025 تاريخ القبول: 10 حزيران 2026 تاريخ النشر عبر الإنترنت: 29 حزيران 2026

الرابط الالكتروني: https://journal.aut.edu.jo/index.php/aut

الملخص

يتناول هذا البحث أوجه الخروج عن السياسة الجنائية العامة في قانون الجرائم الإلكترونية الأردني رقم 17 لسنة 2023، من خلال تحليل مدى انسجامه مع القواعد التقليدية لقانون العقوبات الاردني ومبادئ الشرعية والتناسب والعدالة. ينطلق البحث من أن مواجهة الجرائم الإلكترونية ضرورة تشريعية حقيقية، لكنها لا تبرر التوسع غير المنضبط في التجريم أو تشديد العقوبات بطريقة تمس الضمانات الأساسية للمسؤولية الجزائية. يركز البحث على البنية القانونية للجرائم الإلكترونية، ولا سيما استعمال بعض المصطلحات الفضفاضة، وتجريم الأعمال التحضيرية السابقة على مرحلة الشروع، وإدخال صور من التجريم قد تفتح المجال لتأويل واسع يمس الحقوق والحريات. كما يناقش موقف المشرع من الشروع، مبيناً أن ترك تنظيمه للقواعد العامة في قانون العقوبات هو الأصل الأنسب، وأن النص عليه في بعض مواد قانون الجرائم الإلكترونية قد يخلق ازدواجاً تشريعياً وإشكالات في التناسب. ويبحث كذلك قواعد المساهمة الجرمية والظروف المشددة، مبرزاً أن مساواة الفاعل الأصلي بالشريك أو المتدخل أو المحرض في العقوبة تمثل خروجاً عن مبدأ التدرج في المسؤولية بحسب دور كل مساهم وخطورته. كما يبين أن تشديد العقوبات ومضاعفتها في بعض الظروف قد يكون مبرراً في الجرائم الجسيمة، لكنه يصبح محل إشكال عندما يطبق على أفعال أقل خطورة أو نصوص قابلة للتوسع في التفسير. ويخلص البحث إلى ضرورة مراجعة بعض النصوص الغامضة، وتقييد تجريم الأعمال التحضيرية، واعتماد عقوبات أكثر تناسباً، وإعادة التمييز بين صور المساهمة الجرمية، بما يحقق توازناً أفضل بين مكافحة الجريمة الإلكترونية وحماية الحقوق والحريات. وتؤكد الدراسة أن فعالية القانون لا تتحقق بمجرد التشدد، بل بقدرته على حماية المجتمع دون إضعاف الضمانات التي يقوم عليها نظام العدالة الجنائية في دولة القانون المعاصرة ومجتمع رقمي متوازن.

الكلمات المفتاحية: الجرائم الإلكترونية، السياسة الجنائية، الأعمال التحضيرية، الشروع، التناسب، المساهمة الجرمية

1. Introduction

Cybercrime has become one of the most pressing challenges for modern criminal justice systems. Unlike traditional crimes, it generally crosses borders, exploits technological gaps, and often involves anonymous actors. This reality has forced legislators everywhere to rethink their criminal policies and to design legal frameworks that can respond to the risks of these crimes.

In Jordan, the legislative path has been gradual from issuing the temporary Law on the Protection of Information Systems in 2001, then the Cybercrime Law of 2015, and most recently the Cybercrime Law No. 17 of 2023. The latest law is not merely a continuation of earlier efforts; but it represents a clear shift in criminal policy in Jordan. The legislator has chosen a preventive and deterrent approaches, expanding criminalization and tightening penalties, which have not passed without criticism. Scholars, practitioners, and civil society have all raised concerns about whether the law respects the general principles of criminal law and the guarantees of rights and freedoms.

The research problem addressed in this study lies in the tension between the legislator's preventive ambitions and the fundamental guarantees of criminal justice. While the 2023 Law seeks to deter cybercrime through broader criminalization and harsher sanctions, it raises many questions about its consistency with the principles of legality, proportionality, and the differentiation of liability. The objective of this study is therefore to critically examine the Jordanian legislative approach adopted in the Cybercrime Law of 2023, to identify areas where it departs from established principles or the general principles, and to propose recommendations that may guide future reforms.

The significance of this research lies in its contribution to the ongoing debate on criminal policy in confronting cybercrimes. By focusing on the Jordanian context, the study not only sheds light on the evolution of national legislation but also addresses broader questions about how criminal law should adapt to technological changes without sacrificing its foundational principles. In doing so, it highlights the delicate balance between the state's duty to protect society from crimes and its obligation to safeguard individual rights and liberties. When provisions are vague, the principle of legality is weakened; when penalties are disproportionate, the legitimacy of the criminal justice system itself is questioned; and when preparatory acts are criminalized without safeguards, the risk of overreach becomes real, especially in the digital sphere, where the line between lawful and unlawful conduct is often too blurred.

The study of cybercrime legislation cannot be approached in isolation from the broader academic and legislative debates that have shaped the field over the past two decades. A literature review in this context serves not only to map the scholarly contributions and judicial interpretations that have addressed the phenomenon of cybercrime, but also to situate the Jordanian experience. By examining the relevant writings, statutory developments, and doctrinal controversies, this section provides the intellectual and contextual foundation upon which the subsequent analysis is built.

In particular, the article highlights how criminal policy in Jordan has evolved in response to the challenges of cybercrimes, moving from early attempts at regulating information systems to the more comprehensive framework embodied in the Cybercrime Law No. 17 of 2023. This evolution has generated significant debate in legal scholarships, especially concerning the extent to which the legislator has remained faithful to the general principles of criminal law. Scholars have questioned whether the expansion of criminalization, the treatment of preparatory acts, and the equalization of liability between principals and accomplices reflect a coherent policy or rather a departure from the general principles.

Moreover, it seems that the Jordanian struggle to balance the preventive ambitions of cybercrime law with the constitutional and doctrinal safeguards of criminal justice. By engaging with these debates, the present study situates itself within an ongoing scholarly conversation.

Accordingly, this section is organized into a series of sub-sections. Each sub-section addresses a specific dimension of the literature and contextual background: the criminal policy underlying the legal structure of cybercrime, the treatment of attempt and preparatory acts, and the rules of participation and differentiation of liability, and the role of aggravating circumstances. Together, these themes provide a comprehensive backdrop against which the critical analysis of the 2023 Jordanian Cybercrime Law will be conducted.

2. Background

2.1 Criminal Policy Concerning the Legal Structure of Cybercrime

Studying the legislator's attitude and policy regarding the legal structure of cybercrime requires more than a simple description of statutory provisions. It involves an examination of the constitutive elements of the offense, the boundaries that separate lawful conduct from criminalized behavior, and the dividing line between non-criminal stages, such as mere thought stage , intention stage , or preparation, and the criminal stages that, according to general criminal policy, begin with the commencement of the material element of the crime or the point of attempt. These distinctions are not merely technical; they reflect fundamental choices about how far criminal law should extend into the private sphere of individual autonomy and at what point the state is justified in imposing penal sanctions.

In the context of cybercrime, these questions become even more pressing. The digital environment blurs the line between preparatory acts and the actual execution, since many cybercrimes can be carried out with minimal physical action but significant preparatory planning. Such as the act of writing malicious code or acquiring hacking tools may remain in the preparatory stage for a long time, yet the legislator may be tempted to criminalize such conduct preemptively in the name of prevention. This raises the central issue of whether the expansion of criminalization into earlier stages of conduct is consistent with the principles of legality, proportionality, and fairness that underpin general criminal policy.

Accordingly, this part of the study is divided into two sections. The first examines the legislator's policy regarding the elements of cybercrime, with particular attention to how the material and moral elements are defined and whether they provide sufficient clarity to satisfy the principle of legality. The second addresses the legislator's approach in criminalizing in relation to the stages of the crime, focusing on the extent to which preparatory acts are brought within the scope of criminal liability and the implications of this choice for individual freedoms and rights and systemic coherence. Together, these two sections aim to shed light on the broader question of how the Jordanian legislator has constructed the legal framework of cybercrime and whether it represents a departure from the general policy traditionally observed in criminal law.

2.1.1 The Legislator's Policy Regarding the Elements of Cybercrime

This section focuses primarily on the material element of cybercrimes, since the mental element (criminal intent) remains largely identical in both traditional and cybercrimes. The Jordanian legislator, consistent with the general principles of the Penal Code, criminalizes only intentional acts, while unintentional conduct is punishable only when explicitly provided for by law which is limited to specific areas such as unintentional homicide and bodily harm. With respect to cybercrimes, the legislator has maintained this approach by punishing only intentional offenses, thereby preserving the traditional distinction between intentional and unintentional liability.

Examining the Cybercrime Law No. 17 of 2023 shows that the legislator has, to some degree, adhered to the general rules of criminalizing policy contained in the Penal Code. These rules divide the material element into three components: the act, the result, and the causal link. In certain categories of offenses, particularly endangerment crimes, the legislator suffices with the act alone to establish criminal liability, without requiring a tangible harmful result. In such cases, the risk created by conduct is deemed sufficient to justify legal intervention. This approach reflects a preventive orientation, but it also raises questions about proportionality and the limits of criminalization.

Nevertheless, several provisions of the 2023 Law reveal notable departures from these general principles:

2.1.1.1 Distinction Between Accessing a Network/System and Accessing a website
The Cybercrime Law criminalizes access to a system, network, or website, but the scope of criminalization differs significantly.

- Access to a system or network is treated as inherently criminal, with penalties imposed even for mere unauthorized entry. The punishment is aggravated if the intent is to damage data and further aggravated if the intended purpose is achieved (Article 3/a–b).
- By contrast, access to a website is criminalized only when accompanied by intent to alter, delete, damage, obstruct, encrypt, disable, or impersonate the site or its owner (Article 3/c). This distinction reflects an implicit recognition that websites are designed to be publicly accessible, and that mere access should not be punishable.

This differentiation illustrates the legislator's attempt to balance security concerns with the basic principle of legality, but it also highlights inconsistencies in defining the threshold of criminal conduct.

2.1.1.2 the attitude toward Defamation, Insult, and Contempt

The legislator has adopted a stricter stance by equating the penalty for contempt with that of defamation and insult (Article 15). Traditionally, contempt has been treated more leniently, as usually occurs in private settings without the element of publicity that characterizes defamation. By imposing equal penalties, the legislator departs from the general rules of proportionality, raising concerns about whether the severity of sanctions is justified in cases where the harm is limited to private exchanges.

2.1.1.3 attitude of the Crime of Character Assassination

Article 16 introduces, for the first time, the offense of "character assassination." The provision criminalizes the dissemination or attribution of acts that may result in the assassination of a person's character, through digital platforms. However, the law fails to specify what constitutes such acts, relying instead on vague terminology. This lack of precision undermines the principle of legality, as it opens the door to broad judicial interpretation and potential arbitrariness. Scholars have long warned that vague expressions in criminal law - such as "harm to dignity" or "assault on a person" - risk threatening individual rights and freedoms by enabling overly expansive interpretations. To protect against this, legislative drafting must employ clear and specific terms, confined to demonstrable acts, thereby reducing the risk of arbitrary enforcement and ensuring the protection of fundamental freedoms and rights.

2.1.1.4 Means of Committing Cybercrime

A further issue concerns the distinction between the object of a cybercrime and the means of its commission. The object is often data or information within a system, network, or website, but it may also involve individuals, entities, or institutions. The means, by contrast, refers to the method through which the offense is carried out. In cybercrimes, the means are typically electronic, involving the use of information networks, systems, or other technological tools. The Jordanian legislator has sought to clarify this distinction by employing precise terminology - such as "information network," "information system," and "means of information technology" in the 2023 Law. This precision is commendable, as it narrows the scope of interpretation, prevents ambiguity, and aligns with the principle of legality. At the same time, it reflects an awareness of the need to avoid unwarranted expansion of criminalization while ensuring that the law remains adaptable to technological aspects.

2.1.2 The Legislator's Policy on Criminalization in Relation to the Stages of Cybercrime

As is well established in general criminal law, a crime is deemed to begin with the execution of the act or the (actus reus) of the offense. Prior to this point, there are preliminary stages, such as thought, intention, and preparation. But generally, these are not punishable. These stages may

involve acts that facilitate or pave the way for the commission of a crime, but they remain outside the scope of criminal liability unless they themselves constitute an independent offense (Al-Majali, 2025). This principle reflects a long-standing policy of restraint, ensuring that criminal law does not intrude prematurely into the private sphere of individual autonomy.

Article 69 of the Jordanian Penal Code embodies this general approach by affirming the non-punish ability of preparatory acts. The rationale is clear: criminal liability should not be attached until conduct has moved beyond mere preparation and entered the stage of execution or attempt. This policy safeguards the principle of legality and prevents the imposition of sanctions on individuals whose conduct may never materialize into actual harm.

However, the emergence of cybercrime has challenged this traditional framework. The digital environment allows preparatory acts to carry significant risks, even in the absence of tangible harm. For example, creating malicious software, testing vulnerabilities, or acquiring hacking tools may remain in the preparatory stage for long periods, yet they pose real threats to information systems and social stability. In response to these unique risks, the Jordanian legislator, through the Cybercrime Law No. 17 of 2023, has adopted a different approach to deal with.

The 2023 Law extends criminalization into earlier stages of conduct, reflecting a preventive orientation that departs from the general policy of the Penal Code. While this shift may be justified by the need to protect digital infrastructure and deter harmful behavior before it escalates, it also raises fundamental questions about proportionality, legality, and the limits of state intervention. Understanding this policy therefore requires a closer examination of two key issues: the legislator's stance on attempt and the legislator's stance on preparatory acts. Together, these issues reveal the extent to which the Cybercrime Law represents a clear departure from established criminal policy and the implications of this departure for rights and freedoms of individuals.

2.1.2.1 The Legislator's Position on Preparatory Acts in Cybercrime

In the general criminal law, it is a firmly established principle that preparatory acts are not punishable. Article 69 of the Jordanian Penal Code reflects this rule, confirming that mere preparation, by itself, does not give rise to criminal liability unless the preparatory conduct is independently criminalized under the principle of legality (Al-Majali, 2025). The rationale is rooted in the idea that criminal law should not intervene too early, at a stage where the individual has not yet crossed the threshold into execution or attempt. This restraint protects individual freedom and ensures that the law does not punish mere thoughts, intentions, or acts that may never materialize into actual harm.

The Cybercrime Law of 2023, however, adopts a markedly different approach. Article 11 provides that:

"Anyone who, without authorization, possesses a device, program, or any electronic data prepared for use, or a password or access code, or provides, produces, distributes, imports, exports, or promotes them for the purpose of committing any of the crimes stipulated in this Law

shall be punished by imprisonment for no less than three months, or a fine of no less than 2,500 dinars and not exceeding 25,000 dinars, or both."

Although the provision does not explicitly employ the term "preparatory acts," its scope clearly extends to them. In effect, the legislator has chosen to criminalize conduct that, under general principles, would remain outside the reach of criminal law. This choice has been defended by some scholars who argue that cybercrimes, by their very nature, justify such an extension. Examples often cited include the purchase of hacking software designed to bypass passwords, or the possession of child pornography, both of which are considered inherently dangerous and therefore criminalized in many jurisdictions (Madeen, 2020). The rationale is grounded in prevention, deterrence, and the practical difficulty of detecting cybercrimes once they have been executed (Couzigou, 2019; Qc & Macdonald, 2014).

Yet, from a doctrinal perspective, this represents a significant departure from general principles. Punishing preparatory acts is problematic because such acts may be undertaken for legitimate purposes, for example academic research, professional training, or cybersecurity testing. For instance, a university student specializing in information security may lawfully possess penetration-testing tools as part of their study. Under Article 11, however, such possession could be interpreted as criminal act if linked - by assumption or suspicion - to an unlawful purpose. This creates a chilling effect on legitimate activities and risks discouraging innovation and research in the field of cybersecurity.

Moreover, Article 11 fails to provide a clear standard to distinguish between preparation and attempt. This ambiguity is particularly acute in the cybercrimes' context, where the line between preparation and execution is blurred. For example, downloading or creating a program capable of hacking an information system may be considered mere preparation in one jurisdiction, but an attempt - or even a completed crime - in another (Ramandhanizcha et al., 2023). Such uncertainty risks arbitrariness and undermines the principle of legality (Ohana, 2006).

The legislator has also gone further by treating preparatory acts as independent crimes, such as producing, distributing, or promoting devices, programs, or access codes. While this approach seeks to link preparatory conduct with criminal intent, it departs from established principles that generally require a specific intent to commit a particular offense before criminalizing preparatory behaviors (Bezugly et al., 2020). In traditional criminal law, preparation is not punishable unless it is tied to a clearly defined offense, such as conspiracy or possession of prohibited weapons. By contrast, Article 11 casts a wide net, criminalizing a broad range of preparatory behaviors without sufficient safeguards.

Finally, this legislative policy reveals internal inconsistency. Article 11 punishes preparatory acts as misdemeanors but attempts to commit misdemeanors under the same law are not punishable. This creates a paradox: preparatory acts, which are less dangerous, are criminalized, while attempts, which is more dangerous and represent a more advanced stage of criminal conduct, are not. Even more striking is the fact that preparatory acts may attract harsher penalties than some

completed crimes. For example, unlawful access in its basic form carries a penalty of one week to three months (Article 3), while preparatory acts carry a minimum of three months. Similarly, creating a fake webpage (Article 5) or publishing false news affecting national security (Article 15) may result in penalties equal to or lighter than those imposed for preparatory conduct. This imbalance highlights a lack of coherence in the legislative policy and raises serious questions about proportionality and fairness in the treatment of preparatory acts under the Cybercrimes Law.

From a policy perspective, the criminalization of preparatory acts may be seen as an attempt to adopt a preventive model of criminal justice, one that seeks to neutralize risks before they materialize. While this model may be attractive in the context of cybercrime, where the potential harm is significant and detection is difficult, it must be balanced against the fundamental guarantees of legality, proportionality, and individual rights and freedoms. Without such balance, the law risks overreach, arbitrariness, and the erosion of trust in the criminal justice system.

2.1.2.2 The Legislator's Position on Attempt in Cybercrime

Attempt occupies a central place in criminal law theory, as it reflects the tension between the principle of legality and the preventive ambitions of the state. Article 68 of the Jordanian Penal Code defines attempt as *"the commencement of executing an overt act leading to the commission of a felony or misdemeanor, where the perpetrator fails to complete the acts necessary for the occurrence of such felony or misdemeanor due to circumstances beyond his control"* (Al-Majali, 2025). This definition embodies the classical understanding that criminal liability may attach even when the harmful result has not materialized, provided that the offender has crossed the threshold of execution.

It is well established that legislators sometimes criminalize attempts based on the inherent danger posed by the offender, even in the absence of actual harm. In this regard, the Jordanian legislator did not generally address the punishment of attempts in the Cybercrime Law of 2023, leaving the matter to the general provisions of the Penal Code. This legislative choice reflects a policy of integration: The Cybercrime Law is not designed to stand apart from the Penal Code but to operate under its umbrella. However, there are two notable exceptions where the Cybercrime Law explicitly criminalizes attempts: (1) unlawful access to official websites (Article 4), and (2) electronic fraud (Article 10).

From the researcher's perspective, this approach is largely sound. There is no need to duplicate the provisions of the Penal Code, which already regulate attempts comprehensively. By relying on the general framework, the Cybercrime Law maintains consistency with the broader punitive policy and avoids unnecessary legislative inflation. At the same time, the two exceptions highlight areas where the legislator considered the risks sufficiently grave to warrant explicit regulation.

A. Attempt in Misdemeanors

The general rule is that attempts in misdemeanors are not punishable unless explicitly provided by law. If a provision exists, the attempt is punishable; otherwise, it is not. The Cybercrime Law includes such provisions in certain cases, such as unlawful access to information networks, information technology systems, or any part thereof belonging to ministries, government departments, public institutions, security or financial entities, or critical infrastructure. Article 4(e) provides: *"Attempts to commit the crimes stipulated in this Article shall be punishable by the same penalty prescribed for the completed crimes."*

Yet, the notion of "attempted access" is conceptually problematic. Since unlawful access is a crime of endangerment that is completed upon the act of entry itself, it is difficult to imagine an incomplete attempt. One either gains access or does not. This raises questions about whether the legislator has artificially extended the concept of attempting to cover preparatory behaviors that might better be classified under Article 11 as preparatory acts.

Similarly, Article 10 criminalizes electronic fraud in paragraph (a) and punishes attempts in paragraph (b) with the same penalty as the completed crime. While this reflects the seriousness of fraud, it also raises proportionality concerns. Equating the penalty for attempt with that of the completed crime may undermine the principle of gradation in punishment, which traditionally distinguishes between the danger of an incomplete act and the harm of a consummated offense.

B. Attempt in Felonies

Under the general provisions of the Penal Code, attempts to commit felonies are punishable without the need for a specific provision. This applies equally to felonies under the Cybercrime Law. Examples include:

1. Unlawful access to networks or systems belonging to ministries, government departments, public institutions, security or financial entities, or critical infrastructure, with the intent to delete, destroy, alter, or disclose sensitive data. Article 4(b) prescribes Temporary Imprisonment with Labor and fines, with Article 4(e) equating the penalty for attempt with that of the completed crime.

2. Unlawful access to official websites with the intent to tamper with or destroy sensitive data affecting national security, foreign relations, public safety, or the national economy. Article 4(d) prescribes Temporary Imprisonment with Labor and fines, with Article 4(e) again equating attempt with the completed crime.

3. Creating accounts, pages, or groups on social media platforms and falsely attributing them to official entities or public officials. Article 5 prescribes Temporary Imprisonment with Labor and fines, with attempts punishable under the general provisions of the Penal Code.

4. Intercepting or altering data transmissions involving official entities. Article 7(c) prescribes Temporary Imprisonment with Labor and fines, with attempts punishable under the general provisions of the Penal Code.

5. Cybercrimes involve financial systems such as money transfers, payment services, or banking operations. Articles 3, 5, 6, 7, and 8 prescribe Temporary Imprisonment with Labor and fines, with attempts punishable under the general provisions of the Penal Code.

6. Felonies subject to aggravated penalties due to aggravating circumstances under Article 28. These remain classified under their basic legal description, with attempts punishable under the general provisions of the Penal Code.

In this stage we can say that the legislative policy on attempts in cybercrime reveals both strengths and weaknesses. On the one hand, the reliance on the Penal Code ensures coherence and avoids unnecessary duplication. On the other hand, the explicit provisions in Articles 4 and 10 raise conceptual and proportionality issues. The idea of "attempted access" stretches the traditional definition of attempt, while equating the penalty for attempted fraud with that of completed fraud risks undermining the principle of proportionality. These tensions illustrate the broader challenge of adapting classical criminal law concepts to the digital environment, where the boundaries between preparation, attempt, and completion are often blurred.

2.2. The Jordanian Legislator's Position on Substantive Factors Affecting Criminal Liability

The study of crimes from a substantive perspective does not end with identifying the elements and components that constitute the offense. Beyond the (actus reus) and (mens rea), there are additional aspects that significantly affect the scope and degree of criminal liability. These aspects reflect the legislator's broader criminal policy and reveal how the law balances individual responsibility and collective security. Among the most important of these are the rules governing criminal participation and the treatment of aggravating circumstances.

Criminal participation arises when multiple offenders are involved in the same crime but with varying roles. Not all participants occupy the same legal position or perform the same function. Some may act as principal perpetrators, others as accomplices, and still others as instigators or facilitators. The legislator must therefore determine his policy in dealing with such distinctions: whether to apply the general principles of criminal law, which traditionally differentiate between these roles, or to introduce special provisions that treat all participants alike in certain categories of crimes. The choice between these approaches is not merely technical; it reflects deeper policy considerations about fairness, deterrence, and the distribution of liability.

Furthermore, a single crime may vary seriously depending on the time, place, or the individual involved. Certain circumstances - such as committing the offense against a public official, targeting critical infrastructure, or acting during a state of emergency - may aggravate the offense and justify harsher penalties. These aggravating circumstances compel the legislator to

establish a clear policy: should such factors be left to the general provisions of the Penal Code, or should they be specifically codified in the Cybercrime Law to reflect the heightened risks of the digital environment?

In this section, the article examines the Jordanian legislator's policy in addressing these two issues: (1) criminal participation, and (2) aggravating circumstances. The analysis will assess the extent to which the legislator has adhered to the general rules of criminal law or departed from them in the Cybercrime Law of 2023. By doing so, the study seeks to uncover whether the law maintains coherence with established principles or whether it introduces inconsistencies that may undermine the fairness and proportionality of the criminal justice system.

2.2.1 The Jordanian Legislator's Position on Criminal Participation in Cybercrimes

Criminal participation is traditionally defined as the commission of a crime by multiple persons, whether through principal participation - where all participants contribute directly to the material element of the crime - or through accessory participation, which involves acts related to the crime but not forming part of its material element, such as incitement, aiding, or concealing offenders or objects connected to the crime (Al-Majali, 2025). This distinction is not merely technical; it reflects a fundamental principle of fairness in criminal law, namely that liability should be proportionate to both: the role and danger posed by each participant.

The general provisions of the Jordanian Penal Code (Articles 80 - 84) regulate criminal participation and clearly distinguish between principal and accessory participation. However, Article 27 of the Cybercrime Law of 2023 departs from this framework by stipulating that anyone who intentionally participates, intervenes, or incites the commission of any of the crimes stipulated in the Law shall be punished with the same penalty prescribed for the principal offender. In effect, the legislator has equated principal and accessory participation, thereby erasing the traditional differentiation between varying degrees of involvement. This represents a significant departure from the general rules of the Penal Code.

By contrast, Article 26 of the same Law adopts a system of referrals, providing that anyone who commits a crime not stipulated in the Cybercrime Law but punishable under other legislation - when committed through electronic means - shall be punished with the penalty prescribed in that legislation. This dual approach creates uncertainty: in cases of participation, should the rules of the Penal Code apply, or those of the Cybercrime Law?

The inconsistency becomes clearer when comparing ordinary forgery and electronic forgery. Ordinary forgery is punishable under the Penal Code, where the rules of participation apply in their traditional form. Electronic forgery, however, falls under the Cybercrime Law, where the rules of participation differ. In practice, the Cybercrime Law treats the electronic nature of the crime as an aggravating circumstance, even though the underlying conduct is essentially the same. This approach risks undermining the principle of equality before the law and creates an artificial distinction based solely on the means of crime commission.

Moreover, the legislator has explicitly listed three forms of participation - participation, intervention, and incitement - in Article 27. Yet, intervention and incitement are already recognized forms of participation under the Penal Code, making the wording redundant and somewhat misplaced. At the same time, the legislator omitted concealment as a form of accessory participation when carried out pursuant to prior agreement, despite its recognition in law and jurisprudence (Al-Majali, 2025). This omission leaves concealment to be governed by the general provisions of the Penal Code, thereby creating an inconsistent and fragmented legislative framework.

The explanatory memorandum of the temporary Law No. 30 of 2010 on Information Systems Crimes sheds light on the legislator's reasoning. It clarified that many crimes were already addressed in the Penal Code or in special legislation and therefore did not need to be duplicated in the Cybercrime Law. However, it was deemed necessary to ensure that offenders would be punished even if electronic means were used instead of traditional ones. Accordingly, the Law was designed to cover all crimes criminalized by legislation whenever committed wholly or partially by electronic means, whether through commission, participation, incitement, or intervention (Alshible, 2019).

While this reasoning explains the legislative intent, it does not fully justify the departure from the general rules of participation. Cybercrimes may indeed have unique features that justify certain special provisions, but there is no compelling reason to abandon the principle that liability should be based on the degree of criminal danger posed by each participant. Treating all participants alike, regardless of their role, risks over-criminalization and undermines the fairness of the criminal justice system.

2.2.2 The Jordanian Legislator's Position on Aggravating Circumstances in Cybercrimes

The Jordanian legislator's approach in the Cybercrime Law reveals a clear tendency toward severity. This punitive orientation is reflected in two main forms: special aggravating circumstances that apply to specific crimes, and general aggravating circumstances that extend across a broader range of offenses. Together, these provisions demonstrate the legislator's intent to strengthen deterrence and to emphasize the seriousness of cybercrimes, particularly those that threaten financial stability, public order, or national security.

2.2.2.1 Special Aggravating Circumstances

Special aggravating circumstances are defined as *"conditions or elements expressly stipulated by the legislator in the provision of criminalization itself, such that if they are present in a given case, they lead to an increase in the penalty prescribed for the crime"* (Al-Masoudi, 2017).

Article 9 of the Cybercrime Law provides a clear example of this approach. It stipulates that:

"Anyone who commits any of the acts stipulated in Articles (3), (5), (6), (7), and (8) of this Law, if committed against an information system, information technology, website, or information

network related to money transfers, payment services, clearing or settlement services, or any banking or financial services provided by banks or financial companies, shall be punished by Temporary Imprisonment with Labor for no less than five years and a fine of no less than 25,000 dinars and not exceeding 75,000 dinars."

This provision illustrates how the legislator treats attacks on financial and banking systems as particularly grave. The aggravation here is objective or material, since it relates to the subject matter of the crime rather than the personal characteristics of the offender (Alshible, 2018). It is also special, as it applies only to the crimes listed in Articles 3, 5, 6, 7, and 8. The rationale is clear: financial systems are critical infrastructures, and any disruption to them may have cascading effects on the economy and public trust.

2.2.2.2 General Aggravating Circumstances

General aggravating circumstances, by contrast, are defined as *"conditions or elements stipulated by the legislator that apply to all crimes or to a broad category of them, and which, when present, lead to an increase in the prescribed penalty"* (Al-Masoudi, 2017).

The Jordanian legislator introduced a novel approach by dedicating Article 28 of the Cybercrime Law to a list of general aggravating circumstances that result in doubling the penalty. These include:

- If the offender commits the crime by exploiting his job, position, or granted authority.
- If there are multiple victims.
- If the crime is repeated. The Law explicitly provides repetition as a general aggravating circumstance for the crimes it covers, while repetition in other cybercrimes not listed remains governed by the Penal Code (Alshible, 2018).
- If the offender commits the crime for the benefit of a foreign state or an unlawful organization.

This approach reflects a deliberate policy choice: to emphasize the seriousness of cybercrimes when they involve abuse of trust, systemic harm, or threats to national security. However, it also raises questions about proportionality. For example, doubling the penalty for repetition may be justified in cases of fraud or hacking, but it may be excessive in cases involving less harmful conduct, such as minor online insults.

So, we can say that cybercrime Law reflects a punitive orientation. This is evident not only in the introduction of new aggravating circumstances and harsher penalties, but also in the equal punishment of all participants as principal offenders (Article 27). While such severity may be justified in certain crimes, such as violations of privacy, financial fraud, or character assassination, it appears less justified in others.

Take, for instance, the crime of publishing false or misleading news. If interpreted broadly, this provision could be misused as a tool to suppress freedom of expression. A careful and restrictive interpretation is therefore essential to prevent the law from being weaponized against legitimate criticism or public debate. At the same time, effective legal mechanisms must be provided to protect individuals who face harassment, threats, or reputational harm due to their use of social media.

From the researcher's perspective, the legislator's tendency toward severity is linked to the rapid development of information technology and the growing risks associated with cyberspace. The rationale is preventive: to deter offenders before harm escalates and to ensure both general and specific deterrence. Yet, the challenge lies in ensuring that this preventive ambition does not undermine fundamental rights or lead to disproportionate sanctions.

Interestingly, the legislator balanced this severity with a mitigating excuse in cases of reporting crimes. Article 29 provides:

"The court may reduce the penalties stipulated in this Law by half if the offender provides information about any of the crimes stipulated in this Law before it is referred to the public prosecutor, and such information leads to the disclosure of the crime, its perpetrators, or their arrest."

This provision reflects a pragmatic policy: encouraging offenders to cooperate with authorities in exchange for leniency. It demonstrates that, despite the overall punitive orientation of the Law, the legislator recognizes the value of incentivizing reporting and facilitating the detection of cybercrimes, which are often difficult to uncover.

To maintain an objective analytical stance, it must be acknowledged that the Jordanian legislator's tendency toward severe penalization in Law No. 17 of 2023 was driven by compelling sociopolitical and economic necessities. In an increasingly digitalized state, critical infrastructures, financial electronic wallets, and state institutions have become highly vulnerable to sophisticated cyber threats and systematic misinformation campaigns that threaten public order. From a strict crime-control perspective, the legislator intended to establish a high level of general deterrence. However, from a constitutional and civil liberties perspective, the academic concern remains that such a sweeping preventive model overreaches, potentially chilling legitimate digital expression and undermining the proportionality framework that underpins the state's broader criminal justice system."

3. Methodology

This study adopts a doctrinal legal methodology that integrates descriptive, analytical, jurisprudential, and critical dimensions. The purpose of this framework is not merely to present the statutory provisions regulating and governing cybercrime in Jordan, but to interrogate their coherence, rationale, and broader implications for criminal policy and constitutional guarantees.

The descriptive dimension involves setting out the relevant provisions of the Jordanian Penal Code and the Cybercrime Law No. 17 of 2023 in their precise legal form. This step identifies the structure, scope, and intended application of the provisions, thereby establishing the factual and legislative foundation upon which further analysis was built.

The analytical dimension moves beyond description to examine the internal consistency of these provisions and their relationship to the general principles of criminal law. It considers whether the legislative choices reflect a coherent criminal policy or whether they reveal tensions and contradictions that undermine the stability of the legal framework.

The jurisprudential dimension situates the discussion within the broader theoretical framework of criminal law. Principles such as legality, proportionality, and the differentiation of liability between principal offenders and accomplices are treated not as abstract ideals, but as concrete guarantees that protect and safeguard fairness, predictability, and justice in the criminal process. This dimension ensures that the analysis remains anchored in the doctrinal foundations of criminal law.

The critical dimension is equally central. It evaluates the legislative choices embodied in the 2023 Cybercrime Law, highlighting areas where the law departs from the general principles and rules of the Penal Code and questioning whether such departures are justified in case of committing cybercrime. This critical stance allows the study to expose ambiguities, inconsistencies, and potential risks to rights and freedoms of individuals, while also proposing constructive reforms that could enhance the law's legitimacy and effectiveness.

Taking together, these dimensions combine textual analysis with normative evaluation. Textual analysis ensures that the statutory provisions are examined in their exact form, while normative evaluation allows for a deeper engagement with their implications for general criminal policy and constitutional guarantees. By employing this dual approach, the study does not simply catalogue the provisions of the Cybercrime Law, but interrogates their underlying rationale, their alignment with established and general principles, and their potential impact on the balance between prevention and legality.

Ultimately, this methodology is designed not only to critique the legislative approach but also to contribute to the broader scholarly and policy debate on how Jordanian criminal law should evolve in the digital age aspects. By grounding the analysis in a descriptive, analytical, jurisprudential, and critical framework, the study seeks to ensure that confronting cybercrime remains consistent with justice, proportionality, and the rule of law.

4. Results

The results of this study reveal several substantive and structural issues in the Jordanian Cybercrime Law of 2023. These results highlight both the strengths and weaknesses of the legislative approach and can be summarized as follows:

1. Vagueness in defining the material element of crimes

The Law employs vague terminology in defining the material element of certain crimes. For example, it equates contempt with defamation and insult in terms of penalty, even though contempt is traditionally considered less harmful because it often occurs in private and lacks the element of publicity. Similarly, Article 16 introduces the offense of "character assassination" but refers only to acts that may result in such harm, without specifying what those acts are. This vagueness undermines the principle of legality and risks inconsistent judicial principles.

2. Criminalization of preparatory acts

Article 11 criminalizes preparatory acts, including the possession of devices, programs, or access codes for the purpose of committing a crime. This represents a significant departure from Article 69 of the Penal Code, which excludes preparatory acts from punishment unless they constitute an independent offense. The inconsistency raises concern about proportionality and legal certainty.

3. Duplication in regulating attempts

Although attempts are generally regulated by the Penal Code, the Cybercrime Law specifically criminalizes attempts in two cases: unlawful access (Article 4) and electronic fraud (Article 10). This duplication creates redundancy and risks confusion about whether the general or special rules should apply.

4. A punitive orientation

The Law reflects a punitive orientation, evident in the severity of fines, the doubling of penalties under aggravating circumstances, and the equal treatment of principal offenders and accomplices. While this may be justified in cases involving serious threats, in less serious cases the severity risks being disproportionate.

5. Departure from general rules of criminal participation

The Law departs from the general rules of participation by equating principal offenders and accomplices under Article 27. It also fragments the concept of participation by listing intervention and incitement separately, while omitting concealment as a form of accessory liability. This fragmented approach undermines fairness and coherence.

5. Discussion

The results outlined above raise important questions about the coherence and legitimacy of the Jordanian Cybercrime Law of 2023. Several themes emerge from the analysis.

First, the use of vague terminology threatens the principle of legality. Provisions such as Article 16 on "character assassination" should be revised to specify the acts that constitute the offense. Without such clarification, the provision risks being used to suppress criticism or free of expression.

Second, the criminalization of preparatory acts departs from general principles of criminal law. Preparatory conduct should not be punished unless it clearly demonstrates intent to commit a crime and poses a tangible risk. Otherwise, the law risks criminalizing legitimate activities, such as cybersecurity research or educational purposes use of digital tools.

Third, the duplication of attempt provisions is unnecessary and conceptually problematic. The general rules of the Penal Code are sufficient to regulate attempts, and the inclusion of special provisions in the Cybercrime Law creates redundancy and confusions.

Fourth, the punitive orientation of the Law, while understandable considering the seriousness of cybercrime, risks undermining proportionality. Excessive severity, particularly in cases of minor online offenses, may erode public trust and make the impression that the law is a tool of repression rather than protection.

Finally, the departure from general rules of participation undermines the principle of differentiated liability. Equating accomplices with principal offenders disregards the varying degrees of culpability and danger posed by different participants. Restoring the distinction between principal and accessory liability would enhance fairness and coherence.

Taken together, these issues suggest that the Law requires careful revision and amendments. The discussion therefore points toward several recommendations: clarifying vague terminology, reconsidering the criminalization of preparatory acts, leaving attempts to the Penal Code, adopting a proportionate approach to penalties, and restoring the general rules of participation. In addition, judicial training and interpretive guidance would help ensure consistent application of the Law.

6. Conclusion

The analysis demonstrates that the Jordanian legislator's approach in the Cybercrime Law of 2023 reflects an expansion of criminalization and the imposition of harsher penalties, often at the expense of established principles of criminal policy. While some measures may be justified by the seriousness of cybercrime, excessive severity and legislative inconsistency risk undermining legality, proportionality, and fundamental rights.

Accordingly, the study emphasizes the need to revise certain provisions to ensure greater clarity, coherence, and fairness. Aligning the Cybercrime Law with the general principles of criminal justice will not only enhance its legitimacy but also strengthen its effectiveness in addressing emerging forms of crime.

The broader lesson is that criminal policy in digital development must strike a delicate balance: it must respond decisively to new threats while remaining faithful to the foundational provisions and principles of legality, proportionality, and fairness. Only by maintaining this balance can the law achieve its dual objectives, protecting society from harm while preserving the rights and freedoms that form the cornerstone of justice.

Data Availability Statement

No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Declaration of the Use of AI

The author used Microsoft Copilot to assist in language editing, improving clarity, and refining academic style. The author reviewed and approved all generated content and takes full responsibility for the final manuscript.

Funding Statement

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Declaration of Competing Interest

The author declares no conflict of interest.

Acknowledgements

The author would like to thank colleagues at the Faculty of Law, Jadara University, for their valuable feedback during the preparation of this manuscript. Additionally, the author thanks the editor and the anonymous reviewers for their constructive feedback in the development of this manuscript.

References:

- Abdulkadir, A., & Abdulkadir, A. (2020). Cybercrimes Act in Nigeria: Experimenting compliance with internationally recognized human rights provisions. *Journal of International Studies*, *15*, 115–130. https://doi.org/10.32890/jis2019.15.8
- Al-Ajmi, A. D. (2014). *Practical and legal problems of cybercrimes* [Unpublished master's thesis]. Middle East University. (In Arabic).
- Al-Majali, N. (2025). *Commentary on the Penal Code – General Part* (9th ed.). Dar Al-Thaqafa. (In Arabic).
- Al-Masoudi, I. (2017). Aggravating circumstances in crime. *Al-Manara Journal for Legal and Administrative Studies*, *21*(21), 248–266. (In Arabic).
- Alshible, M. S. (2018). The foundation of the theory of aggravating circumstances in cybercrimes according to the approach of the Jordanian legislator. *Jordan Journal of Applied Sciences – Humanities Series*, *20*(2), 101–130. (In Arabic).
- Alshible, M. S. (2019). The foundation of the theory of criminal participation in cybercrimes according to the approach of the Jordanian legislator. *Jordan Journal of Applied Sciences*, *21*(1), 55–78. (In Arabic).
- Alshible, M. S. (2023). *Information Technology Crimes: The General Theory of Cybercrimes*. Dar Al-Thaqafa. (In Arabic).
- Bezugly, S., Lesnikov, G., Alkhanov, N., Mironuk, I., & Prokhorova, M. (2020). Preparation for crime: Signs, criminalization. *Journal of Advanced Research in Law and Economics*, *12*(2), 1325–1330.

- Couzigou, I. (2019). The criminalization of online terrorism preparatory acts under international law. *Studies in Conflict & Terrorism*, *45*(7), 535–554. https://doi.org/10.1080/1057610X.2019.1678882
- Jordanian Penal Code No. 16 of 1960. *Official Gazette*, No. 1487, p. 314. (In Arabic).
- Macdonald, S. (2014). The criminalisation of terrorists' online preparatory acts. In L. Qc & S. Macdonald (Eds.), Counter-Terrorism and Beyond: The Culture of Law and Justice after 9/11 (pp. 155–173). Springer. https://doi.org/10.1007/978-1-4939-0962-9_9
- Madeen, M. (2020). *The Art of Investigation and Evidence in Cybercrimes*. Dar Al-Nahda Al-Arabiya. (In Arabic).
- Ohana, D. (2006). Responding to acts preparatory to the commission of a crime: Criminalization or prevention? *Criminal Justice Ethics*, *25*(1), 23–39. https://doi.org/10.1080/0731129X.2006.9992200
- Qaseem, F., & Shadeed, F. (2021). *Interpretation of Criminal Texts*. An-Najah National University. (In Arabic).
- Qashqoush, H. (2012). *Criminal Policy in Combating Information Crime*. Dar Al-Nahda Al-Arabiya. (In Arabic).
- Ramandhanizcha, H., Yuniarti, S., & B., A. (2023). Assistance of cybercrime: Practice in Indonesia. 2023 IEEE 9th International Conference on Computing, Engineering and Design (ICCED), 1–4. https://doi.org/10.1109/ICCED60214.2023.10425130
- Shinkaw, A. (2022). Limits and boundaries of judicial interpretation of criminal legal texts. *Al-Bahith Journal*, (49), 233–250. (In Arabic).
- Sorour, A. F. (1972). Principles of Criminal Policy. Dar Al-Nahda Al-Arabiya. (In Arabic)