Indonesian Journal of Law and Justice Volume: 3, Number 2, 2025, *Page*: 1-13

Cybercrimes Between Criminalization and Punishment

Turath Mohammed Abdul Aziz*, Ammar Ali Mohammed

Northern Technical University

DOI:
https://doi.org/10.47134/ijlj.v3i2.5362
*Correspondence: Turath Mohammed Abdul Aziz
Email: turathalanaz@ntu.edu.iq

Received: 26-10-2025
Accepted: 26-11-2025
Published: 26-12-2025

Abstract: This research covers the Iraqi experience regarding cybercrimes, which reveal an obvious discrepancy between the present criminal laws and the widespread nature of the breaches that are common nowadays. This research particularly covers the ongoing use of the Code of Criminal Procedure and the 1980 Wireless Communications Law, despite the reality that the laws were mainly drafted for physical crimes. As such, the legislation doesn't address the wide range of other crimes that are committed using the internet, such as hacking into computer systems, the manipulation of electronic data, and international fraud. In addition, the research focuses on the problems faced by the prosecution regarding the search for electronic documentation, which, as discussed, remains uncharted despite plenty of gaps. In short, the whole criminal justice system only delivers ineffectual penalties despite the gravity of the crime. This research forms the starting point for exploring the gaps that are apparent within the existing Iraqi legal framework. It assesses the applicability of the laws and regulations and attempts to pinpoint where the laws are failing and why there are discrepancies in enforcing them. The authors believe that the criminalization process needs to shift from the imbalance of the laws to the definition of digital behaviors and an accompanying shift in the definition of the evidentiary rules. The conclusion reached highlights that Iraqi legislation and regulations lack the efficacy required *to deal with the comprehensiveness of the threats that come through cyberspace.*

Keywords: Cybercrime, Computers, The Internet, Communication Technologies, The Digital Age.

Introduction

Introductory Overview of the Subject and Its Importance

The presence of digital technologies, therefore, has created new sets of contradictory realities for the Iraqi situation, as it reflects what is occurring globally. On one hand, the technologies have changed the face of everyday life, but, on the other hand, there are new possibilities for criminal conduct that are difficult to accommodate by the classical legal approach. In recognizing the latter point, (Wall, 2007) illustrates the vulnerability that exists for the digital types as it appears through divergent behaviors. These range from accessing systems and databases without authorised permission to scamming people and stealing their identity online. (Wall, 2007) also adds to this list attacks on privacy as well as reputational harm on social media. He reasons that these misconducts represent a blow to our trust in the digital realm and they run the risk of putting us as individuals and institutions alike under vulnerable situations that the current penal laws unprepared to deal with. What adds to the seriousness of the challenge is not a matter of describing the nature

of offenses only but we have to face the fact that evidence for them is often concealed within complex networks. Courts, however, are still unable to build convictions that address these threats of digital nature and they, in most cases, get rejected for lack of procedural clarity.

In view of the state of affairs above, we see that any approach envisaged must put as its core the protection of fundamental rights especially because the tensions that arise between detering such crimes and civil liberties are in need of a framework in which privacy and freedom of expression are preserved rather than ignored. Although the idea seems valid, striking the right balance often becomes hard. In fact, the phenomenon of cybercrime cannot be explained merely on the technological plain, as it gets shaped and bounded by other factors, which define the activity of human beings. At present, it appears clear that the online world represents an ever-changing terrain, on which criminal behaviors, coupled with technological development, increase, and control mechanisms seem less effective.

In the light of the above, it appears that there are threefold steps to resolve the above-stated dilemma, which are discussed after reviewing the literature. In fact, (Casey, 2011: 5-7) discusses the online behavior convincingly and explains the procedural provisions that represent the reality of the existing situation. Also, there ought to be an independent judiciary that possesses the capability to implement such provisions. As we will explain throughout the course of the current study, if such reforms are not put in practice, the criminal-justice system of Iraq, which is the subject of this study, will remain reactive and fragmented and thereby continuing to take action but only after harm has taken place, a matter that runs counter to what is expected in a modern society.

Methodology

Research Problem

Our daily life in Iraq, and very much elsewhere, becomes increasingly dependent on digital technologies. With this increased reliance on such innovations, there does come to the fore some serious doubts about whether the existing criminal law is on a strong footing to deal with cybercrime (Al-Momani, 2008) (Arab, 2001) (Wall, 2007). In view of the foregoing, this study wants to assess the extent to which current Iraqi provisions address offences committed in electronic environments and identifies what does it take to set competent laws for this new reality in stone.

Research Objectives

In light of the above-mentioned background, the research tackles three major objectives. First, it seeks to examine the degree to which the present Iraqi criminal code codifies and punishes the related activity of cybercrimes, as well as the degree to which the common-law provisions are unable to account for the peculiar nature of such crimes. Second, it seeks to examine the available means for the collection and authentication of electronic evidence, while focusing on the degree to which the procedural laws are adequate for the admissibility of such evidence during trials. Finally, the research seeks to assess the capability of the judicial authorities to deal with crimes committed through the use of information and communication technology, as it looks into the practical problems that are faced during the trials.

Research Structure

The research design follows a sequence from diagnosis to prescription. The first part explores the ways for which the Iraqi Penal Code has adapted to deal with crimes committed by the use of computer and network processes, which highlights the doctrinal deficit implicit in the applicability of regulations initially written for physical crimes and later applied to virtual crimes. This section of the research sets out how far the Wireless Communications Law of 1980 contributes to the regulation of the field and how far the gaps that exist are left unrepaired and outdated.

The following section tackles the response of the institutions, discussing the approaches inside the criminal justice system concerning the management of cybercrimes. This section focuses on the evidential process and the capabilities of the prosecutor and the courts, specifically discussing the needs for specialization. This section brings the Iraqi efforts into the debate concerning the criminal policy on the national level, discussing the needs for a common policy and intervention.

The Concept of Cybercrimes

Definition of Cybercrimes

1) Cybercrimes

Hosni (1989) provides an effective definition of crime as conduct that is criminal, outlawed by criminal law, and committed with the intention of breaking the law and punished as such. In the same light (Mustafa, 1983), perceives crime as an act and omission that, according to the applicable laws, gives rise to criminal responsibility. Basically, crime goes beyond the simple breach of the rule as it manifests as an intelligent challenge against the community will, contrary to the standards that define the prohibited behaviors and their corresponding sanctions. This makes crime differentiate from less serious legal errors and signal the most adverse infringement (Behnam, 1996). further explains that crime brings an extra risk as it jeopardizes the basic obligations towards the individual and the community, which makes the penalty necessary for maintaining the community order. Cybercrime can also refer to an attack targeting data stored on computers or information shared through information systems and networks, especially the internet. It is basically a technical crime carried out out of sight by criminals with exceptional capabilities and advanced technical knowledge, and the main goal of them is to violate the right to access information, as per (Arab, 2001). In order to understand cybercrimes and clarify their nature, we may need to be familiar with the general idea of the tools used to commit these crimes. Not only does it entail that but it also involves what they target, and the legal interests that deserve criminal protection. Based on that, we first define electronic tools, then we move on to explain the target of the attack in the second step. Finally, we highlight the interests that require criminal protection in the third step.

2) Introducing Electronic Tools

Electronic tools are inseparable from modern technologies and include computer applications, communication technologies, and information technology (Hijazi, 2009: 1). Many systems and devices are connected in one way or another to the electronic computer,

where the computer is considered a fundamental information system and the hub of electronic dealings, regardless of the form in which it appears. In addition, there is the broader digital infrastructure that combines digital communication worlds, known as the Internet. Therefore, we may need here to clarify the concept of the computer as the primary means in cybercrimes, alongside defining the Internet. The computer is known among specialists as an electronic device consisting of a set of interconnected components controlled through special programming commands, designed to process and manage information in a certain way by performing three basic functions. First, it receives input data as primary facts. Second, it processes this data to convert it into information by performing calculations, comparisons, and processing inputs) (and finally, it displays the resulting information in the form of clear and useful results (Al-Zoubi, 2002). It has been defined by some based on its operating system as an integrated set of devices that work in harmony to achieve processing of input data, according to a pre-prepared program, with the aim of producing predetermined results (Qashqoush, 1992), or it is a computerized electronic device designed to receive data and process it using specific programs, with the aim of performing operational processes on this data and achieving the required results (Murad, 1998). Simply put, it can be described as a device that processes data automatically according to predetermined settings, allowing the results of this processing to be obtained when needed.

Therefore, the computer is considered an integrated system that operates within a three-dimensional equation framework, consisting of three basic elements that contribute to forming its functional structure. The first element consists of a set of tangible physical devices that form the physical structure of the computer, known by the term "Hardware" or equipment. In the second, we find it consists of the information and instructions referred to as “software,” or programs. These programs provide the operational logic that guides the hardware and ensure that each component performs its designated functions in accordance with predetermined commands. The third element, which gives real value to the equipment and software, is represented by the human element, that is, the individuals who interact with the software and use it to achieve their various goals (Al-Momani, 2008).

We may simply describe the Internet as a comprehensive electronic network extending on a global scale, composed of millions of local networks and computers connected to each other through both, wired and wireless means of communication. The Internet is distinguished by its ability to provide a wide array of diverse information services to users continuously and around the clock, which enhances its role as a fundamental pillar for communication and information exchange in the modern era (Abu Farah, 2012). Based on this, this network is considered an ideal environment for committing cybercrimes and information violations.

3) The Subject Matter of Cybercrime

It is undeniable fact that computer is now a fundamental pillar in the field of electronic and information transactions, and is the central axis around which cybercrimes revolve. The threats to such infrastructure are not only limited to the data but extend to the material aspect as well. This, therefore, underscores the multiple effects that can arise from any damage, theft, and illegal use of the material aspect, which pose direct threats to the

integrity of information systems. This, therefore, means that such threats can be directed at either the material and information aspects of information and communications technologies. In fact, it would be wise to recognize the existence of additional threats that lie within the information arena, which would come to pass through various advanced means and approaches, as claimed by (Al-Ghuthbir & Al-Qahtani, 2009). Unlawful or unauthorized activities in the technology field may take the form of a kaleidescope of practices, such as modifying programs or introducing malicious programs like viruses, or unauthorized access to information, networks, and databases, whether intentionally or by mistake. These activities also include entering data for the purpose of falsification or forgery, whether in good faith or bad faith. Moreover, these practices can include deleting or hiding information, refraining from entering it, or manipulating it, including encryption keys and secret passwords.

What we can say from the above is that the fundamental focus of this crime and its subject matter is represented in computer data and information, which are targeted by perpetrators' assaults in general. The nature of these crimes lies in their occurrence either against the computer itself or using it as a means, where the computer is sometimes the subject of the crime, and at other times a tool for carrying out the assault on another subject represented in electronic data and information.

4) Regarding Criminalization

Behnam (1996) underscores an important point that criminalization remains the essence of criminal law, which offers the means whereby society marks conduct detrimental to the basic interests of society and submits it to sanctions. While regulatory provisions merely state that some conduct is prohibited, criminal law specifically labels such conduct as crimes, thus expressing the legitimacy and, by implication, the binding nature of the legal order and people's collective observance of the same. This makes criminalization both a means and an instrument of ensuring that people are loyal to the community's common standards of conduct.

The Interests Subject to Criminal Protection

Referring to the safeguarding of interests in the electronic field, the process begins with the safeguarding of computer and electronic systems and the information that they store and transmit. Safeguarding the above-mentioned interests involves various elements, which are discussed by (Al-Ghuthbir & Al-Qahtani, 2009) as follows:

- Protection of information confidentiality. This requires that information that requires confidentiality be protected against illegal access and misuse. Preventive measures that can be taken to ensure that the information remains confidential include strict information-security policies, encrypting the information, and information-monitoring processes.
- Integrity of information: Information needs to be credible and unaltered, along with the facility for prevention of illegal modification and replication.
- Information and resource availability: it needs to be ensured that authorized users are provided constant and reliable access to the system and information. Safeguarding the right of access needs measures that ensure that the services are not interrupted, nor the information unavailable, when the need arises.

The safety of computer devices and electronic equipment and their contents of programs and information has come to the fore ad an urgent necessity, this is especially true of the computer and Internet's connection to data storage and exchange. Therefore, specialists have gone the extra mile to develop techniques and programs to ensure the security of this information technically. This is nowhere more true than in the fact that computers and networks are considered a virtual space containing personal data equivalent to the financial liability of individuals, what can be called the "information or technological liability." To ensure its continuity, it must be scaffolded with legal protection that reaches its peak by providing criminal protection. Accordingly, we can extract the interests deserving of criminal protection in the following points:

- Keeping the right of secret and keeping privacy of personal life is very important, because it helps the person to stay safe from other people who try to enter his/her private life or share his/her personal details without asking him/her first. This is also why many countries make rules and laws that try to keep personal data safe and use it with care and responsibility. Also, people ought to learn more about why it is important to respect the private life of other people, in normal daily life and also in the digital world tge fast growth of which we clearly see. There is also the need to keep safe the information and the ideas that belong to people, and this is done by making special rules that say these rights are real and must be protected.
- There must be effort to keep safe the rights of material things like machines, tools, and other physical aspects that can be attacked by electronic ways.
- Keeping safe the electronic public order is also of a high importance, because it is part of the bigger public order of the country in administration and economy. This is actually more important now because many countries follow new ways called electronic government. This shows the fast change to electronic administration, and it helps to give many services and transactions in one complete electronic system. This system uses digital technology to serve a number of functions e.g. i) to make things easier, ii) to use less paper, and iii) to make the work of administration and economy more strong. It also helps to make things more clear and fast when giving services to citizens and companies.

3. The Reality of Criminalization in Iraqi Criminal Law

The electronic crimes in Iraqi law is one subject that needs more care, simply because we are witnessing the digital world growing very fast. When technology develops and when the Internet is used in many parts of daily life, new problems naturally appear for the courts and the law in Iraq, because they have an obligation to deal with crimes that come from wrong use of technology. We should acknowledge that Iraqi criminal law has moved step by step to face this situation, and we can indeed find some rules and legal texts were made to try to stop cybercrimes and also to fix the weak points in this area. These crimes include, but are not limited to, hacking computers, stealing data, making false digital papers, and cheating people online. Also new crimes came to the surface, one has to note here, such as breaking privacy and saying bad things about people on social media. However, even with these efforts, there are still many problems for Iraqi criminal law, and the biggest one is that the rules must change to fit the fast and changing ways of cybercrime. It is also important

to make the courts and police stronger in technology, so they can fight these crimes and look into them in an efficient way. So we can say that solving the problem of electronic crimes in Iraqi law needs not only new rules, but also more awareness and more working together between all sides, so the answer we are seeking will be complete and strong for addressing this new problem.

Adapting Penal Code Provisions:

The reality of cybercrimes in the modern era has become a reality forcefully imposed on both the legislative and judicial arenas in most countries of the world, making it a major concern for all those concerned with public affairs in Iraq. Despite the absence of special legislation regulating cybercrimes, this subject has imposed itself as a result of pressures from reality and has become the focus of attention for all sectors concerned with legislative, administrative, and economic frameworks. However, this attention is still in the stage of attempts seeking to formulate modern legal frameworks capable of effectively confronting these crimes. Regarding the criminal procedures currently applied in Iraq, dealing with cybercrimes is done through exploiting the provisions of traditional penal law, where these provisions are adapted to apply to illegal acts with the aim of serving the justice sector and punishing perpetrators of these crimes. However, this approach often proves inadequate. In many cases, either the legal characterization of the behavior is not sufficiently accurate, allowing the criminal to escape punishment, or the prescribed penalty is not proportionate to the size of the act and the resulting harm. For example, some crimes committed via computer or Internet are dealt with through projecting traditional penal code provisions, but this approach highlights the limitations of current provisions in confronting renewed and complex cybercrimes (Hijazi, 2009).

Legislative provisions specific to crimes such as extortion and fraud, theft and damage, seal counterfeiting and forgery, forgery, breach of trust, insult and defamation, libel, disclosure of secrets, and incitement to debauchery are traditional legal frameworks applied when these crimes are committed using computers or via the Internet. However, the present available provisions are lacking effective deterrence and punishment capability against cybercrime. The provisions are active and applicable mainly if the computer serves as an instrument of crime and the direct target of an attack, thus leaving many kinds of electronic crimes outside the boundaries of criminal liability. (Al-Momani, 2008: 112) argues that the lack of clear and broad provisions makes it easy for the criminal to find loopholes to escape from the provisions. As such, the legislation that focuses on the criminalization of the electronic aspects, which are representative of their characteristics, becomes particularly important, as implied by Al-Momani.

The Position of Iraqi Wireless Communications Law No. 159 of 1980

Law Number 159 of 1980 deals with the use of wireless communications in the Iraqi state, determining the regulatory framework for the safe and organized use of communications. This legislation, which lays down the regulations and their accompanying penalties, as well as determining the technical specifications for avoiding interruptions, reflects the contemporary perspective on communications, where it attempts to limit the illegal use of communication for malicious objectives. Nevertheless, as (Al-Momani, 2008) explained, Law 159 covers the situation critically, as it attempts to control the use of wireless

communications but fails to offer complete safeguarding against the wide range of activities representing e-crimes. In other words, the principal aspects of electronic activity lie beyond the legislation.

Dimensions of Iraqi Criminal Law's Dealing with Cybercrimes

1. The Philosophy of Criminal Law in Combating Cybercrimes

An improvement in the criminal policy of Iraq against cybercrime requires, therefore, both creativity and adjustment. According to (Qashqoush, 1992), new laws ought to be created that address crimes such as hacking, fraud, and privacy infringement, and existing laws ought to be adapted to the pace created by technological advance. This requires the preparation of trained personnel for dealing and reacting to such kind of crime. Awareness on the other hand, as the fourth ingredient, requires that users and people understand the risk involved, and the state ought to cooperate and partner internationally to address crimes that are global. Although there are new growths, the reality, the laws are actually not equipped for the kind of complexity involved. There ought, therefore, to be proper legal formulations to address the nature and penalty for such crimes. Here, according to (Qashqoush, 1992) the efforts of the prosecutor would be for naught without proper legal definition and penalty, while (Arab, 2001) argues that the development of legal and prosecutorial capability for dealing with the forensics of the matter ought to play an important position.

Finally, we should remember balance in this equation. On one side, laws must protect privacy and rights of people and on the other side, they must be strong enough to punish cyber criminals. This balance while it is difficult to implement, but it remains necessary. And let us add that community awareness about cybersecurity is equally important. In this way, Iraqi criminal law can play a main role in facing modern electronic problems and protecting society and institutions from the dangers of these crimes.

A word on tbe nature of legislative policy is in order here. (Surur, 1972) explained it for us stating that it can be understood as the group of main ideas and goals that guide how laws are written and used in different stages. Criminal policy, on the other hand, is the structure that shows the rules and principles used to build criminal law, whether it is about defining acts that are crimes, about how prosecution is done, or about steps for prevention and treatment, Surur asserts.

To reach the aims of criminal policy for any specific issue, the first step that needs to be taken is to make a careful and complete study of that issue. The purpose here is to collect and organize all information connected to it. From the current study, the legal system for protecting the issue is made clear, because it shows the important interests that must be included in the law. After that, weak points in the current legal texts can be seen, and this opens the way to expand criminal protection to cover those interests that are most important and need protection. All of this is done while keeping an eye on prevention and deterrence, so the treatment of the issue is complete and systematic.

When we try to explain more about this policy, we can say that the tools used to achieve criminal policy are found in criminal law in its wide meaning. (Surur, 1972) explains further here that law has basic rules about criminalization, where acts that attack protected interests are explained. At the same time, it also has criminal procedures, which are the main

way to apply those rules, whether it is about collecting evidence or about prosecution in court (Surur, 1972). From this, the importance of making this new phenomenon a crime becomes clear, so the adverse effects that come with it can be reduced and damages can be limited to a minimum. A suitable way to go about this is planning and deciding the needed procedures to fight this kind of new crime, which essentially needs strong cooperation from many sides and institutions. In the next section, we deal with position of legislation pertaining to data Protection and individual digital rights.

2. The Position of Legislation Related to Data Protection and Individual Digital Rights

For the effective control and regulation of the online world, there thus needs to be an effective framework for the collection, storage, processing, and transfer of information, as marked by the European Commission (2016). This framework needs to be simple and broad as far as the processes involved are concerned, and it would provide benefit to both institutions and individuals. This would become possible if, besides the standard processes, there were predefined digital rights for the users of computers, information systems, and the Internet. As marked by (Cloudian, 2023), such digital rights would provide the user the option of having safe and reliable information, correcting information if and when the need arises, and having their online space protected from unauthorized access.

For such balance to be achieved, legal safeguarding needs to go beyond criminalization and embrace administrative, regulatory, and civil laws, as advocated by the (World Bank, 2017). For such a framework to be comprehensive, it would ensure that individual rights are matched by the responsibilities of institutions, leading to an arrangement where privacy, accuracy, and security are ensured despite the advancement of technological progress, as postulated by the information on the General Data Protection Regulation (De Terwangne, 2020). In doing this, the regulation of data and privacy laws serves as not only an umbrella for individual rights but as an intervention tool for engagement with the modern information space, as restated by (Ayoub, 2009).

Ayoub argues that the privacy laws of an advanced country are designed to ensure that there are legal conditions that ensure the right to information access, the liberty of information flow, and the safeguarding of privacy (Ayoub, 2009). These laws also try to stop the risks that come from collecting, storing, or processing personal data by institutions or information centers. Some of them even add limits on sending data outside the borders of the state, and they also give people rights to own and manage their data freely (Ayoub, 2009).

In this same line, we can point to the Council of Ministers decision about preparing a draft law for data and privacy protection, which may be considered an important step toward making rights for personal data and the right to access information clearer.

Second, we must also refer to the need for criminal rules that explain acts which attack digital rights and make them crimes, with penalties that can stop people in general and also punish specific offenders. There can also be special penalties for cybercrime perpetrators, connected to their unlawful acts, and these can include steps that put a limit on their use of modern technologies.

If we want to delineate the forms of digital assaults, we can see that they are numerous, and the goals and methods of them are different. Some examples that can be

mentioned here are unlawful access, damaging information, blocking computer data, and stealing or taking data. There are attacks against computers as physical machines, and others against them as information systems. Crimes can also be done through computers, the Internet, and information systems, and this makes many types of crimes, like theft, fraud, money laundering, insult, defamation, libel, forgery, and more. As (Yunis, 2005) noted, dividing cybercrimes into crimes of objective, means, or content is the way followed by many European laws, and this is shown clearly in the European Convention on Computer and Internet Crimes of 2001. Since the early 2000s, efforts started to build a full framework to classify these crimes, by making a reference list for international cooperation in fighting cybercrimes. Even if this effort was led by European countries, it also had strong participation from the United States, Australia, and Canada. The European Convention gave four main groups of computer and Internet crimes, and these became the base for facing these challenges.

Cybercrimes are usually divided into several main groups, and this division tries to show their nature and to make them fit with modern technical changes.

The first group includes crimes that attack the secrecy, accuracy, and trust of computer data and systems. Here we can mention acts, for instance, entering systems or data without permission, watching or intercepting data unlawfully, disturbing or blocking data so it loses stability, damaging systems through interference, and using tools or devices in wrong ways that harm the system.

The second group is about crimes that come from using computers, such as making false digital documents or cheating people with electronic methods.

In the third group, we can see that it focuses on the content of data. This includes crimes linked to immoral or pornographic material, and also crimes that exploit children for prostitution.

The fourth group deals with intellectual rights. This covers things such as breaking copyright rules, violating neighboring rights, and software piracy. It is interesting to note that the draft Iraqi Penal Code follows this division, but it does not make privacy crimes and personal data protection a separate group. This may be because the European Convention treated privacy in another special agreement that was made to protect personal data from risks of automatic processing. The Iraqi Cyber Crime Bill was produced during the same period as the signing of the European Convention, thus giving lawmakers the chance to develop an up-to-date approach that complies with global standards. However, according to (Yunis, 2005), the project was unfinished and unratified due to many lingering uncertainties regarding the process applied to dealing with cybercrimes.

The concern that can be considered substantive involves crimes against the computation device. Where an offense focuses on the machine as it is, the general legal standard would possibly apply. More harsh penalties are recommended for the items because they not only contain physical value but also inherent value to the owner based on the information contained.

The issuance of such laws regarding Iraq is still considered an extremely sensitive process, especially as such laws are linked to freedom of expression and cyber liberty, as well as the responsibility to protect society. The laws are actually the focus of continuous

debate for various interest groups, as attempts are made to ensure that the laws are aligned with the Iraqi social and political environment. In the end, the effectiveness of such laws would depend on the development of the technical infrastructure and the promotion of cyber-security awareness, as well as the use of professionals who would deal with the aspect of cybercrime.

Result and Discussion

In order to understand the nature of cybercrime, it is necessary to define it as much more than just an informational glitch. The defining aspect of the crime revolves around the exploitation of information as it travels, resides, or is located either on computers or communication networks. The direct implication that can be derived from the above-stated point revolves around the crucial aspect that the computer becomes central to the issue, as it becomes the conduit for electronic transactions and the attacked entity.

The obvious conclusion that follows is that the criminal-law system must recognize information as the central entity that needs to be protected. Offences can be directed against the machine itself, and some offences can use the machine as the means to attack information, and as such, the integrity of the machine needs to be protected. For that reason, the interests that qualify for safeguarding are no longer confined to the issues of privacy and confidentiality but must include intellectual property, material property, and the integrity of the electronic order.

On the basis of the above, the need for capacity within institutions emerges. In the absence of such institutions and clear processes, tracing crimes, collecting evidence, and delivering justice are impossible. This can similarly be applied to data governance. While data governance regulations must define the processing and transmission of data, it must, by the same token, protect the individual's right to accuracy, security, and correction of their data.

At last, deterrence requires the use of criminal norms that are necessarily specific in the definition of assault against information rights and provide corresponding sanctions. This, and this alone, would ensure that both the general and the specific deterrence are accomplished.

Conclusion

This study concludes that for criminal legislation to preserve the legitimacy it has achieved, it must and can be assessed based on predictive capabilities and not reactiveness alone. Since the model based exclusively on analogy classifications does not seem resilient enough to withstand the challenges of online delinquent behaviours, the basic characteristics of which lie in the exploitation of the gaps between ancient legal matrices, the following implication emerges.

This same explanation can be applied to the evidentiary process. Where the courts are fixed on analogizing electronic evidence to that which would exist if it were on paper, the consequence of such an approach would not be procedural circumspection but the

fragile nature of the system. An assertion that the legal system cannot deal with the nature of electronic forensic processes would undermine the authority of that legal system, as it would abandon the tools of enforcement.

Finally, the legitimacy of criminal policy depends on equilibrium. An overly rigid criminal policy would jeopardize innovation, and an overly soft one would encourage abuse. As such, there is an exclusive deductive conclusion that there must be an informed and harmonious technological framework to support the integrity and privacy that would facilitate legal data transfer. Criminal policy would not be able to honor the foremost responsibility of ensuring order, especially as the increasing use of information systems typifies society.

5.2 Recommendations

In case the outcome reveals the vulnerability of the system, the recommendations must necessarily point to the basic component of the process. This preliminary finding would naturally suggest that privacy and respective laws are necessary to protect privacy and that such an overriding legislation would oblige institutions to follow the values of transparency and accountability, even as the rights of institutions and people are protected.

The second recommendation pertains to procedural standards. An effective criminal justice system that fails to provide clear procedural standards for the realms of electronic investigations, searches, and seizures cannot rightfully presume the power to rule. Therefore, it becomes necessary that an electronic procedural legislation be enacted that would qualify electronic evidence and establish whether such testimony would be admissible.

The third deduction involves an international perspective. Cybercrimes are undoubtedly global. They cannot be addressed by the laws and regulations of individual nations. Hence, involvement in international bodies that focus on dealing with cybercrimes is essential. This provides an opportunity for monitoring and an exchange of expert knowledge, which complements the efforts of individual nations and provides an opportunity for collaboration.

This last recommendation deals with interjurisdictional collaboration. In combating cybercrime, there must be communication networks, collaborative training efforts, and mutual help for detection and enforcement. This collaboration provides an effective and collective means to thwart the ever-growing threat of cybercrime.

References

Abu Farah, Y. (2012). *Electronic business*. Al-Quds Open University.

Al-Ghuthbir, K., & Al-Qahtani, M. (2009). *Information security in simple language* (1st ed.). King Saud University. https://books.google.com.om/books?id=O2evkRtV24IC&printsec=frontcover&hl=ar#v=onepage&q&f=false

Al-Momani, N. A. Q. (2008). *Information crimes* (1st ed.). Dar Al-Thaqafa. https://www.noor-

book.com/2010-pdf

Al-Zoubi, M. (2002). *Computer and ready-made software*. Dar Wael Publishing.

Alashti, Z.F. (2021). Investigating the Youths1 Cybercrimes through the Lens of Cops: A Case Study of Iranian Television Documentary "Birahe". *International Journal of Cyber Criminology*, *15*(1), 108-121, ISSN 0974-2891, https://doi.org/10.5281/zenodo.4766536

Arab, Y. (2001). *Computer and Internet crimes*. Ittihad Al-Masarif.

Ayoub, P. (2009). *Legal protection of personal life in the field of informatics* (1st ed.). Halabi Legal Publications.

Behnam, R. (1996). *Theory of criminalization in criminal law: The criterion of punishment authority in legislation and application.* Munsha'at Al-Ma'arif.

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet*. Academic press.

Cloudian. (2023). *Core Principles of the GDPR.(nd). Retrieved October 24, 2023*. https://cloudian.com/guides/data-protection/data-protection-principles-7-core-principles-of-the-gdpr/

De Terwangne, C. (2020). Principles relating to processing of personal data. In *The EU general data protection (GDPR): a commentary* (pp. 309–320). Oxford University Press. https://gdpr-info.eu/

Hijazi, A. F. B. (2009). *Emerging crimes* (1st ed.). Munsha'at Al-Ma'arif.

Hosni, M. N. (1989). *Explanation of the Penal Code, General Section* ((6th ed.)). Dar Al-Nahda Al-Arabiya.

Murad, A. F. (1998). *Explanation of computer and Internet crimes* (1st ed.). Legal Library.

Mustafa, M. M. (1983). *Explanation of the Penal Code, General Section* (10th ed.). Dar Nashr Al-Thaqafa.

Qashqoush, H. H. (1992). Computer Crimes in Comparative Legislation. *Dar Al-Nahda Al-Arabiya, Cairo, Egypt*.

Shestak, V.A. (2024). Classification of Cybercrimes in GCC Countries. *Revista De Direito Estado E Telecomunicacoes*, *16*(1), 66-79, ISSN 1984-9729, https://doi.org/10.26512/lstr.v16i1.48885

Surur, A. F. (1972). *Foundations of criminal policy*. Dar Al-Nahda Al-Arabiya.

Wall, D. (2007). *Cybercrime: The Transformation of Crime in the Information Age* (Vol. 1). Polity.

World Bank. (2017). *Data protection and privacy laws. Identification for Development.* https://id4d.worldbank.org/guide/data-protection-and-privacy-laws

Yunis, O. M. (2005). *(Trans.) Explanatory memorandum of the European Convention on virtual crime.*