INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 2 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

ELECTRONIC CRIMES IN JORDANIAN LAW

AUTHOR - SULTAN HAMAD ABDULLAH ALMASHAQBEH, FACULTY OF LAW – STUDENT, ZARQA UNIVERSITY.
CONTACT - DALOUN@ZU.EDU.JO

BEST CITATION - SULTAN HAMAD ABDULLAH ALMASHAQBEH, ELECTRONIC CRIMES IN JORDANIAN LAW, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 4 (2) OF 2024, PG. 916-923, APIS – 3920 – 0001 & ISSN - 2583-2344.

1. Introduction to Electronic Crimes

The twenty-first century has seen the dramatic ascendancy of electronic applications and systems. The massive expansion in the use of these technologies has become so extensive and pervasive as to encompass all aspects of life. One principle cause of that expansion is the Internet. Its use is widespread to the point that it now encompasses the majority of electronic applications. This spread of electronic systems and applications represents both a development for the betterment of human life and a potential source of indescribable dangers. Indeed, such technologies, while offering hope to a vast array of individuals and institutions, also offer an opportunity for expanded criminal activity and a potential source of risk to all aspects of life.

Many attempts have already been made, not only in Jordan, but in a variety of countries—including the Arab world, European Union, and international fora—to attempt to craft electronic crime legislation. The starting point for any endeavor of this nature should encompass the term "electronic crimes." A close examination allows one to surmise that electronic crimes encompass all sorts of conduct that occurs in the greater electronic environment, an environment that encompasses crimes committed against the computer, as well as crimes committed by means of the computer.

Keywords: Crimes, Electronic Crimes , Jordanian Law, Cyberbullying, Harassment

1.1. Definition and Scope of Electronic Crimes

Title Three (Electronic Crimes) includes articles (27/30) that set forth the definitions and scope of electronic crimes. It is worth mentioning that the crime must include all the traditional criminal elements as well as the electronic element, according to the Interpol model law. The Interpol model law defines an "electronic crime" as a crime that can be committed only through the use of an electronic communication network, or which targets such a network, as is required by a number of international instruments.

The definition of electronic crime in Jordan covers a broader scope as it encompasses obscene and offensive messages, where such conduct is committed with an intent to insult or incite violence. In addition, the Jordanian draft law criminalizes the offense of hacking tools, as the means through which the hacking act is committed may be included within the scope of criminal protection (articles 27-30 of the draft law). In addition, the offense of hacking the data system is inclusive, as illicit possession, constitution, or obtaining of data from a computer system, computer data, software, electromagnetic film, and any other legally protected reservoir of computer data. Furthermore, electronic multi-use appears within the meaning of theft crime in article 27/2 and impersonation crime in article 2/31 of the draft law. Understanding the definition and the scope of electronic crimes is crucial for the effective interpretation and enforcement of the anti-electronic crimes provision. In addition, it will assist in comprehending the different types of electronic crimes and their analyzing of implications.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 2 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

2. Legislative Framework in Jordan

Electronic crimes in Jordan are governed within the Jordanian legal framework. Although these crimes were not well addressed before the 21st century and not by specific legislation, they are currently subsumed under the Anti-Cybercrime Law. The discussion of the legislative framework is crucial as it lays the foundation for how the laws governing electronic crimes are situated within the lower structure. This section investigates the legislative framework in Jordan and examines relevant laws and points of references where electronic crimes are governed through a legal framework.

Electronic crimes in Jordan were not legislated until the Anti-Cybercrime Law (25/2010). However, there are several laws and regulations that play the confinement to these crimes and that have criminalized them. Some of the provisions that cover those crimes are the Information Systems Crimes Law (19/2011), where the legislator criminalized illegal access to information systems, the illicit obtaining of credit or value services, phishing, electronic fraud, and illegal acts on information systems data. Moreover, the Electronic Transaction Law (85/2001) and the regulation of the Data, e-Commerce and Postal Law are crucial laws that also play a role in the regulation of electronic crimes. Since the Electronic Transaction Law and E-commerce and Postal Law do not include criminalized provisions, they prohibit some illegal behaviors, and they stipulate protective measures of these crimes.

2.1. Relevant Laws and Regulations

Electronic crimes take different forms and fall under the purview of various laws and codes in accordance with the nature of the criminal act and the mechanisms used in its commission. The provisions regulating electronic crimes vary in nature and scope, and are covered by a range of legal instruments that together address the practical, formal, and substantive aspects of electronic crime, criminal procedure, and criminal responsibility.

The Electronic Transactions Act of 2011 provides a legal framework for internet-based transactions. By creating space for electronic signatures – which are set aside for identifying the signatory and establishing the signatory's approval for the content of the electronic record – the Act is designed to address the paucity of legal safeguards for internet transactions that don't involve physical encounters between buyers and sellers. Additionally, the Act sets forth five scenarios in which electronic signatures are not effective. They include cases involving legal proceedings, the proof required under impracticable or unreasonable circumstances, the consumer protection legislation, the economic crimes legislation, and any other circumstances as may be prescribed. The Act stipulates that "In order to prove the transaction, it is necessary that the content or the supporting record contain the following information: Name of the transaction; the signatures of the sender and the recipient; the time the record was signed; and the electronic transaction is sent. A record is deemed to constitute prior to recording in accordance with official procedures" (Article 12). Jurisdiction, citation, and enforcement are among the other letters of the law that the Act advises on.

3. Types of Electronic Crimes

10) Electronic fraud. Electronic fraud is any act that involves the use or exploitation of information technology, with the intention of defrauding another person, whether this intention is to obtain an amount of money or any goods or services unlawfully, such as manipulating the process of credit card or bank account.

11) Forgery and electronic theft. Forgery is to defraud by using various means because documents have been tampered with. While electronic theft is the same as the usual theft, the difference is the use of ICT in the process. For instance, the hacking of an account username or password system so that illicit access to the account results in transactions that can financially endanger the account

owner. It could also be related to data theft over the internet and finally electronic in the form of plagiarism and piracy.

12) Sending unsolicited emails (Spamming). This crime has affected the rights of others who are technology users by sending unwanted emails that violate privacy, misuse email services, and interfere with normal activities. However, interestingly, laws in the industrial world, such as in the United States, regulate spam, which is sent through email. Currently, four federal laws have been stated specifically regulating spam.

13) Denial of Service Attack (DoS). This crime includes denial of service attacks, which cause damage and restrict access, so that authorized users can send requests and receive replies from systems, computers, and devices connected to the Internet. Data and information stolen, including the installation of programs, system destruction, password theft, and unauthorized access to systems.

14) Electronic defamation. As in the traditional world of communication, technological advances have broadened the scope of defamation opportunities to the electronic world. In the civil field, victims can demand data compensation or the revival of their reputation and drawing damages, while from the criminal side, the perpetrators are threatened with imprisonment. In this case, they can be called as the electronic criminal populace if regulated by positive law.

15) Electronic pornography. The content of electronic pornography is pornographic content in writing, including writing that is violent or offensive to the community, showing imaginary sexual violations, ridiculing human dignity, or inciting immorality. Even though this type does not show an experience of sexual violence in video form or in the real world, it is also a violation of human dignity and destroys religious and social morals.

16) Identity Theft. Initially officially appearing in the United States in 1998, there are abuses of other people's private data in the United States as an organized criminal element. This process has become an electronic crime itself, which has become an issue of concern around the world. "Identity theft" can be defined as a person fraudulently posing as another with the intention of causing harm or harm, usually for economic aspects.

17) International Human Rights Violations. E-crimes of international human rights violations involve some forms, such as cyber-warfare and system-based cyber-terrorists. These attacks pose a very serious threat because they can demolish national and international systems. This part of E-Crime study is based on a global perspective; this is because e-crimes of international human rights violations are a suffixed form of e-crime that uses information technology in all its forms and a worldwide series.

18) Money laundering. The term "money laundering" covers the ways in which profits earned from various criminal activities are reinvested in countries with stronger economies, thereby enhancing the economy of the country in question, which is causing the investment. If it is forbidden in any way, then there will be legal liabilities arising from a law right now. The term "money laundering" itself is derived from a historically related word, the term "money launderer" in Miami, Washington, DC, c. 1984, which refers to illegal activities that generate profits obtained from illegal activities.

3.1. Cyberbullying and Harassment

3.1. Cyberbullying and Harassment

Access to the internet has significantly increased during the last two decades. The internet and digital communications technologies have created new online social spaces such as Facebook, MySpace, Twitter, YouTube, and many other Web 2.0 applications. With the rapid development of Web 2.0, new types of online communication have also appeared, such as blogs, wikis, and other applications using user-generated content. In

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 2 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

this new web-indexed society, if a person is physically harassed by another, then the case is easy to handle and resolve compared to online harassment. There are many ways in which a person can be harassed using the internet or an interactive digital device, such as emails, chat rooms, or even SMS.

Recently, criminal activities have been carried over collaborative and social communications technologies, leaving behind traditional street-level crimes such as burglaries, thefts, and assaults. One of the most prevalent growing patterns of electronic crime is psychological abuse in electronic relationships. Electronic harassment, which merges elements of both harassment and bullying, has already been recognized as the most significant social blogging problem in countries like China and South Korea. This electronic crime was also legally protected by an act, which was passed in Japan (June 18, 2003), and the act was about eliminating computer network harassment. In a Jordanian context, it is difficult to determine cyberbullying and harassment easily because of the lack of a definition or a legal term to describe these practices. Additionally, potential exists for the abuse of authority that was given to prosecutors, as they might perceive these acts as more severe than they are.

4. Investigation and Prosecution of Electronic Crimes

The investigation and prosecution of electronic crimes also represent a fundamental aspect of achieving the legal system's goals for addressing such offenses. It falls on law enforcement agencies to investigate the offenses, and then public prosecutors and courts to intervene in their prosecution, provided that the investigation and prosecution steps are performed in accordance with the rules and principles set forth in law to prevent recourse to illegal methods in collecting evidence during the investigation or at trial.

The aim of investigating these crimes, in addition to the operational procedures for the investigation, includes informing about the evidentiary expedients associated with this type of crime and the best methods to assist the victim, who is often a person from the community, the private sector, and government, or even a technology company, as well as ensuring the smooth and successful conduct of the investigation, which includes providing logistical and technical support and advice on conducting the investigation and providing the necessary tools and equipment for investigations.

Since electronic crimes take place on and through electronic networks, the investigation of such offenses requires law enforcement agencies in Jordan to carry out timely and well-executed procedures within a short period of time. This includes taking immediate and preventive action to prevent the continuation or reintroduction of the crime, raise security levels of networks, information systems, and data from theft, loss, or alteration and use them in other crimes, secure these systems against such acts, and take the necessary measures to ensure the continuity and sustainability of providing services and goods to individuals, companies, government agencies, and the vital sectors of the state.

Underwriting and Planning the Prosecution. In addition to the operational actions for the investigation of electronic crimes, the process of prosecuting these offenses includes informing the public prosecutor about all the evidence, no matter the format, electronic data, or hard copies, and the procedures to be followed for presenting them to the public prosecutor.

4.1. Role of Law Enforcement Agencies

Investigation and Prosecution of Electronic Crimes Role of Law Enforcement Agencies: In Jordan, the mechanism for cooperation among the government parties in the field of ICT is based on the e-Government Executive Committee (E-GEC) chaired by the Ministry of ICT. The E-GEC has two subcommittees for information security and privacy, and one for the protection of digital data. These committees are composed of representatives of the main

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 2 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

government operative entities in Jordan, including the Public Security Directorate, Intelligence Services (GIS.I), Gendarmerie (police), and prosecutors.

Public Security Directorate: It is the primary agency responsible for the prevention and investigation of crimes in Jordan. It is politically controlled by the Ministry of Interior and is responsible for the maintenance of internal security, social peace, and public order. Its main tasks are the investigation of criminal cases such as offenses, arrest of suspects, and the performance of any other activities that aim at the prevention of crimes from occurring. It has a number of specialized core investigatory and crime-agnostic units, and its main unit is the cybercrime unit. Responsibilities: The Public Security Directorate is responsible for most police functions, and regions are divided into districts and then subdivided into neighborhood centers. The main responsibilities of the Public Security Directorate are the protection of citizens and property, accomplishing security measures and operations, in addition to enforcing laws and regulations. Also, to provide and organize traffic, guide and help road users, and carry out administrative matters.

5. International Cooperation in Combating Electronic Crimes

Global cooperation is indeed an approach that is based on the fact that electronic crimes occur across borders, and here we find some mechanisms and agreements that contribute to one another's efforts. These agreements relate to bilateral agreements between two states, and multilateral conventions, with the goal of becoming members of the United Nations. I will first address the bilateral agreement, and then speak about the multilateral international agreement.

Bilateral Agreements: A bilateral treaty can be concluded between more than two states or between two states. Such an agreement is made between states at the same or different levels of development. If an electronically hostile person crosses the border with your country, your country may request the help of the other country so that you or the criminal can be brought to the neighboring country. This is just a simple example that shows that there might be problems that one country cannot solve alone, but it is necessary to have good size and effective regional or international cooperation in order to fight in a functional way.

Multilateral Conventions: Most countries in the world are members of the United Nations, so they can take effective action to respond to the phenomenon of transnational electronic crimes.

5.1. Bilateral and Multilateral Agreements

The extradition of alleged criminals is governed by bilateral and multilateral agreements. Various countries have signed agreements with neighboring countries, regions, and the international community to regulate their bilateral or multilateral cooperation on matters of detection, investigation, punishment, and extradition of persons committing electronic crimes, whether of their nationality or not. The importance of bilateral and multilateral agreements lies in determining the extent of international cooperation aimed at detecting, investigating, and punishing people who commit electronic crimes. Through these agreements, countries also define the mechanisms for international cooperation in this area, as well as the necessary ways to exchange information between the two parties. In the event an agreement against any of these electronic crimes is established among states, problems that may arise from the application of domestic law and extradition procedures cease to exist as long as the electronic crimes that take place in one country violate all the legal requirements from another country. These agreements could contribute greatly to the global response in the field of combating electronic crimes.

However, countries worldwide seem to have different attitudes concerning the possibility of considering electronic crimes within the scope of their agreements for extradition. Geographic considerations are among the factors that

influence countries' willingness to consider the extradition of a person for committing electronic crimes. For the American Embassy in Jordan, a number of agreements have been concluded to regulate the extradition of persons. These agreements cover all matters of extradition and include the detection, investigation, and prosecution of criminals. Such agreements include other measures, such as criminal record verification. The Anti-Strategic Aggression Act covers most electronic crimes. Moreover, the role of the police and the public prosecution is to coordinate with the authorities in the states where such agreements are signed.

6. Challenges and Future Directions

Computer and network operations, transactions, and the use of the internet are continuing to grow, thereby providing cybercriminals rather than traditional criminals. As cyberspace can be accessed from any point in the world, electronic criminals can commit crimes in other countries and remain outside the jurisdiction of a national or federal court in which the electronic burglary, use of computer for theft, etc., occur. The rate of increase of such criminal activity is very high, and many such criminal acts may never come to the attention of the prosecutor and the police. Moreover, there are no specialized rules of procedure and the legal and judicial system has not devised many new rules to combat computer crimes.

Young people are more likely to be influenced than older individuals and are influenced by the excitement and challenging nature of experimenting rather than criminal incentives, economic or otherwise. With increased internet use comes the potential for harm. There are many risks to using the Internet that might pose challenges to any approach to addressing them. Possibilities of future research in this regard may encompass the impact of judicial authority and manpower with training in electronic crimes units, the concept of unique internet law enforcement rather than traditional law enforcement agencies, clearance rates of electronic crimes, some more studies on criminology of cyber criminals' intentions, and legal efforts on the part of investigators to monitor the happenings of cybercrimes rather than to rely on the complaints from the victims of such crimes.

6.1. Emerging Trends in Electronic Crimes

Trends in electronic crimes approach is one of the most significant sections in this study. Electronic crimes gangs are changing their strategies, tactics, and techniques to get the most crime benefit. Prior to discussing whether such efforts are or are not successful, we need to sketch out the rationale underlying the shift in focus brackets and review what is new over the last ten years: invasive and insidious software, a growing criminal marketplace in commodities, offshore gambling, and rapid, shifting frauds made possible by the Internet. By identifying these emerging trends, we need to ask ourselves what we can do about them. The purpose of this section is, first, to acknowledge the range of developments in the electronic environment and technological capabilities that are likely to offer new frontiers for wrongdoing. The section is distinguished by analyzing the size, consequences, adaptability, and policy-making implications of these shifts. The purpose of this section is, secondly, to consider the implications of these trends for policing and regulation.

Developing an intelligence picture on changing trends in electronic crime is not made specifically difficult because of the changing nature of criminal activity. We consider that trends and strategies are worth studying particularly because such an approach is more likely to remain relevant over time with rapid changes in technology. There are two main parts to this section. First, we examine some of the directions in computer and telecommunications-related offending that have been reported in the early part of the new millennium. We look at some of the new criminal tactics that have made an impact in recent years in terms of their size, extent of

coordination that they require, and the consequences for victims. We consider the methods of offense that have their origins in the viral and other malicious programs space, including the invasion of privacy and the theft of confidential data. We go on to consider the development of a crime economy in the online environment comprised of two markets—the sale of the output of offending activity, and the intermediaries in crime that act as blast faxes and spammers do in connection with unsolicited marketing. The development of offshore betting and the involvement of organized crime in the industry offer some indication of the more organized efforts that criminals are willing to go to conduct sophisticated and profitable activities in the commercial sphere.

7. Conclusion

In conclusion, electronic crimes are considered one of the real dangers that threaten the security of individuals, institutions, and countries. Electronic crimes are not limited to acts committed by criminals in order to obtain material or moral benefits or for the purpose of carrying out terrorist operations, but they also represent acts that aim to violate human rights. Electronic crimes are posing more risks to the local communities because the users are not aware of the netiquette and unwritten norms applicable to the use. In addition, such crimes also show that technologies are prone to misuse. Finally, electronic message exchanges can provide evidence of crimes. In Jordan, the act that deals with electronic crimes does not provide an explicit definition.

This part provided an in-depth understanding of electronic crimes in Jordanian law, including the rationale for conducting this study and the definitions of electronic crime and information system that are contained in the Jordanian legal texts and the Organizational Chart of the Jordanian Civil Judicial Bodies. Moreover, this part described the fundamental characteristics of the Jordanian legal system, including an introduction to the Jordanian Penal Code and Cybercrime Law. Moreover, we presented several drafts proposed to Jordanian lawmakers that were drawn to the attention of the Jordanian Legislative System after translating them into three items. In addition, we provided a comparison between perspectives from a number of countries in dealing with electronic crimes. In conclusion, we overviewed several weaknesses in the old legal texts for the Jordanian public legal system. We reduce the electronic crimes by proposing a draft for actions related to them under Jordan. In the end, the main findings and the importance of this study have been mentioned.

References

- Ibn Manzur Al-Ifriqi Al-Misri, Jamal Al-Din Muhammad bin Makram Abu Al-Fadl: Lisan Al-Arab, Volume Three, Dar Sader, Beirut, without a year of publication
- Aloun,Dema Matouk, Women in Trade, International Journal of Recent Research in Social Sciences and Humanities (IJRRSSH) Vol. 11, Issue 2, pp: (97-106), Month: April - June 2024, Available at: www.paperpublications.org Page | 97 Paper Publications
- El-Gammal, Mustafa: The General Theory of Obligations, University Press, Without Country Publishing, 1997.
- Commercial Applications of Electronic Currencies. (2024). *International Journal of Religion*, *5*(10), 2126-2137. https://doi.org/10.61707/gqt3ng89
- Farag, Tawfiq: Lessons in General Theory, University Culture Foundation, Alexandria, without year of publication.
- Dr. Dema Matrouk Aloun. (2024). Legal Accountability for Commercial Contracts in Jordan Legislation. https://doi.org/10.5281/zenodo.12680957
- Aloun,Dema Matruk Aloun, Material copyright in Jordanian legislation, DOI: DOI: 10.13140/RG.2.2.22305.21605 April 2024

- Al-Sharqawi, Jamil: The General Theory of Commitment, Book One, Dar Al-Nahda Al-Arabiya, Cairo, 1995.
- Aloun,Dema Matruk Aloun, DOI: 10.13140/RG.2.2.33872.32008, February 2024
- Calling for unified efforts made by countries to regulate the use of the human genome, as isolated efforts made by countries are without effect or futility
- Commercial Applications of Electronic Currencies. (2024). International Journal of Religion, 5(10), 2126-2137. https://doi.org/10.61707/gqt3ng89
- Al-Amrousi, Anwar: Commentary on the Texts of the Amended Civil Code, 1st edition, all rights reserved to the author, 1978.
- Dr. Dema Matrouk Aloun. (2024). The Impact of Artificial Intelligence on Patents. International Journal of Recent Research in Social Sciences and Humanities (IJRRSSH), 11(2), 63–72. https://doi.org/10.5281/zenodo.11001028
- Dr. Dema Matrouk Aloun. (2024). Foreign Brands and its Effect on Economic Growth in Jordan. https://doi.org/10.5281/zenodo.12178724
- Samir Abdel Sayed: Commitment Theory, Mansha'et Al-Ma'arif, Alexandria, without year of publication.
- Aloun,Dema Matruk Aloun , Women's Economic Independence and Class on Gender Based Violence in Jordan, DOI: 10.13140/RG.2.2.28183.79521, February 2024
- Al-Qaradaghi, Ali Muhyiddin Ali: The Principle of Consent in Contracts, Part 2, 2nd Edition, Dar Al-Bashaer Al-Islamiyyah, Beirut.
- Dr. Dema Matouk Aloun. (2024). Women in Trade. International Journal of Recent Research in Social Sciences and Humanities (IJRRSSH), 11(2), 97–106. https://doi.org/10.5281/zenodo.11001210
- Al-Fadl, Munther: The General Theory of Obligations, Part One, Sources of Commitment, Dar Al-Thaqafa Publishing and Distribution Library, Amman, 1996.
- Al-Far, Abdul Qader: Sources of Obligation - Sources of Personal Right in Civil Law, Dar Al-Thaqafa for Publishing and Distribution, Amman, 2004.
- Aloun,Dema Matruk Aloun , Women's Economic Empowerment, DOI: 10.13140/RG.2.2.30097.44649
- Zarqa University. (2024). Commercial Cybersecurity. https://doi.org/10.5281/zenodo.12663385
- Article (169) and subsequent articles of the Journal of Judicial Provisions: "The offer and acceptance are in the past tense: such as "I sold and I bought," and whichever of these two words is mentioned first is the offer, and the second is acceptance."