Journal of Critical Reviews

ISSN- 2394-5125 Vol 7, Issue 8, 2020

THE IMPACT OF TECHNOLOGICAL DEVELOPMENT ON LEGAL RULES: A CASE STUDY OF JORDAN

Hazem Suleiman Toubat[1], Rohizan Halim[2], Nabeel Magableh[3]

[1] School of Law, Jadara University, Irbid, Jordan
[2] School of Law, UUM College of Law, Government and International Studies (COLGIS), Universiti Utara Malaysia, 06010 UUM Sintok, Kedah, Malaysia
[3]School of Law, Jadara University, Irbid, Jordan
E-mail: [1]toubathazem@yahoo.com/h.toubat@jadara.edu.jo

Received: 20.05.2020 ***Revised: 17.06.2020*** ***Accepted: 04.07.2020***

Abstract
The widespread use of technological means to exchange information has become a major alternative to traditional means, as technology has become one of the basic requirements for managing all day-to-day matters for individuals and institutions in both the government and private sectors alike. At the same time, the use of technology is surrounded by many risks, as information and communication technology systems and networks are exposed to various types of illegal acts, and can also be used to commit unlawful acts, which has raised the need to meet safety requirements and to combat these acts legally .Accordingly, the technological development clearly influenced the legal rules at the international and national level. At the international level, the United Nations General Assembly established a committee called the United Nations Commission on International Trade Law (UNCITRAL), which plays an important role in improving the legal framework for international trade. Jordan has also been affected, where new laws have been enacted and existing laws have been amended to suite this development. Using the doctrinal approach, this study examines how the Jordanian legislator has dealt with the new situation brought by technological development. The study concluded that the Jordanian legislator has taken important steps in amending some relevant laws to suit this development, including the Securities Law, the Evidence Law and the Civil Procedure Law. It has also enacted a special law on electronic transactions and another law on Cybercrime. Despite these efforts, there is a need to develop and enact new, mosre specialized laws to meet the new reality dictated by technology. Therefore, the study recommends the enactment of new laws, such as electronic commerce law, electronic government law, and electronic evidence law.

Keywords--- *Industrial Revelation, Jordan, Technological Development, Electronic Transactions Law, Cyber Crimes Law*

DOI: http://dx.doi.org/10.31838/jcr.07.08.311

INTRODUCTION

In the wake of successive industrial revolutions and rapid technological development, legal relations between individuals, and between individual and society, have taken another trend. This trend, in some aspects, comes out from the traditional simple physical frame to the complex electronic one that controlled by digital technology and computer monitors (Klaus, 2017). This technological development and its subsequent development in the means of communication affected the methods of conducting transactions, whether commercial or non-commercial. It also affected the methods and means of committing the crime to create the so-called Cybercrime, where the computer and the network are used as a tool to commit these types of crimes. Consequently, these developments impose a serious challenge on the legislators requiring the revision of all legislation in order to accommodate new developments. New legal rules that take into account this technological development should also be established in order to help develop mechanisms to deal with these types of transactions as well as to combat the crimes arising from such developments. Furthermore, such legal rules should harmonize technology with the ethical, customary and religious principles and values prevailing in society so that the legal rules does not stand helpless and incapable of dealing with the new development in technology. Therefore, laws have been enacted at the international and national levels to accommodate the new reality imposed by technological developments.

The extension of the law to the scientific fields aims to regulate the relationships that arise between individuals resulting from technological development. It also aims to protect individuals and society from the negative use of science and technology, where the vitality of the law emerges by keeping up with all the successive developments that occur in society. Consequently, this development affected the nature of the legal rules that were characterized by simplicity and ease of application to become more complex. New legal rules, which include scientific and technical terms, will require experience and competence of those who are dealing with them, especially lawyers, judges, and jurists to properly understand and apply the law.

Similar to other countries in the world, Jordan also has been affected by the technological development. This development has brought serious effect to the society with regard to the nature of legal relations and the means of committing crimes. It also jeopardizes the field of cyber and information security, which requires the Jordanian authorities to deal with these developments legally and institutionally.

This study deals with the impact of technological development on the legal system and the extent to which Jordanian authorities responds to the threats posed by the rapid and massive changes brought by the development in information and communication technology. To achieve the objectives of this study, a doctrinal approach was adopted in this regard. where, it provides an in-depth review and analysis of legislation that has been amended or enacted in response to technological developments, as well as its adequacy to deal with the challenges posed by these developments.

THE LEGAL FRAMEWORK FOR ELECTRONIC TRANSACTIONS

The term Electronic Transactions refers to transactions that are carried out in whole or in part by a computer or similar device connected to the Internet, including the exchange, transmission

and storage of information relating to mail, messages, bonds, records, signatures, electronic contracts, and electronic commerce. In addition to electronic funds transfer (Hadithi, 2011). Thus, electronic transactions involve all commercial and non-commercial activities related to the exchange of data and information as well as online goods and services between consumers and companies or between the companies themselves. Electronic transactions are characterized by rapid delivery of services, and transmission of information and data, as well as low costs and high quality. The rapid development of electronic transactions in all its forms requires a legal framework to regulate them and find solutions to all the problems and difficulties that may result therefrom. Accordingly, electronic transactions in all their forms have received international attention from the United Nations General Assembly, which established a special committee in this field. It has also received the attention of States through the enactment of domestic laws regulating this subject.

The Legal Framework for Electronic Transactions at the International Level

In light of the growing economic and trade interdependence at the international level, it has become necessary to improve the international legal framework to facilitate international trade and investment. Therefore, the United Nations General Assembly, by its resolution 2205 (XXI) of 17 December 1966, established a Commission called the United Nations Commission on International Trade Law (UNCITRAL). The Commission plays an important role in improving the legal framework for international trade; it prepares international legislative texts for use by States in developing international trade law. These texts deal with the international sale of goods; the resolution of international commercial disputes, including electronic commerce; arbitration and conciliation; insolvency, international transport of goods; international payments procurement and infrastructure development; and security interests. The Commission also prepares non-legislative texts for use by commercial parties in negotiating transactions. These texts include; rules of Arbitration and Conciliation Procedure; notes on conducting and organizing and arbitral proceedings; and legal guides on industrial construction contracts and countertrade(United Nations Convention on the Use of Electronic Communications in International Contracts, 2007).

The Commission recognized the importance of issuing a model law to be as a guide and reference in the case of enactment a national law governing commercial relations. Accordingly, it established the UNCITRAL Model Law on Electronic Commerce (1996). This law is indicative and not mandatory; it seeks to unify legal terminology in this branch of law, because of the difference between Anglo-Saxon and Latin legal schools. It can also contribute significantly to the development of harmonious international economic relations. The Commission also had a prominent role in the UNCITRAL Model Law on Electronic Signatures (2001). The Committee's work culminated in the United Nations Convention on the use of Electronic Communications in International Contracts (New York 2005). On the other hand, the Secretary-General of the United Nations launched in 2018 a strategy on new technology. This strategy aimed at identifying how the United Nations supports the use of technology to accelerate the achievement of the 2030 Agenda for Sustainable Development and facilitate its adaptation to the values enshrined in the United Nations Charter, the Universal Declaration of Human Rights, and rules and standards of international law. The strategy was based on guiding principles of protecting and promoting global values, especially in the areas of privacy and human rights, ethics, equality, sovereignty and responsibility, transparency and accountability (United Nations Secretary-General's Strategy on New Technology, 2018).

Despite the existence of these model laws and the international treaties on electronic business, national laws are the primary reference for resolving electronic commerce disputes. Therefore, laws have been passed to regulate these e-businesses, and other laws have been amended to keep up with these businesses.

The Legal Framework for Electronic Transactions in Jordan

Jordan began to keep pace with the technological developments that accompanied the Industrial Revolution since the early 1970s, where Jordan has since started to use computers in a limited way. In the 1980s, there was a clear progress in this area, Computer and information technology has been introduced to many institutions in the public and private sectors as well as in education in public schools **(**Jordanian Ministry of Industry and Trade, Summary of Information Technology Sector, 2010**)**.In the field of E-commerce, Jordan has started using networks in the field of electronic commerce since the beginning of this century. While social networking sites play an important role in this field and other E-business such as E-marketing.

In 2001, the Jordanian government launched the E-government program, which means the use of information technology and the Internet to provide government information and services to citizens electronically. In conjunction with the launch of E-government program, the Jordanian legislator made several amendments to relevant laws to conform with the new development. Meanwhile, it issued a temporary law on electronic transactionsin. This law, which named the Electronic Transactions Law No. 85 of 2001, was enacted with the aim of facilitating the use of electronic means in conducting transactions, where the Law legitimizes electronic transactions, and enables parties to prove rights and obligations by using electronic means or that resulting from the use of electronic means. In 2015, this law has been replaced by Electronic Transactions Law No.15 of 2015, which aims to promote E-commerce by clarifying the legal framework for doing business online or concluding contracts through electronic means of communication, where the Law was based on the Model Law on Electronic Commerce of UNCITRAL on December 16, 1996.

Provisions of the Electronic Transactions Law No.15 of 2015

According to the Electronic Transactions Law of 2015 the word "Transaction" covers all transactions, whether commercial or non-commercial, that are carried out through electronic means, including electronic records, electronic data messages and electronic signature, where they are accepted by the courts as authentic evidence alongside traditional means based on bonds and testimony (Electronic Transactions Law of 2015, Article 2). In addition, the Law gives electronic records the same legal value as written documents, provided that such records meet certain security and technical requirements(Electronic Transactions Law of 2015, Article 17).

Article (2) defines certain new terms that are related to technological developments. It defines the concept of transaction, stating that "Transactions are any procedure between one party or more to establish an obligation upon one party, or mutual obligations between two parties or more in relation to a business transaction, a civil work, or a work with a government department", while it defines the Electronic Transactions as any Transactions carried out by electronic means. Moreover, it explained that the electronic means are "the technology of using electronic, magnetic, optical, electromagnetic, or any other similar means". The law also defines the electronic document, the electronic signature, the electronic intermediary and the electronic information message. It gives each of these words a specific and precise meaning to distinguish it from other terms. The Law considered that electronic transactions produce the same legal effects as documents and written bonds in terms of obligation of the parties and their validity in proof.

The electronic mail message is defined as "information created, archived, received or stored by any electronic means, including electronic mail, SMS or any electronic exchange of information. Article (9) considered the information message to be a means of expression of the legally accepted administration of consent and acceptance with a view to establishing a contractual obligation.

With regard to electronic signature, the Electronic Transactions Law of 2015 has adopted the provisions of the UNCITRAL Model Law on Electronic Signatures of 2001. According to Article (2) of Electronic Transactions Law, electronic signature refers to "Information in the form of letters, numbers, codes, symbols, or other and which is electronically, or in any other similar mean, included in, affixed to, or associated with an electronic record. It is used to authenticate the identity and unique usage of the signatory and differentiate him from others". Moreover, the Law contains detailed provisions on electronic signatures, specifying the conditions for electronic signatures to be considered protected or documented (Electronic Transactions Law of 2015, Article 15).

With respect to the authentication authorities, the Law indicates that the Ministry of Information and Communications Technology is the main authentication entity for government agencies, official institutions, and municipalities (Electronic Transactions Law of 2015, Article 5). It shall issue electronic authentication certificates to be used in transactions related to any of the aforementioned institutions. However, The Council of Ministers may, upon the recommendation of the Minister of Information and Communication Technology, appoint any public official committee, institution or government department to issue electronic authentication certificates, while the Central Bank is responsible for the authentication of electronic banking transactions.

This Law also established a clear legal basis for electronic government, where the law recognizes government transactions and procedures implemented through electronic means. Ministries, official and public institutions and municipalities are allowed to conduct their transactions using electronic means (Electronic Transactions Law of 2015, Article 4). They are also required to conduct transactions electronically, to establish electronic records, to use electronic signature, provided that the trading requirements of this law and the regulations and instructions issued pursuant thereto are met. Electronic records and transactions should also be kept secure and their confidentiality and integrity protected. Moreover, it considered the transfer of funds by electronic means an acceptable method of payment, and authorized the central bank to issue relevant instructions to put these payment instruments into actual legal use. The Law also requires each payment and electronic transfer company to obtain a license from the Central Bank of Jordan (Electronic Transactions Law of 2015, Article 22).

The Law exclusively excludes from the scope of its provisions a number of subjects of a special nature as stipulated in Article 3 thereof.

a. "Establishing and amending a will.
b. Establishing Waqf and amending its conditions.
c. Transactions related to movable and immovable properties that legislations necessitate their registration including their power of attorney, their title deeds, in addition to establishing real rights, excluding lease contracts. These transactions include, for example, registering real estate in the Department of Lands and Survey, and vehicles in the Vehicles and Drivers Licensing Department.
d. Powers of attorney and transactions related to civil status.
e. Notices related to canceling or revoking contracts of water and electricity services, health insurance, and life insurance.
f. Court proceedings and pleadings, judicial notification notices, and court resolutions.
g. Securities unless provided under special regulations issued by competent authorities in accordance with the Securities Law or any other legislation in force".

Laws Amended to Suit Technological Developments

In addition to the Electronic Transactions Law as the main law governing electronic transactions in Jordan, other laws have been amended or replaced to cope with technological developments, such as:

1. The Securities Law No. 18 of 2017, which replaced the temporary Securities Law No. 23 of 1997. Article 110 Paragraph (c) of this Law provides for the possibility of proving cases of securities by all means of proof, including electronic data or computer, and records of telephone, telex and fax, and facsimile messages.
2. Article 92, Paragraph (b) of the amended Banking Law No. 28 of 2000 stipulates that: all means of evidence shall be permitted in banking cases, including electronic data, computer printouts and telex correspondence". Paragraph (c) allows banks to maintain reduced copies (microfilms or other modern technology devices) to replace records, books, documents, data, original correspondence, correspondence, cables, notices, and other paperwork related to their financial operations. These reduced copies shall be as authoritative in evidence as the original". Similarly, Paragraph (d) Article provides that banks which use computers or other modern technological equipment to regulate their financial operations shall be exempt from the retention of the commercial records provided for in the applicable trade law, where the information stored in these devices or other modern means is considered as commercial records.
3. In the field of intellectual property legislation, Article 3, Paragraph (c) of the Industrial Designs Law No. 14 of 2000 allowed the Ministry of Industry and Commerce to maintain computerized records for the registration of industrial designs and related data. The data and documents retrieved from them and authenticated by the Registrar must be treated as a valid evidence against others.
4. In Article 3, Paragraph (c) of the Protection of Layout-Designs of Integrated Circuits Law No. 10 of 2000, approved the use of computers to record designs and related information. It also considered that the information and documents derived from such devices approved by the Registrar shall be sufficient evidence towards all, unless the parties concerned prove otherwise. The same provision is contained in Article 7, Paragraph (c) of the Patent Law No. 32 of 1999, where a computer may be used to record patents and their details, and computer data and its extracts are binding on all.
5. In 2017, the Civil Procedure Law was amended with the aim of reducing the slow pace of legal proceedings in the field of litigation. Under these amendments, electronic judicial notification and the possibility of filing the case electronically were recognized. The law authorized court officials to send judicial notice to parties to the case through a mobile phone message or any other electronic means specified by a special regulation.

Based on the foregoing, it has been shown that since the beginning of this century, the Jordanian legislator has shown a clear interest in developing a legal framework governing electronic transactions in all its forms, whether the parties are legal persons for public law (government or official institutions)or private law (individuals and companies). Through the Electronic Transactions Law, the legislator regulated all transactions related to technological developments such as electronic correspondence and records, electronic signature, authentication, payment and electronic transfer. It also regulates the obligations and responsibilities of protecting electronic transactions and its systems. Meanwhile, the judge can resort to traditional laws to cater any deficiencies or lack of provision in

electronic laws. However, the Jordanian legislator did not follow the UNCITRAL approach, which enacted several laws to deal with electronic transactions. The Commission passed a law on electronic transferable records, a law on electronic commerce and another law on electronic signatures. The committee's approach of enacting various laws is better than that of the Jordanian legislator, which is content with the Electronic Transactions Law, where technology is constantly evolving and the resulting transactions and their details are also increasing. Therefore, it would be better to enact specific laws to deal with each form of electronic transaction.

PHENOMENA AND CRIMES RESULTING FROM TECHNOLOGICAL DEVELOPMENT

Although the information systems and their accompanying evolution in data processing and transmission have enabled access to services at high speed without effort or time, however, the spread of the Internet and the development of these systems have created new types of crimes called Cybercrimes, which differ in their means and tools from conventional crimes. Moreover, it has recently emerged a new and dangerous phenomenon that could threaten the future generations; this phenomenon is called Digital Drugs or Binaural Beats. This means that the risks from technological development have increased and that the methods for committing crimes have also evolved. Therefore, it is necessary to confront the threat posed by incorrect use of technology, and to develop means to counter this threat (Fawzi, & Mansouri, 2017).

Concept of Cybercrime

Cybercrime is defined as illegal activities conducted by using a computer or other technological device connected to the cyber space. This crime includes illegal access to a computer, an information system, or a computer network, distribution of illegal materials in cyber space, such as child pornography materials, pirate software, and stolen properties. It also includes the forgery or destruction of a document, record, electronic signature, system or website, seizure of a benefit, money or document using fraudulent methods, access illegally to hardware, software, or data sources (Zheng et al, 2003). On the other hand, electronic means and the Internet can be used to commit crimes that affect individuals by harming their reputation, or society by disturbing public order, public morals, public security or inciting violence (Yar & Steinmetz, 2019).

Information is often the target in Cybercrime, especially since the digital virtual world relies primarily on information as an electronic trading tool and that the criminal scene itself is the digital space, and even crime tools are also to and from the digital virtual world. Thus, Cybercrime may be a transnational crime. In this sense, Cybercrime can be divided into two types:

1. Crime in which electronic means are used as a tool to commit crimes , such as in the case of defamation, slander, libel, threat or distribution of illegal materials.
2. Crime in which electronic means or their contents are themselves the target, such as when an information system is destroyed, information is stolen from an electronic site or system, or infringement of privacy and confidentiality(Ngafeeson, 2010).

Cybercrime has elements that distinguish it from conventional crime, both in terms of the means used to commit it, where it was committed, or the subject of the crime. This is due to the demise of geographical boundaries and the lack of restrictions on movement within the information network, which made it difficult to track it and identify the perpetrators (Ash- Shahri, 2011). The difficulty of determining the material element required for criminalization, or the absence of a legal provision criminalizing acts committed against the information system or information network, makes it difficult to impose a penalty on the acts committed through electronic means(Bin Qara Mustafa, 2010).

Moreover, the perpetrator of Cybercrime is often intelligent and may be a specialist or skilled in the field of informatics and programming, and therefore has the skill to hack networks, break codes and passwords or access and obtain accurate information. Hence, the perpetrator may resort to fraudulent methods, fake names and sites or undocumented electronic mail, and may destroy and erase electronic data immediately, thereby erasing the means of committing the crime and the identity of the perpetrator. Consequantly, the evidence in these crimes has become less accurate and complex (Awad,2017). Accordingly, the legislation on conventional crimes has not been able to keep abreast of developments in this type of crime, nor can the normal means of proof be applied to it. It is therefore necessary to enact new legislation to address this type of crime in all its forms.

The Legal Framework for Cybercrime in Jordan

Cybercrime is one of the most recently categorized crimes in Jordan. Jordan's interest in these crimes began in 2008 with the establishment of the Cyber Crimes Unit in the Criminal Investigation Department of the Public Security Directorate. This Unit is responsible for investigating information and communications technology and Internet crimes. In 2014, Ministry of Communications and Information Technology established a center to Combat Cybercrime and cyber security threats, which is called the National Center for Information Technology, to serve as a reference for the security and safety of information and networks.

At the regional and international level, Jordan has ratified a number of international and regional conventions regulating this field, such as the Arab Convention on Combating Information Technology Offences organized under the umbrella of the Arab League in 2010. This agreement aims at enhancing and improving cooperation among Arab countries in the field of combating cybercrimes to prevent its dangers in order to preserve the security and interests of Arab states and the safety of their societies and individuals. The agreement also includes penalties for introducing, modifying or withholding certain information, cyber fraud, interfering with the sanctity of private life or broadcasting unethical acts(Arab Convention on Combating Information Technology, 2010).

The principle of legality provides that criminalization and punishment may only be permitted in accordance with a legal text. Accordingly, perpetrators of harmful or dangerous behavior to society and individuals may not be punished through the use of computers and the Internet without a legal provision criminalizing such an act.Therefore, a temporary law was issued in Jordan in 2010 named the Information Systems Crimes Law No.30 of 2010. This law laid down the foundation for combating Cybercrime, in particular piracy, infiltrating privacy and eavesdropping on what is sent online, as well as tracking crimes related to online fraud, credit card theft and financial and banking transactions. However, it did not address crimes committed by using social media. In 2015, this law was replaced by the Cybercrime Law No. 27 of 2015, which includes provisions relating to the crimes of defamation, slander, and contempt committed by using technological means and the Internet. The enactment of this law has made it easy to track Cybercrimes and punish their perpetrators.

The Law protects programs and tools designed to create data, access information systems and the Internet. It is also impose sanctions on those who violate or exploit any of them to sabotage, disclose, modify, or alter information. The Law punishes those who intentionally enter an information network or system by any means without authorization or exceed a permit given to him, by imprisonment for a period of not less

than one week and not more than three months, or a fine of between 100 and 200 Jordanian Dinars(JD) or both penalties. The penalty becomes imprisonment for a period of not less than three months and not more than one year with a fine ranging from 200 to 1000 JD in the event that access to the information system to cancel, delete, add, destroy, disclose, withhold, modify or disrupt the network or network information system(Jordanian Cybercrime Law, Articles 3,4).

The Law also deals with crimes related to the interception of payment, clearing, settlement or electronic banking services provided by banks and financial companies.It also deals with crimes of obtaining credit card information, or information and data used in the execution of electronic financial and banking transactions illegally and without authorization from the owner. The law specifies for these crimes, the penalty of imprisonment for a period not less than one year and not more than three years and a fine ranging from 500 to 2000 JD (Jordanian Cybercrime Law, Article 5).

To protect public order and public morality ,the law punish any person who transmits or disseminates intentionally through an information system or the information network all that is audible, legible or visible, including pornographic acts relating to sexual exploitation of those who have not attained the age of eighteen years. The sentence is imprisonment for a period not less than three months and not more than one year. The Law also punishes anyone who uses the information network or information system, creates a website to facilitate or promote prostitution, or who intentionally transmits or disseminates data or information through the information network, website, or any information system involving defamation or slander , or insult anyone(Jordanian Cybercrime Law, Articles 9,10,11).

In order to counter the possibility of using the means of modern technology to spread hate speech in society, amendments were made to the Cybercrime Law in 2018. Under these amendments hate speech was defined as "any statement or action that may provoke strife, religious, ethnic or regional strife, advocating, inciting or justifying violence or spreading rumors against any person that would harm his body, property or reputation." The Government justified these amendments as a response to the rapid technological development in the means of communication and the widespread use of the information network, whether in the social media or smart device software applications. These amendments were also justified as being aimed at punishing those who misuse these methods, on the grounds that the current Penal Code does not address the crimes committed by these technological means.

Therefore, these amendments aimed at punishing those who misuse these means, arguing that the current Penal Code does not address the crimes committed by these technological means. However, Cybercrime Law and its amendments have been criticized that it could be used as a means of restricting freedom of expression and making the law as a barrier between citizens and public censorship on state employees**.** It can also be used to violate the right of privacy of Jordanians guaranteed by the Constitution (Atout, 2018).

Digital Drugs

It is known that addiction is linked to conventional drugs, whether plant or manufactured, which have a serious impact on the nervous, central, respiratory and circulatory systems. However, due to technological development, a new type of drug has emerged in which musical notes are used in a way that may lead to addiction and then affect brain functions. Meanwhile it affects the addict's psychological and physical state, and isolate him from socializing normally. This type of drug is called Digital drugs.

Concept of Digital Drugs

Digital Drugs are audio files that are sometimes associated with visual materials, shapes and colors that move and change according to a thoughtful rate engineered to fool the brain by transmitting sound waves of different frequency in a simple way to each ear. These sound waves are unusual. The brain unites the frequencies of the ears to reach one level, thus becoming unstable electrically. Depending on the type of difference in the brain's electrode, a certain sensation is emulated, which simulates the feeling of one of the drugs or feelings that you want to reach, such as ecstasy. Digital drugs are obtained through specialized websites that sell these tones. as these drugs are promoted on various social media sites, and can also be obtained free of charge on YouTube(Charlotte & Phil, 2011).

The Prevention of the Digital Drugs

Despite the dangers posed by digital drugs to society and individuals, an international or national strategy to deal with this phenomenon has not yet been developed. Therefore, the risks posed by digital drugs require the development of an integrated strategy and necessary legal measures to counter this phenomenon.

This phenomenon can be faced by:

a) Monitor websites that offer this type of digital drug or block it permanently at the national level, and then work within an international network to combat it.

b) The necessity of enacting special laws or developing anti-drug laws to criminalize dealing with or promoting these digital drugs.

c) Establishing specialized international institutions to follow and study negative practices that are published on websites and to develop appropriate solutions for them.

d) Countries, in cooperation with civil society institutions, should adopt awareness-raising initiatives with a view to educating young people and providing them with a culture of rational use of modern technology, and urging them to use the Internet safely.

CONCLUSIONS

The world is witnessing a revolution in technology, as technology largely controls everyday life and intervenes in all its details, whether in practical or scientific life, where some traditional tools have been replaced by electronic or technical tools. Although technological development positively affects the means of conducting transactions, facilitates interpersonal communication, and reduces time and effort, it has created some challenges posed by the negative effects of technology, and affected the means of committing crime.

Technology has become a force and a source for enacting and developing legal rules, as the nature of these rules and the procedures for enacting them have changed, resulting in that legislators have not been able to legislate according to traditional procedures, they are forced to include scientific and technical terms in legal texts, which requires the use of experts and specialists in the technical field to understand the secret of technology.This is also the case for judges and lawyers who must also seek the help of experts and specialists to understand and implement legal texts. On the other hand, technological developments have imposed the necessity to coordinate international and national efforts in the legal field to meet the challenges posed by this development. Accordingly, national law cannot operate in isolation from international law.

These technological developments have forced the Jordanian authorities to adopt a national strategy for regulating the relationships arising from these developments, ensuring information and cyber security, and protecting society and individuals from the threat of crimes stemming from it. As part of this strategy, Jordan has revised and amended a number of

relevant legislation to suit these developments, including the Securities Law, the Banking Law, and the Civil Procedure Law. It also enacted two new laws, one dealing with electronic transactions and the other dealing with Cybercrime.The Electronic Transactions Law contains general provisions covering all electronic business, whether commercial or non-commercial, including electronic signature, electronic authentication, electronic commerce and also includes provisions related to electronic government. However, since the electronic transactions is complex and constantly evolving, an integrated legislative system is required in this regard . Therefore, there is a need to enact other laws covering all branches of electronic transactions such as electronic government law, electronic commerce law and electronic evidence law.

With regard to crimes resulting from technological development that threaten the interests of individuals and society, Cybercrime Law has addressed this type of crime. It includes provisions criminalizing access to the information network without permission in order to delete, add, destroy, disclose, damage, block, modify, change, transfer or copy data or information or stop or disrupt the operation of the information network. Likewise, in order to protect public order or public morals, the law included provisions criminalizing and punishing anyone who intentionally used the information network to promote what would violate public order and public morals or use the Internet to attack or defame individuals 'privacy. However, this Law is not without criticism as it does not balance the protection of individuals and society from the threat of Cybercrime, on the one hand, and the protection of human rights guaranteed by the Constitution, such as the right to expression, on the other hand.Meanwhile , the law does not address the issue of digital drugs in terms of criminalization and punishment, and the reason for this may lie in the fact that this type of drugs has not reached the level of a worrying phenomenon in Jordan that needs to be confronted legally.

REFERENCES

1. Ahmed .K. Farah. (2007) .The Legal System for Providers of Internet- Comparative Analytical Study. Al - Bayt University, Al-Manara Journal of Research. 13(9), 319-390.
2. Aisha bin Qara Mustafa. (2010). Authenticity of the electronic evidence in the field of criminal proof in Algerian and Comparative Law. Alexandria: New University House.
3. Ali .K. Hadithi. (2011). "The Nature of Electronic Transactions and the Legal Consequences of a Legal Dispute (Comparative Study)." Yearbook of the Forum 1, no. 7: 63-124.
4. Akram .R. Antar, & Raghda Moawad. (2015). Electronic Arbitration in Electronic Tourism Disputes. Journal of Faculty of Tourism and Hotels, Vol. 12, (1). 2015.
5. Arab Convention on Combating Information Technology Offences, Preamble. (2010). Available at: https://www.asianlaws.org /gcld/ cyberlawdb/ GCC/Arab% 20 Convention%20on%20Combating%20Information%20Technology%20Offences.pdf
6. Atout, Omar. (2018). Why should we reject the Cybercrime Law? October 14, 2018. https://www.7iber.com/politics-economics/why-we-should-reject-cyber-crimes-law/
7. Badran, Ibrahim. (2018). Social Transformations and Industrial Revolutions. .Al-Rai Newspaper. Available: http://alrai.com/article/10421170/
8. Charlotte Walsh LLB and M.Phil. (2011) Drugs, the Internet and Change, Journal of Psychoactive Drugs, 43:1, 55-63, DOI: 10.1080/02791072.2011.566501.
9. Dolbow, L. E. (2017). Introduction: The Power of New Data and Technology. V and. L. Rev., 70, 1935.
10. El Faily. H. Mohamed. (2013). Law and the Use of Telecommunications Technology in Government Administration and Electronic Transactions. National Conference on Electronic Legislation, University of Kuwait.
11. Fawzi, M. & Mansouri, A. (2017). Awareness on Digital Drugs Abuse and its Applied Prevention among Healthcare Practitioners in KSA. Arab Journal of Forensic Sciences & Forensic Medicine (AJFSFM), 1(6).
12. Hasan Ash- Shahri. (2011). Unified International Law to Combat Cybercrime (Proposed Concept).The Arab Journal for Security Studies and Training, Vol. 27, No. 53.
13. Jordanian Electronic Transactions Law No. 15 of 2015. Available at: http://www.cbj.gov.jo/EchoBusV3.0/SystemAssets/bec70415-2845-42df-bc47-5e0ee 4b859b7.pdf
14. Jordanian Ministry of Industry and Trade. Summary of Information Technology Sector. 2010. Available at: https://www.mit.gov.jo/ EchoBusV3.0/ System Assets/ PDFs/AR/
15. Koops, B. J. (2010). Law, technology, and shifting power relations. Berkeley Tech. LJ, 25, 973.
16. Ministry of Justice in Jordan. Laws and Regulations. http://www.moj. gov.jo/ Pages/ viewpage.aspx?pageID=132
17. Morrar, R., Arman, H., & Mousa, S. (2017). The fourth industrial revolution (Industry 4.0): A social innovation perspective. Technology Innovation Management Review, 7(11), 12-20.
18. Ngafeeson, Madison. (2010). "Cybercrime classification: a motivational model." College of Business Administration, the University of Texas-Pan American 1201.
19. Omar Atout. (2018). Why should we reject the Cybercrime Law? October 14, 2018. https://www.7iber.com/politics-economics/why-we-should-reject-cyber-crimes-law/
20. Prisecaru, P. (2016). Challenges of the fourth industrial revolution. Knowledge Horizons. Economics, 8(1), 57.
21. Resolution adopted by the General Assembly [on the report of the Sixth Committee (A/51/628)] 51/162 Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law. Available at: https://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf
22. Schwab, Klaus. (2017). The fourth industrial revolution. Currency.
23. United Nations Convention on the Use of Electronic Communications in International Contracts. https://www.uncitral.org/pdf/english/texts/electcom/06-57452_Ebook.pdf
24. United Nations Secretary-General's Strategy on New Technology, of the United Nations, (2018). Available at: https://www.un.org/en/newtechnologies/
25. Yar, Majid, & Kevin F. Steinmetz. (2019). Cybercrime and society. SAGE Publications Limited.
26. Yaser Awad. (2017). Proof of Cybercrime with Scientific Evidence. Tikrit University Law Journal, *3*(2), 3-2: 476-506.
27. Zheng, Rong, Yi Qin, Zan Huang, & Hsinchun Chen. (2003). Authorship analysis in cybercrime investigation. In International Conference on Intelligence and Security Informatics, pp. 59-73. Springer, Berlin, Heidelberg.