OPEN ACCESS

Scholars International Journal of Law, Crime and Justice
Abbreviated Key Title: Sch Int J Law Crime Justice
ISSN 2616-7956 (Print) | ISSN 2617-3484 (Online)
Scholars Middle East Publishers, Dubai, United Arab Emirates
Journal homepage: https://saudijournals.com

Review Article

Jordanian Cybercrime Law No. (17) of 2023 between Regulating Social Media Sites and Restricting Freedom of Opinion

Dr. Riyad Mahmoud Al-Sarayreh[1*]

[1]Royal Police Academy, Faculty of Law, Mutah University, Karak, Jordan

DOI: https://doi.org/10.36348/sijlcj.2024.v07i09.002 | **Received:** 24.07.2024 | **Accepted:** 03.09.2024 | **Published:** 07.09.2024

***Corresponding author:** Dr. Riyad Mahmoud Al-Sarayreh
Royal Police Academy, Faculty of Law, Mutah University, Karak, Jordan

Abstract

The primary objective of this research is to study the Jordanian Cybercrime Law No. (17) of 2023 between regulating social media sites and restricting freedom of opinion. In addition, it clarifies the concept of cybercrimes and how to control social media sites while preserving citizens' rights to freedom of expression. In terms of balancing digital security and controlling social media sites. Defining concepts and terms, such as "regulating" social media sites and "restricting freedom of opinion," is crucial to understanding the law's impact on users. Monitoring and implementing the law by the competent authorities to avoid excessive violations of individuals' rights. The researcher used the descriptive analytical method, as well as the inductive method, and the legal text analysis tool was used. This research has reached several results, the most important of which are that the Jordanian cybercrime law has used broad, vaguely defined, inaccurate, ambiguous, and non-specific terms, such as fake news. Even though these texts do not meet the requirements of international law regarding drafting legal texts precisely enough to allow individuals to regulate their behavior accordingly. In addition, the Jordanian cybercrime law focused on the penal and punitive dimensions and did not include any institutional or preventive measures to reduce negative phenomena in the digital environment. This research has reached several recommendations, the most important of which are that the Jordanian legislator must reconsider amending legal texts that are unfair to internet users in a way that leads to the adoption of balanced legal texts compatible with basic rights. These rights include the right to exchange information, the right to express opinions and ideas, and the right to privacy, which the Jordanian Constitution guarantees in Article (7).

Keywords: Crimes, Cybercrimes, Freedom of opinion, Individual rights, Jordan.

INTRODUCTION

Cybercrime issues have become a vital topic in the modern era, as the reliance on technology and social media platforms continues to grow in everyday interactions between individuals. In this context, various countries' legal regulations define the boundaries of safe and responsible use of information and communication technologies. In the Hashemite Kingdom of Jordan, Cybercrime Law No. (17) of 2023 was adopted, aiming to keep pace with the rapid developments in the world of technology and to protect society from new challenges that may arise due to the irresponsible use of social media sites. Among the important aspects addressed by this law are the issues of regulating social media sites and restricting freedom of opinion. This regulation requires identifying mechanisms by which content on these platforms can be regulated without infringing on individuals' rights to express their opinions. It must have a delicate balance that ensures protection from misuse and cybercrime without compromising individuals' rights to freedom of expression. (Al-Taie, 2013: 2-12).

This law establishes the responsibilities and penalties for individuals who violate regulations related to electronic communication. It also includes mechanisms for monitoring content to ensure the preservation of digital security and the rights of citizens. The enactment of the Cybercrime Law in Jordan represents a significant step towards achieving a balance between the use of technology and the protection of individual rights, particularly concerning social media platforms and freedom of expression, while safeguarding national security and maintaining societal stability. (Cybercrime Law No. (17) of 2023).

Research Problem

The problem of this research lies in addressing the Jordanian Cybercrime Law No. (17) of 2023 between regulating social media sites and restricting freedom of

opinion. In terms of the difficulty in understanding the definitions of some terms used in the law, which leads to a lack of clarity in the concepts related to "regulating social media sites" and "restricting freedom of opinion". By addressing the following main question: To what extent does the implementation of the Jordanian Cybercrime Law No. (17) of 2023 aligns with regulating social media sites and restricting freedom of expression. The main question is further divided into the following sub-questions:

1. What is the concept of crimes and cybercrimes and their types?
2. What is the concept of freedom of expression and its importance in the digital age?
3. What is the concept of individual rights in the digital age from the perspective of international legislation and legal frameworks for cybercrime laws?
4. What is the nature of the conflict between freedom of opinion and the Cybercrime Law on regulating social media sites in the Jordanian legal context?
5. How does this law impact the experience of ordinary users of social media sites?
6. Are there any previous cases or examples that illustrate how this law has been implemented and how it has impacted freedom of expression?

Research Objectives

1. Clarify the concept of crimes and cybercrimes and their types.
2. Clarify the concept of freedom of opinion and its importance in the digital age.
3. Clarify the concept of individual rights in the digital age from the perspective of international legislation and legal frameworks for cybercrime laws.
4. Highlight the impact of this law on the experience of ordinary users of social media sites.

Theoretical and legal framework

The nature of crimes under legal systems

The concept of crimes and their types.

First: The concept of crime

A crime is defined as an act that violates the law and is punishable under the legal systems of most countries. The definitions and types of crimes vary from one country to another, depending on the laws and legal systems in place in each country. A crime can be defined as any act or omission committed by a distinguished person that causes a general or specific social breach or disturbance and is punishable by law with a criminal penalty or precautionary measure. (Najm, 2014: 10).

Second: Types of crime (Al-Majali, 2010: 37-38)

There are some common crimes and main types of crimes that can be classified as follows:

1. Crimes against the person.
2. Crimes against property.
3. Crimes against finances and the economy.
4. Crimes against the public.
5. Terrorism.
6. Crimes against the environment.
7. Cybercrimes.

The concept of crimes and their types in Jordanian law

First: The concept of crimes in Jordanian law

The Jordanian Penal Code No. (16) of 1960 and its amendments until (2021) did not include a definition of the crime, leaving that to jurisprudence. These crimes and penalties are regulated within the law according to the legislation and legal systems regulating criminal behavior in the Hashemite Kingdom of Jordan. Article (3) of the same law states: "There is no crime without a text, and no penalty or measure shall be imposed that was not stipulated by law at the time the crime was committed. The crime shall be considered complete if the actions to implement it are completed, regardless of when the result occurred.

Some of the most important basic concepts in the Jordanian Penal Code are:

1. Crime: In the legal context, a crime refers to any act that violates Jordanian law and subjects the perpetrator to legal accountability.

2. Criminal Crime: These crimes involve criminal penalties, such as imprisonment, confiscation of property, and other measures imposed on the accused as a means of punishment and deterrence or other penalties that can be applied to the offender.

From the above, it becomes clear to the researcher that the Jordanian Penal Code defines a variety of crimes, including crimes against persons and property, economic, environmental, and moral crimes, and many other laws related to crimes.

Second: Types of crimes in Jordanian law

Articles (16) to (25) in Chapter Two – in Criminal Provisions, Section on Penalties (in general, criminal, misdemeanor, and disturbance) of the Jordanian Penal Code No. (16) of 1960 and its amendments until 2021 stipulated some types of crimes, including:

1. Criminal crimes.
2. Economic crimes.
3. Environmental crimes.
4. Technological crimes (cybercrimes).
5. Administrative crimes.
6. Human crimes.
7. Health crimes.
8. Political crimes.

From the above, the researcher believes that individuals must abide by the laws and regulations in force in Jordan. In the event of any crime being

committed, the legal authorities will take the necessary measures to punish those involved and achieve justice.

The nature of cybercrimes under legal systems

Emergence and development of international legislation and legal frameworks for cybercrime laws.

International cybercrime laws and legal frameworks refer to a set of conventions and legislations that have been developed over time to combat criminal activities conducted online. These laws and legal frameworks have evolved as a result of the increased use of digital technology and the Internet in cybercrimes. Therefore, most Arab countries (through the Arab Convention on Combating Information Technology Crimes, 2010) and countries worldwide have begun to establish laws and legal frameworks to address these crimes effectively. The main points that contributed to the emergence and development of these international legislations and legal frameworks (Council of Europe, 2001) are:

1. The United Nations and international organizations.
2. International cooperation.
3. Updating local laws.
4. Investigation and trial frameworks.
5. Data protection and privacy.

These international and legal efforts aim to address the emerging challenges of cybercrimes and ensure legal justice and protection for individuals and institutions in the digital age.

Concept of cybercrimes and their types.

Cybercrimes are criminal activities related to technology, digital systems, and electronic networks. These crimes involve the use of technology and electronic devices to conduct illegal activities, manipulate data, breach security, and commit other crimes online (United Nations Office on Drugs and Crime, 2013). The types of cybercrimes include the following (Al-Badayneh, 2014):

1. Security breaches.
2. Online fraud.
3. Identity theft.
4. Cyber espionage.
5. Incitement to hatred and terrorism online.
6. Digital extortion.
7. Online defamation.
8. Financial cybercrimes.
9. Illicit trade.
10. Cyber threats.

From the above, the researcher believes that cybercrime is a rapidly developing field that requires continuous efforts to combat these criminal activities.

Cybercrimes and Jordanian laws and legislation

These laws and legislations aim to provide a legal framework to combat cybercrimes and ensure the protection of individuals' rights on the Internet in Jordan. Effective implementation and continuous guidance of arbitrators and security forces are required to deal with the growing challenges in the field of cybercrime.

Cybercrimes from the perspective of Jordanian laws

The Jordanian legislative system contains many laws that deal with the field of using technology and aims to regulate it and control wrong actions that may be committed through the systems of information, for example, but not limited to:

First: **Jordanian Penal Code No. 16 of 1960 and its amendments until 2021 AD:** The Crimes and Penalties Law has been amended to include articles related to cybercrimes and legal challenges arising from the development of technology and the use of the Internet. New amendments and sections have been added to punish illegal online activities and protect data and privacy. Article No. (401) stipulates the "criminalization of crimes related to data and information manipulation." Article No. (404) of the Jordanian Penal Code stipulates "amendments to the Jordanian Criminal Law that regulate electronic fraud and the use of information technology in committing crimes."

Second: The Information Technology Crimes Law of 2010 and its amendments: This law defines crimes related to information technology and regulates them in detail.

From the above, the researcher believes these provisions form a legal framework for combating cybercrimes in Jordan, defining the related crimes and their corresponding penalties.

The concept of cybercrimes and their types from the perspective of the Jordanian Cybercrime Law

In Jordanian law, cybercrimes are considered different from traditional crimes and are regulated by the Information Technology Crimes Law No. 30 of 2010 and its amendments.

First: The concept of cybercrimes in Jordanian law: In Jordanian law, cybercrimes include various illegal activities carried out using digital technology or electronic networks. These crimes are generally defined as activities committed online or related to computers and information systems in illegal ways and often include violating the rights of others or exploiting technology for illegal purposes. (Electronic Crimes Law No. (17) of 2023) and others defined it as an illegal act punishable by law. Crimes are defined as acts that violate laws and harm individuals or society in general. Penalties and legal procedures are used to deter and punish perpetrators of crimes. (Najm, 2014: 12-15).

Second: Types of Cybercrimes in Jordanian law: The Jordanian legislator has relied on defining some types of these cybercrimes in Jordanian law based on the Arab Convention on Combat Information Technology Crimes

(Arab Convention on Combat Information Technology Crimes, 2010) as follows:

- Cyber intrusion.
- Electronic fraud.
- Violation of privacy rights and cyber espionage.
- Online defamation and abuse.
- Market manipulation and commercial fraud.
- Violation of intellectual property rights online.
- Cyber extremism and terrorism.

Freedom of opinion in Jordanian laws and the digital age (Cybercrimes)

Freedom of opinion is considered one of the fundamental rights in many constitutions and international charters, encompassing the right to express opinions and ideas without unlawful interference or censorship from the state or other parties. (UN Document 2000/23).

Therefore, freedom of opinion is defined as a fundamental right that grants individuals the ability to express their views and ideas freely, without interference or restrictions from government authorities or other entities. This right includes the ability to express opinions through various means, whether by writing, speaking, or the arts. In the digital age, expression extends to social media and the Internet. (Al-Hadidi, 2017).

Freedom of opinion from the perspective of Jordanian laws

In laws related to human rights, there are restrictions on exercising this right according to public security interests and the rights of others. These restrictions are outlined in the following laws:

First: Freedom of opinion in the Jordanian Constitution

- Article No. (7), Clause No. (1) the Jordanian Constitution 1952 and its amendments until 2022 stipulated that "personal freedom is protected." Paragraph 2 of this article states that "any violation of public rights and freedoms or the sanctity of the private life of Jordanians is a crime punishable by law."
- Article 15 of the Jordanian Constitution of 1952, as amended up to 2022, stipulates that "the state guarantees freedom of opinion, and every Jordanian has the right to express their opinion freely through speech, writing, photography, and other means of expression, provided that it does not exceed the limits of the law."

Second: Freedom of opinion in the Political Parties Law

Freedom of opinion and expression is essential in:

- Strengthening democracy.
- Strengthening social interaction.
- Monitoring the government.
- Strengthening cultural and intellectual diversity.

Third: Freedom of opinion in relevant laws

In Jordan, there are laws that regulate the practice of freedom of opinion and expression, including the Press, Publication and Media Laws, the Press Criticism Law, and the Publication, Printing and Publishing Law (Press and Publication Law No. (4) of 2015):

- Responsibility and limits.
- Regulatory issues.
- Contemporary challenges.

Freedom of opinion in the digital age

Freedom of opinion is a fundamental right that allows individuals to express their opinions and ideas freely without interference or restrictions from government authorities or other parties. This right includes the ability to express opinions through various means, including writing, speaking, and the arts. In the digital age, this freedom has become a significant challenge due to technological advancements and the presence of the Internet. It is even more important due to the impact of the Internet and social media on individuals' ability to express their opinions and access diverse information. (Al-Hasban, 2011: 333-344).

From the above, it becomes clear to the researcher that it is important to exercise freedom of opinion and expression in a manner that respects local laws and preserves public safety and the rights of others. Legal authorities in Jordan are working to follow up on developments, update laws to address new challenges, and ensure that laws are implemented fairly. Thus, individuals and media can utilize laws and legislation to protect their rights and ensure they enjoy freedom of opinion in the digital age.

Individual rights in the digital and legal age

In the digital and legal age, individual rights remain crucial and essential to ensure the protection of individuals and the promotion of justice and fundamental freedoms.

The concept of individual rights in the digital age from the perspective of international legislation and legal frameworks for cybercrime laws.

The concept of individual rights in the digital age is influenced by a range of international legislations and legal frameworks that regulate online activities and protect individual rights. Article 19 of the Universal Declaration of Human Rights (1948) states that "the right to freedom of expression includes the freedom to seek, receive, and impart information and ideas through any media and regardless of frontiers." The following is a look at this concept from the perspective of international legislation and legal frameworks for cybercrime laws:

- Right to freedom of opinion and expression.
- Right to digital privacy.

- Right to access information.
- Right to protection from digital discrimination.
- Right to protect children online.
- Right to protect digital rights.
- Right to cybersecurity.
- Right to digital education and participation.
- Right to legal immunity.

From the above, it becomes clear to the researcher that these rights reflect the importance of protecting individual rights in the digital and legal age. These points show the importance and necessity of having strong international legislation and legal frameworks to protect individual rights in the digital age. These laws seek to balance individuals' protection and fundamental rights with the fair regulation of online activities, which are essential to achieving justice and democracy in modern societies.

The concept of individual rights in the digital age from the perspective of Jordanian law

First: Jordanian Political Parties Law No. (7) of 2022:

1. Freedom of political engagement and expression.
2. Electronic participation.
3. Protection of privacy and data.

Second: Jordanian Elections Law No. (4) of 2021:

1. The right to vote and political participation.
2. Access to political information.
3. Protection of digital electoral processes.

From the above, the researcher believes that these laws and regulatory legislation require clear guarantees of individual rights in the digital age. This contributes to creating a democratic and fair political environment that allows individuals to participate effectively and responsibly in political processes and elections, whether traditional or digital.

The conflict between freedom of opinion and the Cybercrime Law on regulating social media sites in the Jordanian legal context.

The Jordanian Cybercrime Law aims to combat online crimes such as incitement to hatred, defamation, electronic fraud, cybercrimes, etc. Thus, this law provides the government with tools to monitor and hold accountable individuals who violate the law online. The resulting conflict between freedom of opinion and cybercrime law in regulating social media within the Jordanian legal context is a complex issue that requires a balance between individual rights and societal and national security interests. This conflict can be discussed through the following points:

1. Freedom of opinion: Freedom of opinion is a fundamental right guaranteed by the Jordanian Constitution, as stipulated in Article 15, Paragraph 1 of the 1952 Constitution, as amended up to 2022, and by international human rights treaties.

2. Balancing rights and responsibilities: The main challenge lies in finding the right balance between individual rights and societal responsibilities.

3. International Court of Justice: The International Court of Justice can consider challenges to the implementation of national laws and make recommendations on how to regulate social media sites according to international human rights treaties.

4. Awareness and training: The government should promote awareness and training on safe online behavior and responsible use of social media sites.

5. Advanced legislation: Laws should be developed and updated to address new challenges in the digital age, such as combating incitement to hatred and online extremism.

Freedom of opinion and the Cybercrime law on regulating social media sites

Cybercrimes and freedom of opinion are two important topics in Jordanian laws, and Jordanian laws deal with these two concepts in different ways. Therefore, regulating and restricting social media through laws and legislation presents a significant challenge concerning freedom of opinion and expression. On one hand, freedom of opinion and expression is considered a fundamental right in many constitutions and international charters. The Internet and social media are regarded as one of the main means of expression in the modern era. On the other hand, cybercrimes and online violations present security and legal challenges that require the intervention of authorities to protect society and individuals. (Al-Badayneh, 2014) through several aspects:

1. The balance between freedom and security.
2. Defining cybercrimes.
3. Legal procedures and oversight.
4. Transparency and accountability.
5. Public awareness and education.

From the above, it becomes clear to the researcher the importance of achieving a balance between freedom and security in the digital age and how laws can be developed to achieve this balance. It is important that these laws are based on human rights standards and cybersecurity to ensure the protection of individuals and society.

Examples of countries that have successfully developed effective legislation for cybercrime laws and protecting individual rights

Several countries have successfully developed effective legislation for cybercrime laws and protecting individual rights in the digital age. Here are some examples:

1. The United Kingdom.
2. Canada.
3. Germany.
4. Japan.

From the above, it becomes clear to the researcher that these examples demonstrate how countries can develop effective legislation to protect individual rights in the digital age and combat cybercrime. Success depends on striking a balance between cybersecurity, individual rights online, and effective law enforcement.

Evaluation of the Jordanian Cybercrime Law on regulating social media sites

Evaluation requires reviewing and analyzing the effectiveness of this law in dealing with current and future challenges and determining its suitability to new technological developments, methods of spreading cybercrimes, and content on social media platforms. This law includes many provisions that aim to regulate the use of social media and protect users. It can be evaluated through several aspects:

First: Definitions stipulated in the Jordanian Cybercrime Law No. (17) of 2023:

Article No. 2, which includes the definitions stipulated in:

- Data: "Everything that can be processed, stored, supplied or transferred using information technology and technology, including writing, images, numbers, videos, etc."
- Information: "Data that has been processed electronically and has become meaningful."
- Information Technology: "All forms of managing information systems that rely on computers, cell phones, software, programming commands, or any other electronic devices for transfer, storage, or any other means that achieve the same goal."
- Information System: "A set of programs, applications, social media platforms, devices, or tools designed to create, send, receive, or otherwise create data or information electronically."
- Authorization: "The permission granted by the concerned party to one or more individuals or to the public to access or use an information system."
- Programs: "A set of technical commands and instructions designed to accomplish a task that can be executed using information systems or any means of information technology."
- Traffic Data Flow: "Any data movement related to communication through an information system or any means of information technology that arises from it and forms part of a sequence."
- Information Network: "A connection between more than one information system or any means of information technology to provide and access data and information."
- Website: "A space for making information available on the information network through a specific address."
- Social Media Platform: "Any electronic space that allows users to create an account, page, group, channel, or similar entity through which the user can post, send, or receive images or other content."
- IP Address: "A digital identifier assigned to each information technology device for communication purposes within an information network."
- Service Provider: "Any natural or legal person, public or private, who provides subscribers with electronic services through technology."
- Critical Infrastructure: "A set of electronic systems, networks, and physical and intangible assets, or cyber assets, whose continuous operation is essential to ensure the security of the state, its economy, or the safety of society."

Second: Crimes stipulated in the Jordanian Cybercrime Law No. (17) of 2023:

1. Cyber Hacking Crime:

By defining cyber hacking and applying this definition to the provisions of the Cybercrime Law, the following can be observed:

- Article 3, paragraphs (a, b, c) all state that "Anyone who intentionally accesses or reaches a website to alter, delete, destroy, modify its contents, occupy, encrypt, stop, disable it, impersonate its identity, or impersonate the owner" (Cybercrime Law No. 17 of 2023)
- Article 4, paragraphs (a) and (c), state that "Anyone who accesses or reaches, without authorization or in violation of or exceeding the authorization, the information network, information technology, information system, or any part thereof belonging to ministries, government departments, official public institutions, public institutions, security or financial or banking institutions, or companies owned or partially owned by any of these entities or critical infrastructure, and views data or information not available to the public that affects national security, the Kingdom's foreign relations, public safety, or the national economy"(Cybercrime Law No. 17 of 2023)

2. Electronic Fraud Crime:

By defining electronic fraud and applying this definition to the provisions of the Cybercrime Law, the following can be observed:

- Article 12 states, "Anyone who manipulates the IP address by using a fake address, an address belonging to another person, or by any other means with the intent to commit a crime or to prevent its detection" (Cybercrime Law No. 17 of 2023)

3. Crime of Privacy Violation and Electronic Espionage:

By defining the violation of privacy rights and electronic espionage and applying this definition to the provisions of the Cybercrime Law, the following can be observed:

- Article 5, paragraphs (a) and (b) state that "Anyone who creates an account, page, group, channel, or similar entity on social media platforms and falsely attributes it to a natural or legal person."
- Article No. 18, paragraphs (a, b) stipulate that "anyone who blackmails or threatens another person to compel him to do or refrain from doing an act or to obtain any benefit from that through the use of an information system, information network, website, social media platform or any means of information technology."

4. Crime of Defamation and Abuse via the Internet:

By defining defamation and online abuse and applying this definition to the provisions of the Cybercrime Law, the following can be observed:

- Article 11 states that "Anyone who possesses, without authorization, a device, software, or any prepared electronic data, a password, or access codes, or who provides, produces, distributes, imports, exports, or promotes them with the intent to commit any of the crimes specified in this law."
- Article 16 states, "Anyone who intentionally spreads, attributes, or falsely assigns actions to another person, or contributes to this through the information network, information technology, information system, website, or social media platforms, which could defame or assassinate their character."
- Article No. 21 states that "anyone who requests or accepts for himself or another a gift, promise, or any other benefit, whether this is done inside or outside the Kingdom, to publish or republish illegal content, using an information network, any electronic website, or social media platform" (Cybercrime Law No. 17 of 2023)

5. Crime of Market Manipulation and Commercial Fraud:

By defining market manipulation and commercial fraud and applying this definition to the provisions of the Cybercrime Law, the following can be observed:

- Article No. 8, Paragraph (A), Item No. (1) stipulates that "whoever intentionally and without authorization or in excess of authorization obtains, via the information network, information technology, or information system, data or information related to electronic payment methods or in the implementation of electronic financial or banking transactions, or uses or publishes any of this data."
- Article No. 9 stipulates that "anyone who commits any of the acts stipulated in Articles (3), (5), (6), (7) and (8) of this law if they occur on an information system, information technology, website or information network related to the transfer of funds, or the provision of payment, clearing or settlement services, or any of the banking services provided by banks and financial companies."

6. Crime of Intellectual Property Rights Violation Online:

By defining the violation of intellectual property rights online and applying this definition to the provisions of the Cybercrime Law, the following can be observed:

- Article 6 states that "Anyone who intentionally introduces, publishes, or uses a program or software command via the information network, information technology, or by using an information system to cancel, delete, add, destroy, disclose, damage, block, encrypt, modify, change, transfer, copy, capture, or enable others to access data or information, or to obstruct, disrupt, or halt the functioning of an information system, or to access it, or to change, cancel, damage, or modify the contents of a website, or occupy it without authorization, or in excess of or in violation of that authorization, or to impersonate its identity, or impersonate the owner."

7. Crime of Cyber Extremism and Terrorism:

By defining cyber extremism and terrorism and applying this definition to the provisions of the Cybercrime Law, the following can be observed:

- Article 13, paragraph (a), item (1), states that "Anyone who sends, publishes, prepares, produces, stores, processes, displays, prints, buys, sells, transfers, or promotes pornographic activities or materials using the information network, information technology, information system, or a website."

Third: Penalties for crimes under the Jordanian Cybercrime Law No. (17) of 2023:

1. Penalty for Cyber Hacking Crime:

Article 3, paragraph (a) stipulates a penalty of imprisonment for a period between one week and three months, or a fine not more than 600 dinars and not less than 300 dinars, or both penalties. Paragraph (b) establishes a penalty of imprisonment for three months to one year, accompanied by a fine ranging from 600 to 3,000 dinars. If the perpetrator successfully achieves the intended result, the penalty increases to imprisonment for one to three years and a fine between 3,000 and 15,000 dinars.

2. Penalty for Electronic Fraud:
Article 12 establishes a penalty of imprisonment for at least six months or a fine from 2,500 to 25,000 dinars.

3. Penalty for Privacy Violation and Electronic Espionage:
Article 5, paragraph (a), stipulates a penalty of imprisonment for a period not less than three months, or a fine not less than 1,500 dinars and not more than 15,000 dinars, or both penalties. Paragraph (b) stipulates a penalty of imprisonment for a period not less than six months, along with a fine of not less than 9,000 dinars and not more than 15,000 dinars. Paragraph (c) provides for a penalty of temporary hard labor and a fine of not less than 15,000 dinars and not more than 45,000 dinars.

4. Penalty for Defamation and Abuse Online:
- Article 11 stipulates a penalty of imprisonment for a period not less than three months, or a fine not less than 2,500 dinars and not more than 25,000 dinars, or both penalties.
- Article 15, paragraph (a) stipulates a penalty of imprisonment for a period not less than three months, or a fine not less than 5,000 dinars and not more than 20,000 dinars, or both penalties.

5. Penalty for Market Manipulation and Commercial Fraud:
- Article 8, paragraph (a), items (1), (2), and (3) impose a penalty of imprisonment ranging from one to three years, along with a fine between 2,500 and 10,000 dinars. Paragraph (b) establishes a penalty of imprisonment for two to three years, accompanied by a fine ranging from 5,000 to 15,000 dinars.
- Article 9 stipulates a penalty of temporary hard labor for a period not less than five years, along with a fine of not less than 25,000 dinars and not more than 75,000 dinars.

6. Penalty for Intellectual Property Rights Violation Online:
Article 7 specifies the following penalties: Paragraph (a) imposes a minimum imprisonment of six months and a fine ranging from 1,500 to 6,000 dinars. Paragraph (c) mandates a minimum imprisonment of one year and a fine between 3,000 and 6,000 dinars.

7. Penalty for Cyber Extremism and Terrorism:
Article 13, paragraph (a), item (1) establishes a penalty of imprisonment for a minimum of six months and a fine ranging from 3,000 to 6,000 dinars. Item (3) specifies a penalty of imprisonment for a minimum of one year and a fine ranging from 6,000 to 15,000 dinars. Paragraph (b), item (1) of this article specifies a minimum imprisonment term of one year, accompanied by a fine ranging from 6,000 to 30,000 dinars.

Fourth: The severity of penalties under the Jordanian Cybercrime Law:
Do the penalties stipulated in the law provide a sufficient deterrent to perpetrators of cybercrimes related to social communication?
- Article No. 27 stipulates that "anyone who intentionally participates in, intervenes in, or incites the commission of any of the crimes stipulated in this law shall be punished with the penalty specified therein for their perpetrators."
- Article No. 28 stipulates that "the penalties stipulated in this law shall be doubled in the following cases: (a) If the perpetrator commits his crime by exploiting his position, work, or powers granted to him. (b) If there are multiple victims. (c) If any of the crimes stipulated in this law are committed repeatedly. (d) If the perpetrator commits his crime in the interest of a foreign country or an illegal organization."
- Article No. 28 stipulates that "the penalties stipulated in this law shall be doubled in the following cases: (a) If the perpetrator committed his crime while exploiting his position, work, or powers granted to him. (b) If there are multiple victims. (c) If any of the crimes stipulated in this law are committed repeatedly. (d) If the perpetrator committed his crime in the interest of a foreign country or an illegal organization."

Fifth: Accountability and Investigation under the Jordanian Cybercrime Law:
Article 13, paragraph (a), item 1 states: "Prosecution for the crimes mentioned in item (1) of this paragraph shall be initiated based on a complaint by the victim who has reached the age of eighteen, and the public right lawsuit shall be dismissed if the victim pardons the offender." Item (3) states: "If the actions mentioned in item (1) of this paragraph are intended to direct or incite the commission of a crime, or are for the purpose of sexual exploitation, they shall be prosecuted without the need for a complaint, and the punishment shall be imposed."
- Article No. 29 stipulates that "the court may reduce the penalties stipulated in this law by half if the perpetrator provides information about any of the crimes stipulated in this law before referring it to the Public Prosecutor, and this would reveal the crime or its perpetrators or arrest them."

Sixth: Strengths and weaknesses of the Jordanian Cybercrime Law:
The strengths and weaknesses of the Jordanian Cybercrime Law can be summarized as follows:

Strengths
- The law has influenced the development of the Jordanian legal system to adapt to the new challenges posed by cybercrimes.

- The law sets strict penalties for offenders to discourage cybercrime practices and deter potential crimes.
- The law has encouraged institutions and individuals to invest in cybersecurity technology and innovation to prevent cyberattacks.
- The law has contributed to raising public awareness about the dangers of cybercrimes and how to prevent them.

Weaknesses

- The law does not provide a precise definition of cybercrimes, which has led to ambiguity in clarifying concepts and identifying illegal behaviors online.
- The law does not establish regulatory arrangements for electronic evidence and its use in proving crimes.

Evaluating the efficiency of current legal procedures in combating cybercrimes.

The Jordanian legislator has shown great interest in cybercrime and has taken it seriously, considering it like other crimes punishable by law in Jordan. It has punished and combated cybercrimes through the Cybercrime Combating Unit, which pursues perpetrators of cybercrimes and hands them over to the competent authorities. Moreover, the Hashemite Kingdom was one of the first Arab countries to enact laws on cybercrimes without leniency.

Therefore, the most important procedures for filing a complaint regarding cybercrimes can be summarized as follows:

- One should report to the nearest security center, which will forward the case to the Cybercrime Unit in the Criminal Investigation Department via an official letter.
- Submit a complaint of an electronic crime by going to the Public Prosecutor closest to the complainant's place of residence and submitting a summons for the case. He, in turn, transfers it to the Cybercrime Unit in the Criminal Investigation Department by means of an official letter. As stipulated in Article No. (3), Item (2) of the Jordanian Code of Criminal Procedure of 1961.
- If a cybercrime specified in the Cybercrime Law is committed using information systems within the Hashemite Kingdom of Jordan and causes harm to its interests, the interests of its residents, or has effects within the country, then a public right and personal right lawsuit shall be filed against the defendant before the Jordanian courts.
- Article 15, paragraph (b) of the Cybercrime Law No. (17) of 2023 states: "The crimes specified in paragraph (a) of this article shall be prosecuted by the public prosecution without the need to file a complaint or claim of personal right if they are directed at any state authority, official bodies, or public administrations."

Impact and Analysis of the Jordanian Cybercrime Law:

The Cybercrime Law in Jordan has influenced the creation of a safer online environment and enhanced trust in the use of the Internet and information technology. However, successfully implementing the law requires sustained cooperation between security and judicial agencies, the private sector, and civil society to combat cybercrimes effectively and safeguard individual rights in the digital age.

The impact of the Jordanian Cybercrime Law on restricting freedom of opinion and regulating social media sites.

Through the Internet, a new kind of social connection has been made possible by the vast developments in communication technology and the quick adoption of this technology in the modern period. As a result, new behaviors have emerged that call for regulation to safeguard persons and the public interest, as well as to give Internet users and other information systems the protection they need. It is now necessary to have legislation that keeps up with these advancements. As a result, the Cybercrime Law No. 27 of 2015 was passed, broadening the definition of cybercrimes to reflect current trends and advancements.

In 2022, the Jordanian government proposed a draft modification to the Cybercrime Law, which is a repeal of the prior law consisting of 17 articles, while the new law involves 41 articles to become more comprehensive and expansive than the previous law in terms of the type of cybercrimes. This affects freedom of opinion and expression, which the Jordanian Constitution guarantees in Article 15/1, which states: "The State guarantees freedom of opinion, and every Jordanian has the right to express his opinion in speech, writing, photography freely, and all other means of expression, provided that he does not exceed the limits of the law."

Impact of the law on restricting freedom of opinion in regulating social media sites.

The Cybercrime Law has significantly impacted and protected individuals' rights in the digital environment. This law directly threatens digital rights, including freedom of opinion and the right to information. It will not ultimately achieve the Jordanian government's stated goals of combating "fake news," "hate," and "defamation" on the Internet. This leads to the deterioration of electronic environment spaces and restricting freedom of opinion, whether in civil, political, economic, or judicial issues, effective for members of society, especially young men and women, at all levels. (Al-Majali, 2010: 39-40).

Examples of legislation and decisions that impacted the restriction of freedom of opinion on regulating social media sites.

These are general examples of legislation and decisions that enable governments to monitor and restrict freedom of opinion on social media platforms. These laws and decisions must be carefully evaluated to ensure a balance between cybersecurity, individual rights, and freedom of expression, which have impacted freedom of speech by regulating social media platforms in some Arab countries and around the world (Al-Taie, 2013: 14-22).

- **Laws known as "anti-cybercrime laws" in many countries:** These laws include legislation that prohibits the publication or distribution of information via social media if it exposes the authority or regime to criticism. (Council of Europe, European Treaty Series, No. 185, Convention on Cybercrime, Budapest, 2001).
- **Anti-hate laws on the Internet:** In some countries, restrictive legislation is being passed that prevents the publication of content that contains hatred or incitement to violence on social media platforms.
- **Encryption ban legislation:** Some countries restrict the use of encryption technologies through legislation that limits privacy and individuals' ability to express themselves freely.
- Ban on information and news distribution on social media during election periods: In some countries, restrictions are imposed on the distribution of information and news on social media platforms during election periods to monitor content.
- **Temporary bans on websites and applications:** In emergency situations, governments may issue decisions to temporarily block access to social media websites and applications to prevent the organization of protests or the spread of specific information.
- I**SP monitoring legislation:** In some countries, ISPs are required to cooperate with authorities to monitor and track users' activity on social media platforms.
- **Anti-cybercrime legislation:** Many countries have laws in place to combat cybercrime, but these laws can sometimes be used to restrict freedom of expression.

Analysis of the impact of the Jordanian Cybercrime Law on restricting freedom of opinion on regulating social media sites.

Cybercrimes can occur at any time and within any organization. No institution, whether private, governmental, or even law enforcement and security agencies, is immune to the effects of cybercrimes. Ultimately, the responsibility for combating it lies with the state, especially with the security services (in 2015, the Public Security Directorate established a specialized unit called the Cybercrime Unit). Therefore, the state needs to take steps to combat cybercrimes, including protecting security and ensuring freedom of opinion online, so that they are treated as complementary goals. (Al-Taie, 2013: 31-41).

Analyze the impact of the Cybercrime Law on restricting the individual's rights to privacy and personal freedom.

Social media is full of many activities, the widespread use of smartphones and tablets, in addition to the ease of access to the Internet and the desire of young people to know and their sense of curiosity on many occasions, which can result in cybercrimes and many harms and risks. This can extend to harm individuals' rights and personal freedoms, as stated in Article 15, Paragraph (b) of the Cybercrime Law No. 17 of 2023, which defines "false news" as those that affect societal peace and national security, making them subject to punishment. In addition, what is stipulated in Article 16 of the same law defines "character assassination" morally. Prosecution for these crimes does not require filing a complaint if it is directed to state authorities, official bodies, or a public employee while performing his job.

When analyzing the impact of the Cybercrime Law on restricting individual rights to privacy and personal freedom, it becomes evident that there are significant positive and negative effects.

Positive effects: Among the most important are:

- The law focuses on regulating and punishing harmful online activities such as cyber hacking and online fraud.
- The aim of the law is to combat cybercrimes and punish offenders to deter such activities and enhance cybersecurity.
- The law may allow for the collection and analysis of electronic data for the purposes of investigation and accountability.
- Data protection laws focus on ensuring the protection of individual privacy and personal data.
- The purpose of the law is to regulate how personal data is collected and processed, allowing individuals to have control over their personal information.
- The law imposes strict requirements on data collection organizations and imposes heavy fines for non-compliance.
- Regarding individual rights, there must be a balance between the need to combat cybercrimes and ensuring that cybercrime laws protect individual privacy.
- Data protection laws are designed to provide strong protection for personal privacy and impose strict standards on data collection and processing.

Negative repercussions:

- The law restricts and criminalizes individual activities, which may stifle criticism and undermine public accountability.
- Violations of the freedoms and rights guaranteed by the Jordanian Constitution of 1952 and its amendments up to 2022. Articles (12, 15, 17, 20) in particular are questionable as they use vague phrases with unclear intent and purpose. All of this raises questions about the underlying truth of these articles and the objectives that the government does not seem eager to disclose.
- It will impose silence on the rights of the individual and human rights activists in Jordan, indicating that an individual's "human error" in inaccurate information may cost him his professional life due to the large financial penalties, some of which are multiplied by 50 times.

Analysis of cases from Jordan demonstrating the law's impact on restricting freedom of opinion and regulating social media sites.

Among the broad and ambiguous cybercrimes in the legislation are "incitement to immorality or enticing another person or violating public morals," "character assassination," "stirring up sedition and sectarianism or undermining national unity," and "disrespecting religions." Article 16 of Cybercrime Law No. 17 of 2023 states that these provisions target online expression content. They do not comply with the legality, legitimate purpose, necessity, and proportionality requirements for limitations on the right to freedom of speech set down in international human rights law because they are ambiguous and susceptible to various interpretations. The legislation penalizes infractions severely. As Jordan's civic space is smaller and activist intimidation, harassment, and arrests are rising, worries about the law are mounting. Human rights advocates and journalists have been detained on the grounds of alleged "defamation." One such instance involves the satirical journalist Ahmad Hassan Al-Zoubi, who was given a one-year prison sentence on August 9th under the current legislation for sharing a Facebook update in December that expressed disapproval of handling a truck drivers' strike by the authorities.

RESULTS

This research has reached several conclusions based on the explanation and clarification of the Jordanian Cybercrime Law. The main findings can be summarized as follows:

- This research confirmed that the Jordanian Cybercrime Law was not guided by the discussion papers presented by His Majesty the King in the past years, which urged the importance of engaging in political life and adopting "active citizenship." The digital space is considered part of the tools for this participation.
- This research highlighted that laws and legal frameworks should guarantee the protection of these rights and enhance the balance between protecting cyber security and freedom of opinion and expression.
- This research showed that the ultimate goal of the law is to preserve freedom of opinion, ensure cyber security, and balance rights and responsibilities between individual rights and the public interest.
- This research highlighted that the Jordanian Cybercrimes Law focused on the penal and punitive dimensions and did not include any institutional and preventive measures to limit negative phenomena in the digital environment.
- This research highlighted that the Jordanian Cybercrime Law had used broad, vaguely defined, imprecise, ambiguous, and unspecified terms, such as "fake news". Nevertheless, these writings fall short of what is required by international law in terms of being precisely worded enough to enable people to govern their behavior in accordance with them.
- This research showed that the Jordanian Cybercrimes Law permitted the filing of a public rights lawsuit directly by the Public Prosecution, and it would have been more proper to let the complainant start the public rights case.
- This research showed that the Jordanian Cybercrime Law did not include any standards related to permissible public criticism.
- This research reveals that the Jordanian Cybercrime Law does not include a specific definition or clarification of a "public figure."
- This research showed that the Jordanian Cybercrimes Law did not include a clear legislative regulation regarding hate speech, its call, and incitement in a clear manner, and the draft law does not define the concept of hate or the criteria upon which it is based.
- This research reveals that the Jordanian Cybercrime Law does not include provisions that could impact investment in the digital environment in Jordan and its overall economy.
- This research showed that the Jordanian Cybercrimes Law violates the draft law's general rules in criminal theory in terms of criminal complicity and attempted crime.
- This research showed that the Jordanian Cybercrime Law hinders freedom of expression and access to information and increases censorship of the Internet, which limits the spaces for civil participation of citizens.
- This research has shown that a major challenge in implementing the Jordanian Cybercrime Law lies in balancing these two approaches: societies need cybersecurity and combating cybercrime,

but they also need to protect individual rights and privacy.

- This research showed that the Jordanian Cybercrime Law does not include corrective, cancellation, or publication ban measures as preventive institutional measures that must be followed before punishing.
- This research showed that the Jordanian Cybercrime Law is not compatible with international human rights standards, especially the right to freedom of opinion and expression.
- This research revealed that the Jordanian Cybercrimes Law does not consider the non-custodial societal penalties stipulated in the Penal Code.
- This research clarifies that the Jordanian Cybercrime Law tends towards increasing penalties and does not follow a legislative plan to impose or lift penalties gradually.
- This research clarifies that freedom of opinion and expression should be exercised in a manner that respects local laws while maintaining public safety and the rights of others. Thus, Jordanian legal authorities should work diligently to monitor developments, update laws to address new challenges, and ensure the fair implementation of these laws. Also, to enable individuals and media to benefit from laws and regulations to protect their rights and ensure their freedom of expression in the digital age (Internet).

RECOMMENDATIONS

Based on the above results, this research provides several recommendations as follows:

The researcher believes that the Jordanian legislator must reconsider amending the unfair legal texts to internet users to implement balanced laws that align with fundamental rights. These rights include the right to privacy, the right to exchange information, and the right to express opinions and ideas, which the Jordanian Constitution guarantees in Article (7). This article states, "Any violation of public rights and freedoms or the sanctity of the private life of Jordanians is a crime punishable by law." Also, Article (15) states: "The state guarantees freedom of opinion, and every Jordanian has the right to freely express their opinion through speech, writing, photography, and other means of expression, provided that they do not exceed the limits set by law." Additionally, these rights are guaranteed under international law and human rights treaties. The index of Internet freedom in Jordan may decline as a result of the enactment of these arbitrary provisions.

- The strategy to combat cybercrimes should be based on international human rights law and be clear and focused on addressing core cybercrimes while avoiding the definition of crimes based on online expression content.
- The researcher believes Jordanian legislators should reconsider this law to ensure compliance with international human rights law, including the International Covenant on Civil and Political Rights, to which Jordan is a party.
- The researcher suggests that Jordanian legislators should draw on available expertise, including input from IT specialists, legal experts, relevant civil society organizations, and the United Nations Human Rights Office, to develop legislation that addresses legitimate cyber threats while protecting fundamental human rights.
- The researcher believes that Jordanian legislators should implement awareness and education programs, with the government increasing public awareness of the risks of cybercrimes and the importance of safe online behavior.
- The researcher believes that the Jordanian legislator must ensure transparency, such that the authorities must ensure the transparency of the procedures and legal measures related to regulating social media sites and restricting freedom of opinion.

REFERENCES

- Arab Convention on Combating Information Technology Crimes, General Secretariat of the League of Arab States, Legal Affairs Department, Arab Legal Network, 2010.
- Universal Declaration of Human Rights (1948) states: "The right to freedom of expression includes the freedom to seek, receive, and impart information and ideas through any media and regardless of frontiers."
- Al-Badayneh, Diab Musa (2014). Cybercrimes: Concept and Causes. Scientific Symposium on Emerging Crimes in the Context of Regional and International Changes and Transformations, September 2-4, 2014, Center for Strategic Studies, Amman, Jordan.
- Al-Hadidi, Said Mahmoud (2017). Challenges in the Legal Regulation of Internet Communication: A Comparative Study. Paper presented at the Conference on Law and Media, Faculty of Law, Tanta University, April 23-24, 2017.
- Al-Hasban, Eid Ahmad (2011). The Reality of Freedom of Opinion and Expression in Light of Contemporary Technological Developments. Journal of Law, Kuwait University, Issue (1), Year (35), March 2011, pp. 333-365.
- Jordanian Constitution of 1952 and its amendments until 2022, pursuant to the amendment published in the Official Gazette No. 5770 dated 1/31/2022 AD
- Al-Taie, Jaafar Hassan Jasem (2013). Information Technology Crimes: A New Perspective on Cybercrime. Dar Al-Bidaya, Amman, Jordan.
- Jordanian Code of Criminal Procedure of 1961 issued in Official Gazette No. 1539 dated

03/16/1961 on page 311, Status of the law: Valid and amended until 2021

- Jordanian Political Parties Law No. 7 of 2022, published in the Official Gazette, Issue No. 5784, dated April 14, 2022.
- Cybercrime Law No. 17 of 2023, published in the Official Gazette, Issue No. 5874, on page 3579, dated August 13, 2023.
- Jordanian Penal Code No. 16 of 1960 and Amendments up to 2021.
- Press and Publication Law No. 4 of 2015, published in the Official Gazette, Issue No. 5329, dated March 1, 2015.
- Al-Majali, Nizam Tawfiq (2010). Commentary on the Penal Code: General Part. Dar Al-Thaqafa for Publishing and Distribution, 3rd Edition, Amman, Jordan, pp. 37-40.
- Council of Europe, European Treaty Series No. 185, Convention on Cybercrime, Budapest, 2001.
- United Nations Office on Drugs and Crime (2013). Comprehensive Study on Cybercrime. United Nations.
- Najm, Muhammad Sobhi (2014). Penal Code – General Part: General Theory of Crime. Dar Al-Thaqafa for Publishing and Distribution, Amman, Jordan.
- United Nations Document E/2000/23, Resolution 38/2000, The Right to Freedom of Opinion and Expression, Human Rights Committee, Fifty-sixth Session, April 20, 2000.