Dirasat: Human and Social Sciences, Volume 53, No. 12, 2026, 11875

Deanship of Scientific Research

The Adequacy of the Jordanian Cybercrime Law No. (17) of 2023 in protecting personal data

***Ashraf Fatehi Al-Rai*[1], *Amal Yousef Alrfoua*[2], *Sabah Mousa Almomani*[3], *Wasfi Mahmoud Masoud Al-Khraisat*[2], *Dina Imad*[1], *Duha Sulaiman Nazzal*[2], *Dujanna Abdel kafi Mohd Naji Helali*[4], *Ghenaa Musaed Mohammed Almatri*[4]**

[1] Public Law Department, College of Law, Abu Dhabi University, United Arab Emirates.
[2] Public Law Department, Faculty of Law, Al-Ahliyya Amman University, Jordan.
[3] Faculty of Law, Al-balqaa Applied University, Jordan.
[4] Independent researcher

Received: 21/5/2025
Revised: 17/6/2025
Accepted: 16/7/2025
Published online: 1/9/2026

* *Corresponding author:*
ashrafraie@gmail.com

Citation: Al-Rai, A. F., Alrfoua, A. Y., Almomani, S. M., Al-Khraisat, W. M. M., Imad, D., Nazzal, D. S. ., Helali, D. A. kafi M. N., & Almatri, G. M. M. (2026). The Adequacy of the Jordanian Cybercrime Law No. (17) of 2023 in protecting personal data. *Dirasat: Human and Social Sciences*, *53*(12), 11875.
https://doi.org/10.35516/Hum.2026.11875

© 2026 DSR Publishers/ The University of Jordan.

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY-NC) license https://creativecommons.org/licenses/by-nc/4.0/

Abstract

Objectives: This study aims to assess the adequacy of Jordanian Cybercrime Law No. (17) of 2023 in protecting personal data. It examines the relevant legal provisions, evaluates their effectiveness, identifies legislative gaps, and proposes amendments to enhance legal protection of digital privacy amid rapid technological advancements.
Methodology: The study adopts a descriptive approach to analyze legal texts related to the Jordanian Cybercrime Law, with particular attention to the protection of data and privacy on digital platforms, social media, and modern communication tools. Additionally, a qualitative analytical approach is employed to examine constitutional provisions and the Cybercrime Law in order to identify legal strengths and weaknesses. The study also proposes legislative amendments that would improve criminal protection for digital privacy.
Findings: The study reveals that the Jordanian Cybercrime Law does not sufficiently keep pace with evolving digital realities, particularly concerning personal data protection. It lacks clear definitions of key concepts such as data breaches and privacy violations, and fails to explicitly criminalize the breach of private life via technological means. Furthermore, Article 9 of the law contains legal ambiguities that could hinder enforcement and judicial interpretation.
Conclusion: The study recommends amending several legal provisions, especially Article 9, to address its legislative deficiencies. It also calls for the inclusion of a clear legal definition of data breach crimes and a specific provision safeguarding the sanctity of private life, in accordance with the Jordanian Constitution and international legal standards.
Keywords: Constitutional protection, criminal protection, personal data, digital platforms, media, Jordanian legislation.

مدى كفاية قانون الجرائم الإلكترونية الأردني رقم (17) لسنة 2023 في حماية البيانات الشخصية

***أشرف فتحي الراعي*[1]، صباح موسى المومني[2]، أمل يوسف الرفوع[2]، وصفي محمود مسعود الخريسات[2]، دينا عماد[1]، ضحى سليمان نزال[2]، دجانة عبد الكافي محمد ناجي هلال[3]، غناء مسعد محمد الماطري[4]**

[1] قسم القانون العام، كلية القانون، قسم القانون العام، جامعة أبوظبي، أبوظبي، الإمارات العربية المتحدة.
[2] قسم القانون العام، كلية الحقوق، جامعة البلقاء التطبيقية، البلقاء، الأردن.
[3] عمان، الأردن.
[4] دبي، الإمارات العربية المتحدة.

ملخّص

الأهداف: هدفت الدراسة إلى تحليل مدى كفاية قانون الجرائم الإلكترونية الأردني رقم (17) لسنة 2023 في حماية البيانات الخاصة عبر دراسة النصوص القانونية ذات الصلة، وتقييم مدى فعاليتها، وبيان أوجه القصور التشريعي، واقتراح تعديلات تعزز الحماية القانونية للخصوصية الرقمية في ظل التطورات التقنية المتسارعة.

المنهجية: اعتمدت الدراسة المنهج الوصفي عبر دراسة النصوص القانونية المتعلقة بقانون الجرائم الإلكترونية الأردني، وتحقيق الحماية للبيانات وخصوصيتها لا سيما تلك التي تستخدم من خلال المنصات الرقمية ومواقع التواصل الاجتماعي ووسائل الإعلام الحديث، فضلاً عن منهج التحليل النوعي عبر دراسة النصوص الدستورية ونصوص قانون الجرائم الإلكترونية وتحديد نقاط القوة، والثغرات التشريعية، واقتراح التعديلات التي تسهم في تعزيز الحماية الجنائية.

النتائج: توصلت الدراسة إلى عدة نتائج أهمها أن قانون الجرائم الإلكترونية الأردني لم يواكب بالشكل الكافي التطورات الرقمية في مجال حماية البيانات الخاصة، ولم يحدد بدقة مفاهيم خرق البيانات أو الاعتداء على الخصوصية، كما لم ينص على جريمة خرق حرمة الحياة الخاصة عبر الوسائل التقنية بصورة محددة، فضلاً عن وجود لبس تشريعي في نص المادة 9 من القانون.

الخلاصة: أوصت الدراسة بضرورة تعديل عدد من النصوص في القانون، لا سيما المادة (9) التي تعاني من خلل تشريعي، واقتراح نص قانوني يُعرف جرائم خرق البيانات بشكل دقيق، بالإضافة إلى النص الصريح على حماية حرمة الحياة الخاصة، بما ينسجم مع أحكام الدستور الأردني والمعايير الدولية في هذا المجال.

الكلمات الدالة: الحماية الدستورية، الحماية الجنائية، البيانات الخاصة، المنصات الرقمية، وسائل الإعلام، التشريع الأردني

Introduction:

It is a well-established legal principle that the mere storage of information does not imply a transition from privacy to publicity. Similarly, consent to the collection and storage of information and data does not equate to a license for its unrestricted dissemination.

Crimes involving the disclosure of private data and information can be defined as "unlawful acts that involve revealing personal or sensitive information without the consent of its owner, thereby violating the privacy of individuals or organizations and causing financial or moral harm to them." These crimes may also involve breaches of data or unauthorized access to digital platforms that contain such information or exceeding the scope of authorized access *(Al-Rai, 2024)*.

Upon reviewing the provisions of the Jordanian Cybercrime Law No. 17 of 2023, we find that it criminalizes numerous acts involving the disclosure of data or information whether financial, personal, medical, familial, or otherwise through unauthorized access to information systems or by remaining within such systems even if access was originally lawful but exceeded the granted authority *(Al-Atoum,M. 2020).*

This criminalization reflects the serious threat posed by unauthorized access to such systems, particularly given that they often contain highly sensitive and important data. Furthermore, this information is frequently accessible to individuals with expertise in cybercrime, who may exploit it for dissemination, especially with the widespread use of digital platforms and social media. These crimes may include data theft, cyber espionage, and the use of stolen data for illicit gain.

According to figures from the Jordanian Cybercrime Unit, 2,115 cases of cyber intrusion were recorded in 2022 *(SIGI-Jordan, Tamkeen Center for Support and Empowerment, 2022)*.

Additionally, the National Cybersecurity Center monitored 2,455 attempted breaches during the same year *(Al-Wakeel News, 2023).*

Such data or information may contribute to the commission of even more serious crimes beyond mere unauthorized access. The General Data Protection Regulation (GDPR) defines such incidents as “any operation or set of operations performed on personal data, including unauthorized disclosure, loss, or destruction” *(General Data Protection Regulation, GDPR)*.

The issue of safeguarding private data and protecting privacy has garnered considerable attention from international and regional organizations, all of which affirm the human right to data protection. This is reflected in the efforts of the United Nations, the Council of Europe, the Organization for Economic Co-operation and Development (OECD), and the European Common Market, which have signed numerous treaties affirming the confidentiality of data and the right to privacy.

National constitutions across the globe, including Jordan's, have enshrined the protection of private life. Jordanian Cybercrime Law No. 17 of 2023 includes multiple provisions to safeguard data and information, as previously discussed.

Although new communication technologies, particularly the Internet, have facilitated the fast and easy exchange of data and information, this does not justify exposing such data to intruders. This information holds great value for its owners, who trust the entities requesting access to it. Consequently, it is essential to protect and preserve this information, especially since the Internet does not offer absolute confidentiality or security for the data transmitted across it *(Al-Shawabkeh, 2011)*.

Regrettably, protecting private data remains a growing concern in the face of digital threats, and countries have not adopted a unified approach within their legal frameworks. However, there is a universal consensus on the necessity of protecting private life. Various countries have enacted specific legislation to safeguard privacy in the digital age including the United States, France, Canada, China, and Tunisia while others, such as Spain, Portugal, and Austria, enshrine these protections in their constitutions. Some even grant constitutional protection to personal data subjected to electronic processing.

Against this backdrop, this study seeks to examine in detail two main areas: the constitutional and criminal protection of private data on digital platforms and media under Jordanian legislation. It concludes with a set of findings and recommendations based on an in-depth analysis of the legal provisions and an assessment of their adequacy in addressing data breach crimes.

Research Problem:

The study investigates the adequacy of Jordan's Cybercrime Law No. 17 of 2023 in addressing crimes involving the breach of private data on digital platforms and modern media. This issue has become particularly salient given the rapid advancements in data collection and processing technologies, which pose legal challenges to the protection of personal data against unauthorized access or misuse. The study also notes that some legal provisions suffer from drafting inconsistencies, a matter that will be explored in detail.

The study aims to assess the comprehensiveness of these legal texts and their effectiveness in offering legal protection for private data. It also explores the extent to which these provisions align with constitutional protections of privacy under the Jordanian Constitution and highlights legal loopholes that may undermine efforts to combat data breach crimes.

Research Questions:

- What is the constitutional framework for protecting private data?
- What is the criminal legal framework for protecting private data?
- What are the elements of crimes involving data breaches under the Jordanian Cybercrime Law?
- What are the shortcomings of the Jordanian Cybercrime Law in addressing data breach crimes?

Significance of Study:

The importance of this study lies in the context of the rapid evolution of digital platforms and social media, which have made private data increasingly vulnerable to breaches and violations. As reliance on technology grows, so does the need to address gaps in Jordanian cybercrime legislation.

The study aims to analyze the adequacy of Jordan's Cybercrime Law No. 17 of 2023 in protecting private data, identifying its strengths and weaknesses. It also examines the legal challenges posed by digital developments and the extent to which the law addresses them. Furthermore, the study offers recommendations to improve the legislation in line with international standards and best practices for digital privacy protection, especially given the limited number of specialized studies on this vital subject.

Objectives of Study:

This study aims to analyze and evaluate the adequacy of Jordan's Cybercrime Law No. 17 of 2023 in protecting private data and to propose suitable amendments to enhance its effectiveness in combating data breach crimes on digital platforms. It also seeks to clarify relevant legal concepts and terminology to ensure legislative precision and to assess how the current law responds to modern digital challenges in personal data protection. Finally, it provides legal recommendations to improve the law's effectiveness, in keeping with technological developments and international legislation.

Methodology:

The study adopted a descriptive method by examining the legal texts related to the Cybercrime Law and the protection of data and privacy, particularly those used through digital platforms, social media, and modern media outlets. In addition, the study employed a qualitative analytical approach by analyzing constitutional texts and the provisions of the Cybercrime Law to assess the extent to which these crimes are addressed, identify strengths and legislative gaps, and propose appropriate amendments that contribute to enhancing protection across websites and modern media platforms.

Section One: The Constitutional Regulation of Private Data Protection in Jordan:

Many constitutions around the world emphasize the inviolability of private life. International covenants, agreements, and treaties also stress the prohibition of violating an individual's right to privacy and liberty, as this is a fundamental aspect of human dignity. This principle is clearly reflected in the Jordanian Constitution, like other constitutions such as the Egyptian, Lebanese, French, Algerian, and American constitutions, among others. Virtually all modern constitutions include provisions safeguarding this essential right.

The Jordanian Constitution explicitly guarantees the "right to privacy." Article 7(2) states: "Any infringement on public rights and freedoms or on the sanctity of private life of Jordanians shall be considered a crime punishable by law".

Furthermore, Article 10 affirms the inviolability of one's home. The constitution also protects physical integrity, prohibiting any unauthorized access to personal belongings, private images, bodily harm, photography, or information

concerning an individual's medical, personal, or psychological condition, whether during their lifetime or after death. Jordanian law criminalizes the violation of the sanctity of the deceased and bodily integrity *(University of Minnesota Human Rights Library, 2025*). It also prohibits the invasion of privacy through unauthorized access to an individual's physical or medical data *(El-Shahawi, 2005)*.

From birth, every person is entitled to physical privacy, meaning no one may search or touch their body unlawfully. Scholars have defined private space as the realm in which a person keeps the secrets of their life, expressing their individual will, distinguished by their image and physical features. Hence, beyond the physical protection of the body, moral protection also exists *(Aqli, 2012)*.

This includes personal medical and genetic information, which should not be accessed, especially with advancements in science and technology. Psychological conditions and confidential information also fall under this protection. In language, a "secret" is defined as something a person conceals within themselves and does not disclose *(Al-Waleidat, 2010)*.

In this section, we will examine, first, the constitutional protection of communications, correspondence, personal data, and information, including political, social, religious, and sectarian beliefs. Second, we will discuss the constitutional protection of credit, banking, and health data more broadly.

1- Constitutional Protection of Communications, Correspondence, Personal Information, and Data:

Communications, correspondence, and personal data enjoy constitutional and legal protection, whether such communications occur through traditional means such as postal letters, personal notes, or telephone calls or through modern technological methods such as mobile applications, which have evolved significantly in recent years *(Al-Qatatsheh, 2022)*.

This protection also extends to rules regarding the collection of personal and digital identity data or personal electronic accounts on digital platforms, including banking systems and others *(Saleh, 2016)*. These can be defined as "a set of facts, measurements, terms, numbers, or symbols processed by a computer" (Salem 2007). It includes information such as identification details, religious beliefs, marital status, medical and health records, financial accounts, and data about an individual's whereabouts from the moment it is collected, stored, and processed until it is deleted *(Cristina Blanton, 2021)*.

The researcher notes that evidence collection within domestic data transmission networks is relatively easier today, despite its challenges, compared to international networks where the internet is used by organized transnational criminal groups. This raises multiple constitutional and legal issues when data, information, or communications are obtained through such means.

The Jordanian Constitution underscores the importance of preserving this right in Article 18, which states: "All postal, telegraphic, and telephone communications and other forms of correspondence shall be considered confidential and shall not be subject to censorship, inspection, suspension, or confiscation except by judicial order and in accordance with the provisions of the law."

It is noteworthy that the 1952 Jordanian Constitution was progressive in this domain, as it established such protections well before the digital and technological revolutions, yet it remains relevant and applicable to this day.

Revealing personal beliefs whether social, sectarian, or religious is prohibited under comparative constitutional and legal systems. Many legal frameworks globally prohibit such intrusions, whether through traditional means like physical breaches (which are now rare) or through modern methods like media platforms, digital tools, or social media. This is due to the risks such actions pose to societal harmony, including inciting racial and sectarian hatred, stirring conflict, and fueling hate crimes *(Aawisheh S. Al-Hassan, T. Mansour, A. 2024)*.

2. Constitutional Protection of Credit and Banking Information and Data:

Credit data is considered among the most sensitive types of personal information, and no one should be allowed to access it particularly considering the massive technological revolution in banking operations on the one hand, and the global spread of organized crime on the other. Despite various jurisprudential attempts to define this complex concept, the Jordanian legislator has not yet provided a clear definition *(Al-Nawaisa, 2017)*.

Such data may be compromised through means such as credit card hacking, access to personal bank accounts, or electronic auctions through which an individual's credit information can be obtained, considered a violation of one's private

life. Privacy, as the researcher sees it, pertains to anything that reveals personal information about a victim's life.

These issues of privacy invasion are not limited to Arab countries but extend globally, even to technologically advanced nations like the United States. For instance, the Federal Trade Commission (FTC) filed 80 cases against companies that engaged in unfair or deceptive practices involving "inadequate protection" of consumer data. In 2020, the FTC continued to enforce its orders in data security cases to ensure consumer protection and corporate accountability *(Federal Trade Commission, 2020).*

Jordanian law includes several provisions protecting individuals' credit information, such as Article 8 of the Jordanian Credit Information Law and Articles 72, 73, and 75 of the Banking Law. There are also penal provisions in the Cybercrime Law, which will be addressed in detail later. These laws aim to prevent the misuse and publication of such data by both traditional and modern media outlets.

Due to the complex overlap within data protection in information systems and the various methods of obtaining such information, Arab legislation in general has fallen short in addressing these crimes. This is largely due to the rapid development of the internet environment. Some digital systems can access and use personal information under the terms of a privacy policy document that users typically agree without reading often because it is lengthy and incomprehensible *(Alhasan,TK. Awaisheh, SM.2024).*

Sometimes, the policy is even written in a foreign language *(Ayoub, 2009).* Employees who have access to this data may handle it in ways that violate legal rules set by the Cybercrime Law. Depending on the circumstances, this may also constitute a violation of personal privacy under the Penal Code.

The concept of unauthorized access remains a point of legal and scholarly debate. Although the idea is like a real-world scenario, like someone entering a restricted area without permission, it differs significantly due to nature and rapid evolution of the internet.

The tools used to infiltrate an unauthorized information system are advanced and fast. Unauthorized access implies that the system contains data, figures, and information, possibly sensitive or personal, which is the subject of this study. Such data can be used for blackmail, defamation, or other harmful purposes.

Regarding its legal nature, legislations differ in criminalizing unauthorized access to information systems. Some countries treat it as a material crime, others as a mere act with no punishment unless harmful consequences occur, and still others consider it a formal crime punishable simply by the act of access.

In a ruling by the Amman Magistrate Criminal Court, it was stated that:

"Unauthorized access to a computer information system is realized when someone accesses the data and information stored within the system without the consent of the relevant party. This means accessing the information system itself, not merely turning on the computer. Therefore, crime is established by gaining access to the computer's information system or the network "(Qistas Publications. 2019).

Section Two: Penal Protection of Personal Data in the Jordanian Cybercrime Law:

Article 3 of the Jordanian Cybercrime Law No. 17 of 2023 prohibits accessing the information network for the purpose of obtaining any data or information about individuals whether such data is personal or related to the victim's family, movements, or other aspects. This prohibition is particularly significant because today's information networks, particularly the internet, have become the primary repository for institutions and individuals to store their data.

The provision also imposes stricter penalties for actions such as deletion, addition, destruction, disclosure, publication or republication, damage, blocking, modification, alteration, transfer, copying of data or information, loss of confidentiality, encryption, suspension, or disabling of the information network. Thus, the law provides direct protection for the sanctity of private life, even though it does not explicitly state the phrase "sanctity of private life"; instead, it addresses the actions that constitute a violation of this protection *(Alrfoua, A.Y. R.alsweilmieen, S.M. Al-Zubi, J.Kh. Hatamleh, S.S.h. Al-Rafoo, A.Y. ALja'afreh, I.A..Alja'afreh ,B.I.A.(2024).*

Moreover, Article 4 imposes harsher penalties when the unauthorized access targets a government, security, or financial entity. Unauthorized access to an information system is defined as access by a person who is not authorized to view such

information or data but proceeds to access, view, store, delete, publish, or transfer it to others for dissemination. This scenario is plausible in modern digital platforms, where an offender may hack or access an information network or system to obtain data related to the victim if access occurs without the victim's consent. If the victim agrees to share the data or information, it cannot be considered unauthorized access.

Jordanian jurisprudence defined unauthorized access to electronic systems at the onset of the technological evolution in the current decade. A 2013 ruling by the West Amman Magistrate Criminal Court stated:

"As for the crime of unauthorized access and use of an information system attributed to the defendant, the court finds that this crime occurs when a person uses an information system with the intent to cancel, delete, add, destroy, disclose, damage, block, modify, alter, transfer, copy, move, capture, or enable others to access data or information; or to hinder, jam, suspend, or disable the system; or to access it, alter its website, delete it, damage it, modify its contents, overload it, impersonate it, or impersonate its owner without authorization or in excess or violation of such authorization" (Qistas Publications, 2013).

The rationale behind criminalizing intentional access to the information network lies in protecting the right to such data or information and preserving its confidentiality and privacy. This is based on the principle that everyone has the right to determine when, how, and where their data and information may be shared with others *(Rabee, 2016)*.

Many legislations have defined "unauthorized access" to an information network. Among them is the UK's Computer Misuse Act of 1990, which, under Section 17(2), considers unauthorized access to data or information to include the ability to transfer, copy, store, or use the data.

Similarly, Tennessee State Law (Section 39) in the United States describes access as:

"Any means of viewing, issuing instructions, communicating, storing data, or intercepting data from a computer system or computer network, or the information exchanged between computers, or access by a person authorized to use the computer whether electronically, audibly, mechanically, or otherwise" (Al-Nawaisa, 2017).

Despite the lack of an explicit definition of unauthorized access in Jordanian legislation and ongoing scholarly debate over whether the existence of passwords or security codes is required for an act to be deemed criminal, some legal scholars argue that a protective mechanism must be in place and breached for the act to be punishable. Others criticize this view, asserting that unauthorized access should not require the presence of security codes. We align with this latter opinion and propose that unauthorized access be defined as:

"Infiltration of a computerized information system, regardless of the presence or absence of security mechanisms, with the aim of obtaining information about others regardless of the nature of the data or information and whether it can be transferred, stored, deleted, used, or viewed".

The Jordanian Court of Cassation further ruled:

"We find that crimes committed through electronic means may involve physical acts occurring in one location while the outcome is realized in another. If the result is realized through the victim viewing the published content and since the complainant resides in Amman, Al-Rashid district, where she viewed the published content, and since the defendant was apprehended in Amman by the Cybercrime Unit then, assuming the crime is proven, it occurred in Amman, Al-Rashid district. Given that the case was registered at the North Amman Magistrate Criminal Court, the conditions for jurisdiction are satisfied, and this court is competent to hear the case" (Qararak Publications, 2024).

1. The Crime of Intentionally Accessing or Entering an Information System Without Authorization or in Excess of Authorization:

The material element of the crime of disclosing data or information through unauthorized access to an information network, information system, or website is represented by the act of disclosure of data or information obtained by a person who is either not authorized to access such data or is authorized but exceeds the scope or duration of that authorization.

Article 3 of the Jordanian Cybercrime Law No. 17 of 2023 stipulates:

(a) "Anyone who intentionally accesses or enters the information network, information system, information technology means, or any part thereof by any means without authorization or in violation or excess of the authorization shall be

punished with imprisonment for a period not less than one week and not exceeding three months, or with a fine not less than three hundred (300) dinars and not exceeding six hundred (600) dinars, or with both penalties".

(b) "If the access or entry referred to in paragraph (a) of this Article is for the purpose of deleting, adding, destroying, disclosing, publishing, republishing, damaging, blocking, modifying, altering, transferring, copying data or information, causing a loss of confidentiality, encryption, stopping or disabling the information network, an information system or any part thereof, the perpetrator shall be punished with imprisonment for a period not less than three months and not exceeding one year, and with a fine not less than six hundred (600) dinars and not exceeding three thousand (3000) dinars. The penalty shall be imprisonment for a period not less than one year and not exceeding three years and a fine not less than three thousand (3000) dinars and not exceeding fifteen thousand (15000) dinars if the intended result is achieved".

(c) "Anyone who intentionally accesses or enters a website to modify, delete, damage, alter its content, block, encrypt, stop or disable it, or impersonate its identity or the identity of its owner shall be punished with imprisonment for a period not less than three months and a fine not less than six hundred (600) dinars and not exceeding three thousand (3000) dinars".

Article 4 of the same law specifies the following penalties:

(a) "Anyone who accesses or enters the information network, information technology, information system, or any part thereof belonging to ministries, government departments, official public institutions, public institutions, security, financial or banking entities, or companies owned or partially owned by any of those entities or critical infrastructure, without authorization or in violation or excess of authorization, and reviews data or information not available to the public that affects national security, the foreign relations of the Kingdom, public safety, or the national economy, shall be punished with imprisonment for a period not less than six months and not exceeding three years and a fine not less than two thousand five hundred (2500) dinars and not exceeding twenty-five thousand (25000) dinars".

(b) "If the access referred to in paragraph (a) of this Article is for the purpose of deleting, damaging, destroying, modifying, altering, transferring, copying, publishing, republishing, compromising confidentiality, encrypting, deleting, adding, blocking, disclosing, or intercepting such data or information, the perpetrator shall be punished with temporary hard labor and a fine not less than five thousand (5000) dinars and not exceeding twenty-five thousand (25000) dinars. If the intended result is achieved, the penalty shall be temporary hard labor for not less than five years and a fine of twenty-five thousand (25000) dinars".

(c) "Anyone who intentionally accesses or enters a website belonging to ministries, government departments, official public institutions, public institutions, security, financial or banking entities, or companies owned or partially owned by any of those entities or critical infrastructure, with the intent of reviewing data or information not available to the public that affects national security, the foreign relations of the Kingdom, public safety, or the national economy, shall be punished with imprisonment for a period not less than four months and not exceeding three years and a fine not less than two thousand five hundred (2500) dinars and not exceeding twenty-five thousand (25000) dinars".

(d) "If the access referred to in paragraph (c) of this Article is for the purpose of deleting, damaging, destroying, modifying, altering, transferring, copying, deleting, adding, blocking, or encrypting such data or information, the perpetrator shall be punished with temporary hard labor and a fine not less than five thousand (5000) dinars and not exceeding twenty-five thousand (25000) dinars. If the intended result is achieved, the penalty shall be temporary hard labor for not less than five years and a fine of twenty-five thousand (25000) dinars".

(e) "Attempt to commit any of the offenses mentioned in this Article shall be punishable by the same penalty prescribed for the completed crime".

The penalty is doubled for anyone who commits these acts by abusing their job, position, or granted authority, or if there are multiple victims, repeated offenses, or if the crime is committed in the interest of a foreign state or an unlawful organization, as stipulated in Article 28 of the Jordanian Cybercrime Law.

In such cases, the court must apply the harsher penalty unless it decides otherwise, in accordance with Article 72 of the Penal Code, which states:

"1. If several felonies or misdemeanors are proven, a penalty shall be imposed for each crime, and only the harshest penalty shall be executed.

2. However, the court may combine the imposed penalties, provided that the total does not exceed 15 years in misdemeanors and 30 years in felonies".

3. The Moral Element of the Crime of Intentionally Accessing or Reaching an Information System Without Authorization or Beyond the Scope of Authorization:

This offense is considered an intentional crime, requiring the presence of general criminal intent, namely, the elements of knowledge and will. This means the offender must be aware that when they intentionally access or reach an information system to obtain information related to a particular individual, they are committing an act in violation of the law.

Furthermore, the will of the perpetrator must be directed toward committing this act. However, if the individual comes across this information by coincidence without intentionally accessing the information system, they are not considered to have committed the criminal act. In such cases, neither the element of knowledge nor will is present, as the person's will was not directed toward committing a criminal act, and they were unaware that their action was legally prohibited.

Most Arab legislations have adopted this position, considering such offenses as intentional crimes. Under Jordan's Cybercrime Law, intentional access with the purpose of violating data or information is considered an aggravating circumstance *(Al-Nawaisa, 2017).*

2- The Crime of Disclosing Data or Information through the Introduction, Publication, or Use of Electronic Programs:

Article 6 of the Jordanian Cybercrime Law states:

"Anyone who intentionally introduces, publishes, or uses a program or programming command through the internet, or via an information technology means, or by using an information system, to cancel, delete, add, destroy, disclose, damage, block, encrypt, modify, alter, transfer, copy, intercept, or enable others to access data or information, or to obstruct, disrupt, suspend, or disable the functioning or access to an information system, or to alter, cancel, destroy, or modify the content of a website, occupy it without authorization or beyond or in violation of authorization, or impersonate the site or its owner shall be punished by imprisonment for no less than six months and a fine no less than 2,500 dinars and not exceeding 10,000 dinars".

The legislator here provides criminal protection for cyberspace containing personal information or data. However, the law does not explicitly state protection for private life. Therefore, a breach of privacy occurs when the perpetrator publishes or uses a program via the internet or an information system to transfer, copy, intercept, or enable others to access data or information.

This implies that the legislator assumes the crime is established merely upon the act of transferring, copying, or intercepting data, which aligns with general provisions in the Penal Code, which consider merely accessing personal information a breach of privacy even if that information is not used.

After explaining the concept of the crime of disclosing data or information through the introduction, publication, or use of electronic programs, we will examine this crime in further detail in three subsections.

A. The Material Element of the Crime of Disclosing Data or Information via the Introduction, Publication, or Use of Electronic Programs:

The material element of this crime is realized when the perpetrator intentionally publishes or uses electronic programs with the intent to disclose data or information, or to enable others to access this data or information, whether it pertains to natural persons, companies, large institutions, individual institutions, social entities, organizations, associations, or public institutions.

Publication means distributing the program, data, or information in any manner via the information network or information system. Professor Dr. Abdel-Ilah Al-Nawaisah argues that "publication, use, and introduction should be carried out through the program" *(Al-Nawaisa, 2017).*

It is not necessary for the information to be of significant or dangerous importance, as it is sufficient for the information

to be simple personal data. Accessing such data constitutes a violation of privacy, infringing upon privacy protected by constitutional and legal texts. However, the difficulty arises here in that the perpetrator may remain hidden due to the use of certain technological systems that do not allow the identification of the perpetrator, the most notable of which are viruses, which can be defined as malicious technical systems containing executable programming instructions that typically spread by being attached to another executable document.

It is important to note the distinction between Articles 3, 4, and 6 of the Jordanian Cybercrime Law. Article 6 does not require entry into an information system or information network to disclose data or information; it is sufficient to use certain electronic programs, even remotely, in any manner to disclose, copy, or capture data or information. It is conceivable in this case that specific data is collected and stored by authorized individuals and then unlawfully disclosed or misused by them *(Rabee, 2016)*.

However, French law and courts were more cautious regarding data collection and storage by institutions than the Jordanian Cybercrime Law. Article 41 of the French Data Processing Law (1978) prohibits collecting and storing data without official permission. In one case, the French court convicted the company SKF for storing employees' political opinions. The law has since been amended several times, notably in 2004, 2016, 2017, and 2018, providing further protection for personal data *(Ibrahim, 2011)*.

B. The Mental Element of the Crime of Disclosing Data or Information via the Introduction, Publication, or Use of Electronic Programs:

This crime is intentional, requiring not only the general mental element of knowledge and intention the knowledge that the perpetrator is committing the act and the intent to commit it but also a specific intent related to the act of publication, use, introduction, as well as capturing, copying, transferring, or allowing others to access data or information, all of which constitute a violation of privacy in its broadest sense.

Thus, if the perpetrator enters an information system and obtains certain data or information without having a specific intent, the criminal intent is absent. The purpose of the crime should be to cancel, delete, transfer, capture, copy, or disclose the data to others.

If the owner of the data or information provides consent, this serves as evidence that the criminal intent is absent, and thus, no crime is committed.

A recent ruling by the Amman Misdemeanor Court of First Instance stated: "The criminal intent, as defined in Article 63 of the Penal Code, is the will to commit the crime as recognized by the law. Criminal intent consists of two elements: knowledge and intention, in which the perpetrator's will is directed to commit the act despite being aware that this act is punishable by law and would result in the crime upon its commission." The court found that the complainant acknowledged that the defendant accessed her account on Messenger/Facebook (an information system) to resolve matters between them, thus ruling that the criminal intent was absent and declaring the defendant not guilty (*Qistas Publications, 2022)*.

C. The Penalty for the Crime of Disclosing Data or Information via the Introduction, Publication, or Use of Electronic Programs

Anyone who intentionally enters, publishes, or uses a program or command via an information network, a technical information tool, or an information system for the purpose of deleting, adding, destroying, disclosing, corrupting, blocking, encrypting, modifying, changing, transferring, copying, capturing, or enabling others to access data or information, or obstructing, distorting, stopping, or disabling the information system's operation, or accessing or altering a website, or deleting it, or destroying or altering its content, or operating it without permission or exceeding or violating that permission, or impersonating its owner or his identity, shall be punished by imprisonment for no less than six months and a fine of no less than 2,500 Jordanian Dinars and no more than 10,000 Jordanian Dinars.

The penalty is doubled for anyone who commits this act while exploiting their position, work, or the powers granted to them, or if there are multiple victims, or if the crime is repeated, or if the perpetrator commits the crime on behalf of a foreign country or an unlawful organization, according to Article 28 of the law.

The accomplice and instigator are punished with the same penalty as the principal perpetrator, according to Article 27

of the law, which states, "Anyone who intentionally participates, intervenes, or incites the commission of any of the crimes set out in this law shall be punished with the same penalty as the principal offenders."

The penalty is also aggravated in cases of recidivism, as outlined in Article 28 in the following instances:

A – If the perpetrator commits the crime using their position, work, or powers granted to them.

B – If there are multiple victims.

C – If the crime is repeated.

D – If the perpetrator commits the crime for the benefit of a foreign country or an unlawful organization.

Thus, if the perpetrator commits the act because of their job or position, or exploits either of them, such as by using information they were entrusted with to disclose others' secrets and harm them, their penalty is aggravated. This is a commendable tightening by the legislator, in our view, as the perpetrator may have obtained the data or information through their job, violating the privacy of others.

In a recent ruling by the Amman Misdemeanor Court of First Instance, the court linked the violation of privacy (under Article 348 of the Penal Code) with Article 4 of the Jordanian Cybercrime Law and stated, "In relation to the crimes of privacy violation contrary to Article 348 of the Penal Code, as referenced by Article 15 of the Cybercrime Law, and the crime of threatening to reveal something that harms a person's dignity and honor under Article 415 of the Penal Code, as referenced by Article 15 of the Cybercrime Law, the court finds that the legislator, in paragraph one of Article 52 of the Penal Code, has provided for the dismissal of public claims if the personal right is waived. Since the complainant waived her personal right against the defendant, the court must, in accordance with Article 52 of the Penal Code, dismiss the public claim without the need to examine the elements of the crime." The court found no evidence linking the defendant to the crimes and declared him not guilty *(Qistas Publications, 2011).*

3- The Crime of Eavesdropping on and Intercepting Electronic Correspondence and Communications:

This crime is explicitly addressed in Article 7 of the Cybercrime Law, which states:

"A. Anyone who intentionally and without legal justification intercepts the path of data, captures its content, obstructs, alters, deletes, or records that content whether transmitted via an information network, information technology, an information system, or data exchanged within the system or the network shall be punished by imprisonment for not less than six months and a fine of no less than 1,500 dinars and not exceeding 6,000 dinars.

B. The offender shall be punished by imprisonment for no less than one year and a fine of no less than 3,000 dinars and not exceeding 6,000 dinars if they disclose, leak, or use the information obtained through interception.

C. If the interception involves information, data, or any communication related to an official entity, the penalty shall be temporary hard labor for no less than five years and a fine of no less than 15,000 dinars and not exceeding 45,000 dinars".

This article demonstrates the legislator's strict stance, particularly if the data interception or eavesdropping involves government entities, regardless of whether the information pertains to the government itself or individuals using government devices.

Moreover, Article 76 of the Jordanian Telecommunications Law No. 13 of 1995 states:

"Anyone who intercepts, obstructs, records, or deletes the contents of a message via telecommunications networks or incites others to do so shall be punished by imprisonment for not less than one month and not more than six months and a fine not exceeding 200 dinars, or by both penalties".

Therefore, it is prohibited for anyone to intercept, capture, or eavesdrop on electronic correspondence over the information network, to publish it, or even to retain it for personal use whether used immediately or later. It is likewise prohibited to eavesdrop on, intercept, or capture any messages via telecommunications networks or encourage others to do so.

A. The Material Element of the Crime of Eavesdropping on and Intercepting Electronic Correspondence and Communications

The material element of this crime is established when the perpetrator intercepts, captures, records, or eavesdrops on data transmitted via the information network even if they do not publish the data or use it, and even if the targeted individual is a public figure.

It also applies if the perpetrator encourages or engages in eavesdropping or interception via telecommunications networks, as per Article 76 of the Telecommunications Law.

The term "electronic correspondence" includes all forms of communication, whether printed, imaged, symbolically encoded, numerically stored, word-based, or audio recordings interpretation that aligns with Article 76 of the Telecommunications Law.

A specific result is not required for the crime to be complete; the act itself is sufficient. It is considered a formal crime that occurs merely by carrying out the act, regardless of the consequences. Moreover, it is not required that the data be sensitive; even simple information that infringes on an individual's private life, family, or dignity is enough.

The offense can also involve intercepting fragmented or unstructured information and compiling it to form a comprehensive profile. This is possible due to the nature of digital and technical networks and tools such as computers that aggregate and analyze data to build full images of individuals, including bank details, social ties, family, political or economic affiliations (Khalaf. 2021).

Often, such data is collected through cookies small data files or text files sent by websites or servers and stored in the client's web browser during browsing. These cookies track the user's online activity *(S.D.R.M. Weerasinghe).*

B. The Mental Element of the Crime of Eavesdropping on and Intercepting Electronic Correspondence and Communications

This crime requires general criminal intent, which includes both knowledge and willful intent. The perpetrator must intentionally access the information system or network to capture or eavesdrop on transmitted data knowing that the act is criminal and willingly committing it, even if the result does not occur.

C. The Prescribed Penalty for Eavesdropping on and Intercepting Electronic Correspondence and Communications

Anyone who intentionally and unlawfully intercepts, captures, alters, obstructs, or records the content of data whether transmitted through an information network, technology, system, or internally exchanged is subject to imprisonment for not less than six months and a fine of no less than 1,500 dinars and not more than 6,000 dinars.

If the person leaks, discloses, or uses the obtained information, the punishment is imprisonment for not less than one year and a fine between 3,000 and 6,000 dinars.

If the intercepted data or communication pertains to an official entity, the punishment is temporary hard labor for no less than five years and a fine ranging between 15,000 and 45,000 dinars.

The penalty is increased if the crime is committed by someone exploiting their job, role, or authority, or in cases of repeat offenses, multiple victims, or if the act benefits an illegal entity or a foreign state (as per Article 28). Additionally, the same penalty applies to accomplices and instigators, according to Article 27, which states:

"Anyone who intentionally participates in, intervenes in, or incites the commission of any crime mentioned in this law shall be punished with the same penalty as the principal offender",

The court may impose the harsher penalty, unless it decides otherwise, in accordance with Article 72 of the Penal Code, which stipulates:

"1. If multiple felonies or misdemeanors are proven, a penalty shall be determined for each crime, and only the harsher penalty shall be executed.

2. However, the court may combine the penalties, provided that the total does not exceed 15 years for misdemeanors and 30 years for felonies."

4- Obtaining Electronic Credit Information:

Electronic credit or banking information is considered protected under the law. Article 8(a) of the Credit Information Law provides for the protection of such data. Credit information varies in nature: there is a set of credit data specific to companies, public institutions, or civil society organizations, while another set pertains exclusively to companies.

There has been doctrinal disagreement over the right of legal people to privacy. One school of thought considers that a legal person is entitled to privacy, based on the idea that legal people enjoy rights, duties, and freedoms. Another view

refers to this as "internal life." However, a third opinion which we support argues that the information related to a legal person consists merely of "a set of trade, industrial, or professional secrets" and does not fall within the scope of privacy. Privacy is a personal space that an individual reserves for themselves and restricts others from accessing; it applies to natural people, not legal entities.

This section will discuss the crime of obtaining electronic credit information in three subsections: the first on the material element, the second on the mental element, and the third on the prescribed punishment.

A. The Material Element of the Crime of Obtaining Electronic Credit Information:

The material element of obtaining electronic credit information varies depending on the circumstances. If the perpetrator accessed this information after it was provided by another person and was already in their possession, and then disclosed or published it, they would be considered an accomplice to the crime under general criminal law. For example, a bank employee who violates Article 8(a) or Articles 72, 73, and 75 of Banking Law, or any relevant provisions of the Cybercrime Law specifically Articles 6 and 7, which protect credit data could be held accountable.

The situation is different if the perpetrator directly hacked an information system or network to obtain credit information belonging to a specific individual. In such a case, the perpetrator would be considered the main offender under Articles 6 or 7 of the Cybercrime Law. These actions cannot be carried out under Credit Information Law or Banking Law, as those laws apply specifically to bank employees, not to ordinary individuals.

The material element here involves the act of obtaining data or information related to credit cards. However, the law does not adequately cover all types of credit information related to clients. Banking cards are not limited to credit cards but also include debit cards, special credit cards, and check payment cards, which are less commonly used in Jordan.

This is a result-based crime, meaning it is only considered complete when the information is obtained. Mere attempts without success do not constitute crime.

Because of the protection granted to credit data, credit providers are not allowed to access such information without explicit consent from the client or their authorized representative. Likewise, “CRIF” a licensed company authorized to provide credit information to financial institutions may only issue credit reports after confirming such consent.

However, CRIF is exempt from this verification process when the request comes from a bank, an insurance company, or another entity approved by the Central Bank Governor. Thus, banks, insurance companies, or authorized entities are exempt from verifying consent under the license granted to them.

Articles 72 and 73 of the Jordanian Banking Law also reinforce this protection, prohibiting financial institutions and their employees from obtaining credit information unlawfully.

If a bank, financial institution, insurance company, or approved entity obtains credit information during their duties, and that information reaches an unauthorized individual, it is prohibited for that person to publish or disclose such data.

Penal protection for credit information and bank cards is also found in the Cybercrime Law. Article 8 provides:

A. A prison sentence of no less than one year and no more than three years, and a fine between JOD 2,500 and JOD 10,000, shall be imposed on anyone who:

Intentionally and without authorization beyond the scope of authorization obtains or uses electronic payment data or information through information technology, networks, or systems, or publishes such data.

Fabricates, creates, installs, or programs any technological tool or software with the intent of facilitating access to such data.

Deals with forged, copied, or illegally obtained payment cards or data, knowing their illicit nature.

B. If such data is used to obtain money or services without success, the penalty shall be imprisonment of no less than two years and no more than three years, and a fine between JOD 5,000 and JOD 15,000.

C. If the above actions lead to obtaining money or services for oneself or another, the penalty shall be imprisonment of three years and a fine between JOD 10,000 and JOD 20,000.

Article 9 further states that anyone committing an act mentioned in Articles 3, 5, 6, 7, or 8 against systems or platforms related to fund transfers, payment services, settlements, or any other banking services, shall face temporary hard labor for

no less than five years and a fine between JOD 25,000 and JOD 75,000.

Thus, penal protection ensures that no one is legally permitted to access such data under Jordanian Cybercrime, Banking, or Credit Information Laws.

B. The Mental Element of the Crime of Obtaining Electronic Credit Information:

This is an intentional crime that requires general criminal intent. The perpetrator must willfully commit the prohibited act, aiming to achieve the unlawful result and being fully aware of their actions. If someone accesses such information without intending, by accident or during routine work without the intention to obtain or disclose it would not meet the criteria of a criminal mental element.

No one can claim the right to access information under the "Right of Access to Information Law" or related laws to justify obtaining such credit data. Article 13(1) of the Right of Access to Information Law mandates that responsible officials refrain from disclosing protected secrets and documents under any other legislation, including financial or credit data of individuals, as these fall under private life protection even when claimed under public interest criticism.

Public interest criticism is a fundamental aspect of freedom of expression but is not absolute. It must not infringe upon an individual's privacy and should remain within the bounds of public concern.

Jordanian legislation does not explicitly define public interest criticism, but it recognizes it, provided that:

- It is based on a factual event.
- It is expressed in appropriate language, not breaching privacy or financial data.
- The event is socially beneficial.
- It is made in good faith *(Al-Ra'I, 2010).*

C. Punishment for the Crime of Obtaining Electronic Credit Information:

The penalties outlined in Article 8 of the Cybercrime Law differ from those in Article 9, which has been criticized for legislative inconsistencies.

As previously noted, the instigator and accomplice receive the same penalty as the primary offender, according to Article 14. Repeat offenses result in harsher penalties under Article 28(c), and the court may impose the more severe punishment unless otherwise decided, as stated in Article 72 of the Penal Code: If multiple felonies or misdemeanors are proven, each offense receives its own sentence, but only the most severe punishment is carried out. The total combined sentence may not exceed 15 years for misdemeanors and 30 years for felonies.

Conclusion:

This scientific study has examined the extent to which the Jordanian Cybercrime Law No. (17) of 2023 sufficiently regulates crimes related to the violation of private data through digital platforms and modern media in Jordanian legislation. It has also analyzed and studied the provisions of the Cybercrime Law and has reached several findings and recommendations in this field, and the study reached a set of key findings, the most important of which are the Jordanian legislator has regulated crimes related to privacy violations and personal data in the Cybercrime Law in a manner that does not keep pace with developments in this field, and the text of Article 9 of the Cybercrime Law also appeared ambiguous and unclear, and the legislator has not defined, as it has for other crimes, the concept of data violation, and The law provides specific examples of data violations but does not stipulate a crime for breach of privacy through technological means as well.

Recommendations:

1. The study recommends repealing Article 9, which suffers from legislative distortion, as previously discussed, and emphasizes the need for legal provisions to keep up with developments in this area.
2. The study recommends that the Jordanian legislator include a specific provision in the Cybercrime Law that defines data violation crimes.
3. The study recommends explicitly including the term "breach of privacy," as is done in the Jordanian Penal Code, which serves as the general legal framework in this context.

REFERENCES

Aawisheh, S., Al-Hassan, T., & Mansour, A. (2024). The status of digital evidence in administrative litigation. *Al-Balqa Journal for Research & Studies*, 27(3), 42–55.

Aqli, F. (2012). *Legal protection of the right to the sanctity of private life: A comparative study. Doctoral dissertation*, Mentouri Brothers University, Constantine, Algeria.

Ayoub, P. A. (2009). *Legal Protection of Personal Life in the Field of Informatics*. Lebanon: Al-Halabi Legal Publications.

Al-Atoum, M. (2020). Arbitrary Dismissal in Jordanian Labor Law. *Balqa for Research and Studies*, 9(1), 182–185.

Alhasan, T. K., Awaisheh, S. M., & Awaisheh, S. M. (2024). The right of public employee to defend disciplinary penalty in Jordan. *International Journal of Public Law and Policy*, *10*(2), 190-203.

Al-Nawaisa, A. (2017). *Cybercrime: Explanation of the Substantive Provisions in the Cybercrime Law*. (1st ed.). Jordan: Dar Wael for Publishing and Distribution.

Al-Qatatsheh, B. (2022). *Criminal Protection of the Privacy of Digital Personal Data. Doctoral Dissertation,* World Islamic Sciences and Education University, Amman, Jordan.

Al-Ra'i, A. (2010). *Press and Publication Crimes – Defamation and Libel*. (1st ed.). Jordan: Dar Al-Thaqafa for Publishing and Distribution.

Al-Rai, A. (2024). *Cybercrimes – Substantive Provisions of Information Technology and Artificial Intelligence Crimes*. Jordan: Dar Al-Badeel for Publishing and Distribution.

Alrfoua, A. Y. R., Alsweilmieen, S. M., Al-Zubi, J. Kh., Hatamleh, S. S. H., Al-Rafoo, A. Y., Alja'afreh, I. A., & Alja'afreh, B. A. (2024). Administrative Control Measures in Protecting Tourism Activities. *Relações Internacionais no Mundo Atual*, 3(45), 786–805.

Al-Shawabkeh, M. (2011). *Computer and Internet Crimes – Cybercrime*. Jordan: Dar Al-Thaqafa for Publishing and Distribution.

Al-Waleidat, A. A. (2010). *Criminal protection of professional secrets in Jordanian law. Master's thesis*, Middle East University, Amman, Jordan.

Al-Wakeel News. (2023). Cybersecurity: We Detected 2,455 Hacking Attempts in the Kingdom Last Year. Retrieved February 25, 2025, from https://shorturl.at/mvGQ2

Cristina Blanton. (2021). China's Personal Information Protection Law (PIPL). The University of Texas System. Retrieved February 9, 2022, from https://bit.ly/3vfoFqz

El-Shahawi, M. (2005). *Criminal protection of the sanctity of private life*. Egypt: Dar Al-Nahda Al-Arabiya.

Federal Trade Commission. (2020). Privacy and Data Security Update: 2020. United States: Federal Trade Commission. Retrieved February 10, 2022, from https://shortest.link/2Eyi

General Data Protection Regulation (GDPR). GDPR – General Data Protection Regulation. Retrieved May 29, 2024, from https://shorturl.at/fpFHZ

Ibrahim, H. (2011). *Emerging Crimes via the Internet*. Lebanon: Dar Al-Nahda Al-Arabiya.

Khalaf, F. (2021). The Nature of the Violation of Personal Data of Social Media Users and Its Practical Applications. *Al-Muhaqqiq Al-Hilli Journal for Legal and Political Sciences*, Baghdad, Iraq, 13(3).

Rabee, E., & Rabee, Z. (2016). Violation of the Sanctity of Private Life. *Journal of Legal and Political Sciences, Faculty of Law, Jerash University, Jerash, Jordan*, 11(1),

Weerasinghe, S. (n.d). Cookies, Privacy and Cyber Security. *Faculty of Information Technology, University of Moratuwa, Sri Lanka*.

Saleh, M. (2016*). International Legal Protection of Personal Data Online Between International Treaty Law and National Law. Doctoral Dissertation*, Ain Shams University, Cairo, Egypt.

Salem, M., & Wahjeej, H. (2007). Cybercrime. *Journal of the University of Babylon*, 14(2), Babylon, Iraq.

SIGI-Jordan (Tamkeen Center for Support and Empowerment). (2023). Cybercrime Unit: 2,115 Cyber Intrusion Cases Recorded in Jordan During 2022. Retrieved February 25, 2025, from https://www.sigi-jordan.org/article/6189

University of Minnesota Human Rights Library. (2025). Arabic version – Human Rights Library. Retrieved April 29, 2025, from https://shorturl.at/BJSX3

Court Rulings:

Qararak Publications. (2024). Judgment No. 793 of 2024, Court of Cassation in its Criminal Capacity, issued on 2024-02-13.

Qistas Publications. (2013). Judgment No. 6276 of 2013, West Amman Magistrate Criminal Court, Jordan.

Qistas Publications. (2019). Judgment No. 20776 of the year 2019, Amman Magistrates Criminal Court, Jordan.

Qistas Publications. (2022). Judgment No. 5337 of 2022, Amman Criminal Conciliation Court, Amman, Jordan.