

The Extent of the Impact of Cybersecurity Rules on Electronic Civil Transactions in Jordanian Law

Sanaa Maaytah¹ and Hiba Kobarie²

Abstract

The Jordanian legal system faced challenges in keeping up with technological developments, particularly concerning electronic civil transactions. The issue of this study lies in the possibility of incorporating cybersecurity rules into electronic civil transactions. While also clarifying the position of Jordanian legislation on this matter. The Jordanian legislator relied on general rules in civil law and specific rules in the Cybersecurity Law and the Electronic Transactions Law to address this issue. Moreover, the cybersecurity rules aimed to protect the data contained in the electronic register related to civil transactions and contracts entered into by individuals, institutions, and civil companies by combating cyber-attacks that sought to exploit this information illegally. Furthermore, this study recommended the necessity of including a legal provision in the Cybersecurity Law to enhance the role of these rules for civil companies, governmental, and private institutions by incorporating these rules into civil electronic contracts and transactions conducted with individuals (consumers), due to the connection between them in activating the role of protection.

Keywords: Rules, Security, Cyber, Electronic Transactions, Jordanian Law

INTRODUCTION

The technological revolution has introduced new legal concepts, such as artificial intelligence (Al-Haimoudi, 2023), and cybersecurity, which have brought about many fundamental changes in the electronic contracting environment, especially in protecting the security of electronic transactions and the electronic systems based on them from electronic hacking attacks. Further, these attacks target the information in electronic transactions and the unauthorized use of information and exploitation.

During the present age, transactions conducted electronically have multiplied, and they cannot be confined to a single field. Therefore, it has become necessary for the law to intervene and establish rules that help in following sound methods for using modern technological means, As a consequence establishments are allowed to keep papers that prove their assets electronically.

Also, replacing the traditional obligation imposed on establishments and companies, which involves keeping traditional commercial books, by filling in electronic commercial records (Ali, 2016). There is no doubt that the issue of maintaining the protection and security of networks, systems, and information, which electronic transactions rely on, is of great importance. Its impact has been reflected in the stability of national security, as well as in the international community, due to the relationship between electronic transactions and cybersecurity rules. Hence, the problem of this study emerges in shedding light on the possibility of including cybersecurity rules in electronic civil transactions, while stating the position of Jordanian legislation on this.

Moreover, cybersecurity crimes take various forms, such as fraud, assault on bank cards, and individuals' electronic payment tools. This could expose the state's rights to violation, or even threaten to disclose secrets or data related to companies or establishments represented by their electronic transactions with individuals (Mustafa, 2022).

The study's importance is twofold. Practically, it clarifies the impact of cybersecurity rules on civil transactions in Jordanian law, a crucial topic in contemporary times. This clarification aids in guiding consumers practically by integrating these rules into the electronic transactions they undertake. Scientifically,

¹ PhD in Private Law from the Islamic Sciences University, Amman, Jordan. E-mail: sanaa_maaytah@yahoo.com

² PhD in Private Law from the Islamic Sciences University, Amman, Jordan E-mail: hibakobarie@gmail.com

the study highlights legislative gaps in the texts regulating cybersecurity rules and their influence on civil transactions under Jordanian law. And this enriches the scholarly resources available to legal researchers studying this subject area.

Accordingly, the researchers will address the extent of the impact of cybersecurity rules on electronic civil transactions according to Jordanian legislation in this study.

LITERATURE REVIEW

Study of Hensali, Sabrina (2022), "Protection of Personal Data for Electronic Contractors: Towards Achieving Cybersecurity," Algerian Journal of Legal and Political Sciences, Volume (59), Issue (2). This study aims to clarify the protection of personal information related to electronic transactions in general, whether civil or commercial, and to explain the meaning of personal data and the legal mechanisms established to protect these personal data, both criminal and civil, according to Algerian legislation.

Study of Abu Hussein, Hanin Jameel (2021), "The Legal Framework for Cybersecurity Services" This study discusses the services provided by cybersecurity in all electronic fields related to commerce and the role of the cyber environment in contributing to economic activities at the regional and international levels within the scope of the commercial framework.

Study of Maharib, Abdul Aziz, Qasim (2023), "Artificial Intelligence and Cybersecurity" This study explores the relationship between artificial intelligence systems and the role of cybersecurity in facing threats that individuals might pose by using AI tools. It also attempts to explain the AI-related software used by companies and how they confront threats to cybersecurity.

Study of Al-Haimoudi, Badr (2023), "Cybersecurity and Information Systems Protection" This study highlights the importance of cybersecurity in protecting personal bank accounts and personal data, as well as the protection of electronically recorded commercial ledgers. This is achieved through cooperation agreements between companies and the National Cybersecurity Center, which include specific strategies to protect the necessary data.

Study of Mohammed, Nasser (2022), "Forms of Cyber Space Violations, Means, and Impacts," Nadao Journal for Legal Studies, Issue (40). This study showcases the forms of cyber space violations and their consequent impacts, explaining the concept of cyber space and classifying its violators. It employs a descriptive-analytical approach within Saudi legislation.

Research Objectives

The concept of cybersecurity in the rules of Jordanian legislation.

The concept of electronic civil transactions and civil contracts.

The extent to which cybersecurity rules can be included in civil contracts, and the position of Jordanian legislation towards this.

Research Questions

What is meant by cybersecurity within the rules of Jordanian legislation?

What is the concept of electronic civil transactions and civil contracts?

Can cybersecurity rules be included within the provisions of electronic civil transactions and contracts, and what is the position of Jordanian legislation on this?

METHODOLOGY

This study employs both descriptive and analytical methods. It involves using these approaches to gather information by reviewing legal texts concerning the impact of cybersecurity rules on electronic civil transactions as outlined in Jordanian legislation, analyzing them, and examining relevant decisions from the Jordanian Court of Cassation.

The Concept of Cybersecurity and Electronic Civil Transactions

Cybersecurity has emerged recently (Al-Rabdi,2023), with the increasing prevalence of electronic attacks, which include data hacking, theft, and unauthorized use.

Hence, with technological advancements, major companies have turned to adopting and innovating new practical solutions to cope with sophisticated electronic attacks. This is due to the growing trend towards engaging in electronic transactions among individuals and the disruptive impact these attacks have on national entities and their sovereignty (Hansali, 2022)

wherever data, personal, and financial information of contracting individuals (consumers) constitute a target for electronic attacks, due to the high sensitivity and confidentiality of this information. Therefore, in this study, we will address the definition of cybersecurity in the first chapter, followed by defining electronic civil transactions in the second chapter.

Definition of Cybersecurity

The need for legislation regulating cybersecurity arose from the necessity for cybersecurity professionals to achieve the required level of data protection while also enjoying a certain level of freedom in navigating the data that needs protection. This depends on the parties involved in electronic transactions and their adherence to the rights and responsibilities within the framework of these transactions or electronic activities (Abu Hussein, 2021).

On the other hand, establishing legislation to regulate cybersecurity represents a shift of the world's personal, professional, scientific, and vocational interactions into the digital realm. Consequently, any transgression or violation that could occur to these interactions in the physical world translates to electronic platforms, necessitating their protection (Nasser, 2022).

Cybersecurity is a modern technology that focuses on maintaining the security and confidentiality of data, including data related to electronic civil transactions conducted between individuals. Additionally, "Security," in language, is defined as "the state of being free from fear (Ibn Manzur, 2000)," and in terminology, it is defined as "a serious process aimed at managing the public affairs of a state, its entity, dignity, and sovereignty in the name of national sentiments (Hajj, 2016) ".

As for the term "Cyber," linguistically, it is a word of Greek origin meaning "governance and direction." As a terminology, it refers to "everything related to or associated with computers, information technology, and virtual reality." Cybersecurity, in turn, is defined as "the process of protecting banking systems, networks, and software against digital attacks aimed at accessing sensitive information and exploiting it in actions that threaten the security of nations and individuals (Al-Haimoudi, 2023)."

Regarding the position Jordanian legislation, it defines cybersecurity in Article (2) of the Cybersecurity Law. Further, the definition provided encompasses all measures aimed at safeguarding the infrastructure from incidents that impact cybersecurity or result from failure to adhere to proper security procedures.

Thus, cybersecurity can be defined as a set of rules aimed at protecting the security of systems, networks, and the information they contain from exploitation or deception that affects national security and stability, as well as individuals associated with them. Cyber-attacks are defined as actions that diminish the capabilities or functions of a computer network for national or political purposes, exploiting specific vulnerabilities that enable the attacker to manipulate the system (Al-Kassasbeh, 2023).

Therefore, crimes against information security are described as organized and transcontinental. Consequently, cybersecurity focuses on protecting vulnerabilities in devices used by individuals in companies and institutions that are connected to the Internet (Muharib, 2023).

Definition of Electronic Civil Transactions

The Jordanian legislator recognizes transactions conducted electronic way, in response to the adaptation of private and governmental entities to the requirements of the modern era. Most data are now recorded

electronically due to its accuracy in storing information and quick accessibility at any time. Moreover, the Jordanian Electronic Transactions Law has determined the methods of entering data and information, the conditions that must be met in the electronic record, and in any agreement concluded between the parties for the purpose of creating an obligation between them (Jordanian Electronic Transactions Law No. 15 of 2015, 2015).

Hence, the researchers believe that the importance of electronic transactions is evident through the vast number of daily transactions conducted between consumers, as well as the contracts concluded by civil institutions and companies. And these electronic civil transactions require the rapid storage of a large amount of data, as is the case for civil service institutions and the local community.

As for the difference between civil electronic transactions and the electronic civil contract, the Jordanian legislator defined the contract in Article (87) of the Civil Law as "the binding of the offer issued by one of the contracting parties with the acceptance of the other, and their agreement in a manner that establishes its effect on the subject matter, and results in the obligation of each party to what is due to the other (Obaidat, 2024)."

The researchers believe that the above article defines the contract in general, and thus serves as a reference for the concept of the electronic contract. However, the electronic contract differs from the traditional contract in the provisions that arise from it and in that it is concluded by electronic means, even if only part of the contractual phase (the Jordanian Consumer Protection Law, Article No.2, 2017, Official Gazette).

Further, the commercial contract does not differ from civil contracts, except in acquiring its commercial nature through the characteristics of the person who concludes it or the nature of the subject (type of work). Its elements do not differ from those of the civil contract (Jordanian Electronic Transactions Law No. 15, 2015).

As for the position of the Jordanian Electronic Transactions Law, it did not provide a direct definition of the electronic contract, unlike its position in the Jordanian Electronic Transactions Law No. (85) of 2001 (before the amendment), which defined it as "an agreement concluded entirely or partially by electronic means."

As a result. the researchers found that the Jordanian legislator considers contracts part of electronic transactions, which may be civil or commercial. The Electronic Transactions Law includes both civil and commercial transactions in its provisions.

Although, article No.: 2 of the Electronic Transactions Law defines transactions as "any action between one or more parties to create an obligation on one party or a reciprocal obligation between two or more parties, whether commercial or civil or involving a governmental entity." Additionally, electronic transactions are defined in the same article as "transactions, executed by electronic means."

On the other hand, the use of electronic civil transactions is not limited to individual contractors "consumers" (Jordanian Consumer Protection Law, 2017, Official Gazette, Issue 5455, p. 2725); it extends to civil companies as well, which engage in electronic civil transactions and contracts, or even electronic records.

So, these companies, unlike profit-seeking entities, are subject to civil law provisions, such as law firms that establish relationships among professionals and maintain their own record called "Civil Companies Register (the Jordanian Companies Law, Article 7/c/1, No. 22, 1997, Official Gazette, Issue 4204, p. 2038)."

As for electronic writing of a contract or beneficiary data, it is an expression of what is stated in the contract or document using symbols, and it can be extracted in paper form if needed, allowing it to be used as written evidence in judicial courts (Mu'min, 2007).

The researchers raise a question: If these electronic civil transactions must inherently be written electronically, how can the legislator prevent the modification or manipulation of data?

In reality, for electronic writings to be admissible, several conditions must be met: the data should not be susceptible to modification, such as deletion or addition, so that this electronic written evidence can be secure and trustworthy, and can be referred to when needed (Al-Romi, 2006).

In addition to identifying the creator of electronic writing, this is accomplished through electronic signatures (The Electronic Transactions Law, 2015) that meet the required conditions under the Electronic Transactions Law. These conditions include that the signature uniquely identifies its owner to distinguish them from others, remains under their control, and allows the identification of the creator's identity, time, and date (The Electronic Transactions Law, Article No. 15, 2015).

Moreover, electronic writing is a protective measure for safeguarding the contracting parties in electronic transactions. Accordingly, the law permits data retention in electronic form, allowing any ministry, municipality, or institution to maintain all transaction-related data electronically if the conditions required for electronic transactions are observed (The Electronic Transactions Law, Article No. 4).

Hence, the purpose of adhering to the conditions required by the law in electronic transactions is to ensure that they produce their legal effects if used as written evidence (The Electronic Transactions Law, Article No. 8 & Jordanian Evidence Law, Article 13, No. 30, 1952, Official Gazette, Issue 1108, p. 200).

Also, the Court of Cassation confirmed this by considering the electronic correspondence that took place between the two parties over a certain period regarding the item to be purchased and dealt with and the mechanism for providing it to the concerned party. In addition to the method and dates of payment of the price, which are considered messages that enjoy the normal attribution of proof and are considered to have been issued by the defendant as long as he does not provide evidence to prove otherwise (Court of Cassation Judicial Decision, No. 4191, 2023).

Therefore, the researchers believe that the concept of electronic transactions is derived from the method used to store data related to beneficiaries and consumers, as well as the method used to conduct civil transactions in institutions and companies, where no alteration is permissible until they are relied upon as written evidence.

The Relationship Between Cybersecurity Rules and Electronic Civil Transactions

There is a close relationship between cybersecurity rules represented by the procedures that seek to maintain the security of electronic networks and information and protect them, and electronic civil transactions; which take place between individuals and civil companies electronically, and civil companies, which aim to satisfy personal needs.

Therefore, it is necessary to clarify the extent of the relationship between cybersecurity rules and electronic civil transactions in the first requirement, followed by the Jordanian legislation's stance on the possibility of incorporating cybersecurity rules into electronic civil transactions.

The Relationship of Cybersecurity Rules With Electronic Civil Transactions

The study previously illustrated the concept of electronic civil transactions by examining the manner in which they are conducted, specifically highlighting that these transactions and civil contracts are carried out electronically.

Given the legislator's consideration of maintaining trust and security for the beneficiary or consumer, he explained the conditions that must be met in electronic civil transactions. Hence, the researchers raise a question: What if data and information are the focus of cyber-attacks that aim to exploit companies or even damage their reputations, as is the case with banks and civil service institutions?. And to answer this question, it is necessary to clarify the link between cybersecurity rules and electronic civil transactions.

Cybersecurity rules relate to electronic civil transactions through several things: Cybersecurity rules seek to maintain the protection of electronic civil transactions and to confront electronic attacks represented by hacking, exploitation, or unauthorized use. Hence, the information on which electronic civil transactions are based constitutes the essence and primary target of electronic (cyber) attacks, due to the sensitivity and danger of this personal information; such as banking information related to electronic payment operations.

The Jordanian legislator has organized a set of controls and provisions that regulate the protection of personal data and information in a law called the "Personal Data Protection Law" (Jordanian Personal Data

Protection Law No. 24, 2023, Official Gazette, Issue 5881, p. 4338). This legislation has addressed the issue of requiring prior consent to process and use personal data related to natural persons electronically (Jordanian Personal Data Protection Law, Article No.5).

Further, the Jordanian legislator exempted the requirement of obtaining prior consent in several specific cases, as indicated by Article No. (6) of the Jordanian Personal Data Protection Law. Finally, cyber-attacks in their various forms adversely affect national security and the economy. They harm public interests that states seek to protect in pursuit of sustainable development goals. As well as, the prosperity of electronic commerce.

The Jordanian legislation's stance on the possibility of incorporating cybersecurity rules into electronic civil transactions

The Jordanian legislator recognized cybersecurity rules in a law called "Cyber Security Law" numbered (16) of 2019. The law established the National Cyber Security Council, whose primary goals include building an effective cybersecurity framework at the national level to protect the Hashemite Kingdom of Jordan from cyber threats and attacks and to safeguard the safety of individuals, properties, and information.

The National Cyber Security Council has engaged in several cooperation agreements with numerous institutions and companies whose data nature is critical and worthy of protection, such as the Central Bank. Additionally, partnerships and memoranda of understanding have been signed with a group of educational and academic institutions, including the Talal Abu-Ghazaleh Organization and Amman University, to exchange expertise and conduct cybersecurity training courses (National Cyber Security Council website).

As the Cyber Security Division, it verifies the use of applications available to beneficiaries, such as WhatsApp and Telegram, if there is any use that harms the rights of users or the occurrence of violations that could threaten their lives by taking appropriate measures (Judicial decision of the Jordanian Court of Cassation, No. 4140, 2022, Qarark Website).

Paragraph (D) of Article 6 of the Cybersecurity Law issued instructions for classifying cybersecurity incidents, where cyber incidents were classified as.

Furthermore, cyber incidents are classified into several categories, starting with the most severe incident, which leads to the complete disruption of essential services or the leakage or destruction of sensitive data, and then the serious incident, which is the incident caused by malware or hacking that has a limited impact on services or hacking operations that do not affect a group of data that characterized as sensitive or incidents that occur in higher education institutions and lead to the complete disruption of essential services.

This is followed by medium incidents, which involve impactful reconnaissance and scanning operations or non-impactful hacking attempts targeting data belonging to security agencies, the military, ministries, companies, and government institutions. These incidents also include the erasure of sensitive data and the destruction affecting a limited part of the essential services provided by higher education institutions, as well as incidents that lead to the complete disruption of services provided by individual companies and private institutions.

As for low incidents, these occur in higher education institutions through non-impactful hacking attempts on sensitive data. They also include incidents that do not result in the complete disruption of services provided by private institutions and individual companies. Based on what has been mentioned, the researchers find that the provisions of the Jordanian legislation are consistent with and support the inclusion of cybersecurity rules in electronic civil transactions. This ensures effective protection for the parties involved in the contractual relationship from any cyber-attacks and breaches targeting the information that forms the basis of this electronic contractual relationship.

RESULTS AND DISCUSSION

Cybersecurity rules aim to protect the data contained in electronic records related to civil transactions and contracts, which are concluded by individuals, institutions, and civil companies. This protection is achieved by

countering cyber-attacks, hacking, or breaches intended to exploit this information illegally or to damage the reputation of the institution and the parties involved.

There is a close relationship between cybersecurity rules and electronic civil contracts governed by the Electronic Transactions Law. These laws complement each other by protecting the data contained in electronic civil transactions and contracts. Consequently, the National Cyber Security Center was established to expand the protection umbrella of these rules over all electronically recorded data.

CONCLUSION

Electronic means are currently among the most important means used to conclude contracts and conduct civil electronic transactions in various institutions and companies due to their accuracy and speed in storing data and information. Therefore, this study reached several results and recommendations, the most important of which are:

Recommendations

The researchers recommend that the Jordanian legislator include a legal provision in the Cybersecurity Law to enhance the role of these rules for civil companies, government and private institutions, and individual civil companies. This can be achieved by incorporating these rules into electronic civil contracts and transactions conducted with individuals (consumers). Also, the integration of these rules is crucial for activating protection and enhancing the trust and security sought by those dealing with civil companies and institutions, thereby reducing potential damages from any breach or hacking. The researchers propose the following wording: "The provisions of this law, including its protection and risk response measures, shall apply to electronic civil transactions and contracts conducted by governmental and private institutions and companies by the cooperation agreements concluded between them."

The researchers recommend that the Jordanian legislator add a provision to the Cybersecurity Law to enhance the role of the National Cyber Security Center. This can be achieved through entering into cooperation agreements with state institutions, private institutions, and individual entities to define the issues to be protected and conduct training courses for specialists in these civil companies and institutions. They should be trained to respond to cyber-attacks and data breach attempts related to private, governmental, and civil institutions. Therefore, the researchers propose the following formulation: "The National Cyber Security Center, in cooperation with the Board of Directors of governmental and private institutions, undertakes the task of identifying sensitive issues and data to be protected through a cooperation agreement concluded between them." Additionally, the researchers recommend adding a provision related to conducting training courses and propose the following: "The National Cyber Security Center shall conduct regular training courses at specified intervals with technical experts nominated by the institution or company to train them on responding to cyber-attacks and breach attempts, thereby expanding the protection umbrella of cybersecurity rules and enhancing its concept among individuals in society."

REFERENCES

- Abu Hussein, Hanin Jameel (2021), *Legal Framework for Cybersecurity Services (A Comparative Study)*, Master's Thesis, Middle East University, Jordan.
- Al-Haimudi, Badr (2023), *Cybersecurity and Protection of Information Systems*, Published Research, Al-Manarah Journal of Legal and Administrative Studies, Issue 46.
- Ali, Nawal Abdul Rahman Ahmed (2016), *Modern Technological Means and Their Impact on Civil and Commercial Transactions*, Master's Thesis, Al-Imam Mahdi University, Algeria, p. 15.
- Al-Kassabah, Rashid Omar Muthqal (2023), *Criminal Protection of Data and Electronic Information in Jordanian Cybersecurity Law (A Comparative Study)*, Master's Thesis, Al-Zarqa University.
- Al-Rabadi, Malik Ya'qub (2023), *Legal Regulation of Cybersecurity in E-commerce*, Master's Thesis, Yarmouk University, Jordan.
- Al-Romi, Muhammad Amin (2006), *Legal Framework of Electronic Arbitration*, Dār al-Fikr al-Jāmi'ī, Alexandria.
- Hajj, Miloud Amer (2016), *Arab National Security and Its Future Challenges*, Dār Jāmi'at Nāif for Publishing and Distribution, Riyadh, Saudi Arabia.
- Ibn Manzur, Jamal al-Din ibn Makram (2000), *Lisān al-'Arab*, Letter Ayn, Dār Ṣādir, Beirut.
- Maharib, Abdul Aziz Qasim (2023), *Artificial Intelligence and Cybersecurity*, Egypt, Al-Mal wal-Tijarah Magazine, Issue 653.

The Extent of the Impact of Cybersecurity Rules on Electronic Civil Transactions in Jordanian Law

Moumen, Taher Shoukry (2007), *Electronic Sales Contract*, Dār al-Nahḍah al-‘Arabīyah, Egypt
Nasser, Mohammed (2022), *Forms of Cyber Space Violations, Means, and Impacts*, Algeria, *Al-Nadwah Journal of Legal Studies*, Issue 40.

Obaidat, Ibrahim Muhammad (2024), *Legislation of Electronic Commerce: A Comparative Study*, Dār al-Thaqāfah for Publishing and Distribution, Amman.

Mustafa, Islam Gomaa (2022), *Cybersecurity Breach Crime and Protection of Data and Information Use in Egyptian Law*, *Legal Journal*, Volume 12, Issue 3, p. 725.

Laws

Cybersecurity Law No. 16 of 2019, published in the Official Gazette on 16/9/2019, Issue 5595.

Jordanian Data Protection Law No. 30 of 1952, published in the Official Gazette on 17/5/1952, Issue 1108.

Jordanian Companies Law No. 22 of 1997, published in the Official Gazette on 15/5/1997, Issue 4204.

Jordanian Electronic Transactions Law No. 15 of 2015, published in the Official Gazette on 17/5/2015, Issue 5341.

UAE Electronic Transactions Law No. 46 of 2021.

Jordanian Personal Data Protection Law No. 24 of 2023, published in the Official Gazette on 17/9/2023, Issue 5881.

Jordanian Consumer Protection Law for the year 2017, published in the Official Gazette on 16/4/2017, Issue 5455.

Instructions for Classifying Cybersecurity Incidents for the year 2023, available on the National Cyber Security Center website, www.ncsc.jo.

Agreements

Memorandum of Understanding with Talal Abu Ghazaleh International Group, and Memorandum of Understanding with Amman University, National Cyber Security Council website, www.ncsc.jo.

Judicial Decisions

Judicial Decision of the Jordanian Court of Cassation, in its Criminal Capacity, No. 4140, issued on 9/3/2022, yourlegaldecision.com.

Judicial Decision of the Court of Cassation, in its Civil Capacity, No. 4191/2023, issued on 28/12/2023, yourlegaldecision.com.

Websites

<https://en.oxforddictionaries.com/definition/cyber>.

<https://www.un.org/sustainabledevelopment/ar/>.