INTERNATIONAL JOURNAL OF CYBER CRIMINOLOGY

VOLUME NO. 19
ISSUE NO. 1
JANUARY - APRIL 2025

ENRICHED PUBLICATIONS PVT. LTD

S-9, IInd FLOOR, MLU POCKET,
MANISH ABHINAV PLAZA-II, ABOVE FEDERAL BANK,
PLOT NO-5, SECTOR-5, DWARKA, NEW DELHI, INDIA-110075,
PHONE: - + (91)-(11)-47026006

INTERNATIONAL JOURNAL OF CYBER CRIMINOLOGY

Managing Editor
Mr. Amit Prasad

INTERNATIONAL JOURNAL OF CYBER CRIMINOLOGY

(Volume No. 19, Issue No. 1, January - April 2025)

Contents

The Electronic Contract in Civil and Commercial Codes

Ahmad Mahmoud Al Masadeh1*, Ahmed M.Khawaldeh2, Mohammad Assaf Al-salamat3
College of Law, Amman Arab University

A B S T R A C T

In the domain of electronic contractual agreements, both in theoretical discourse and practical implementation, this subject carries substantial significance. This endeavours to scrutinize Jordanian legislative frameworks by means of a comparative examination delineated in two sections. Our investigation places particular emphasis on elucidating the fundamental nature and distinguishing characteristics of electronic contracts vis-à-vis their traditional counterparts, delineating the methodologies involved in their formation, and elucidating their applications within civil and commercial contexts, all within the purview of the Jordanian Electronic Transactions Law, specifically Law No. 15 of 2015 and its subsequent amendments. Methodologically, our approach is chiefly descriptive and analytical in nature. Secondary sources constitute the primary reservoir of data for this study, with a methodology predominantly reliant upon simple content analysis to evaluate and present the accrued information. Drawing upon key insights derived from this analytical framework, our study concludes that electronic contracts predominantly manifest through online platforms, with email technology serving as a pivotal conduit for electronic commercial transactions. Furthermore, the research discerns certain reservations and constraints within the ambit of Jordanian legislation concerning electronic contracts, elaborating upon the principal implications thereof.

Keywords: *Electronic Contract, Electronic Offer, E-Commerce, Digital Environment.*

1. INTRODUCTION

The rapid convergence of technology and digitalization has catalysed profound transformations in the everyday operations of contemporary society. Departing from time-intensive, formal, and less convenient transactional methods, individuals have embraced digitalized, technologically advanced means of communication and information exchange (Van Veldhoven & Vanthienen, 2022). This paradigm shift in transactional and communicative modalities has yielded dual effects: enhancing convenience, efficiency, and utility, while simultaneously presenting challenges inherent to the integration of electronic mediums within the digital landscape.

Indeed, the pervasive integration of electronic mediums in the digital age has engendered significant challenges for traditional norms and regulatory frameworks, necessitating their adaptation to accommodate the evolving requisites of the electronic and digital domain. Notably, this evolution seeks to mitigate innovative obstacles such as hacking, cybercrimes, and fraudulent legislative documentation (Yuri et al., 2021). These challenges are not unique to any specific locale but present uniform concerns and hurdles across jurisdictions, including Jordan.

Jordan's legal framework, renowned for its rich civil law tradition and robust Islamic jurisprudence, has come under critical scrutiny from empirical scholars (Arabi, 2021). Despite concerted efforts to modernize and accommodate technological advancements, such as the enactment of specialized legislation governing electronic transactions and laws addressing cybercrimes, the prevailing consensus among scholars is that Jordanian legislation and regulatory mechanisms remain inadequate to effectively contend with the dynamic and evolving landscape of technological interfaces (Toubat, Halim, & Magableh, 2020). These divergent assessments underscore a pressing challenge confronting Jordanian state and judicial authorities.

In a similar vein, a comparative study conducted by Alsheyab (2023) further elucidated the challenging state of Jordan's electronic legislative framework. This analysis juxtaposed Jordan's Electronic Transactions Law No. 15 with the Trust Service Law of 2021 in the UAE. Employing a comparative approach, the study sought to assess the efficacy of these respective legislations in facilitating secure electronic transactions with minimal time investment. The findings of this study suggested that Jordan's Electronic Transactions Law No. 15 exhibited significantly lower efficiency compared to its counterpart in the UAE. Specifically, the enactments within Jordan's legislation were found to demonstrate suboptimal performance in discerning and addressing various security concerns, including the proliferation of counterfeit data, fraudulent content, inaccurate reports, spurious documentation, and breaches of contract (Alsheyab, 2023).

The precarious state of safety concerning commercial transactions in Jordan underscores a pressing need for scholars to address this critical issue. Recent research has highlighted deficiencies within Jordan's civil laws pertaining to consumer rights in electronic contracts, revealing alarming inadequacies. Scholars have drawn attention to the incapacity of Jordan's civil law to effectively navigate the complexities of electronic transactions in the digital era, expressing a pessimistic view towards its ability to address the intricacies inherent in such transactions. Moreover, a recent study has identified inherent flaws and fundamental shortcomings within Jordan's electronic contract laws, amplifying concernsregarding legal deficiencies and the deprivation of consumer protections (AlZawahreh, Alghathian, & Al-Lasasmeh, 2024). This underscores the sensitive nature of the legal shortcomings within Jordanian legislation, particularly evident in the Electronic Transactions Law No. 15 of 2015, as previously referenced.

Hence, this research undertook a deliberate endeavour to scrutinize the Electronic Contract No. 15 of 2015 within the legal framework of Jordan, aiming to elucidate its commercial and civil dimensions and gain a comprehensive understanding of its underlying principles. Additionally, the study aimed to unveil

latent limitations within Jordan's legal frameworks, thereby shedding light on discrepancies that may impede their alignment with the evolving expectations ofthe digital realm. Employing a rigorous methodology, this study rigorously examined the challenges and intricacies associated with the formation, validity, and enforcement of electronic contracts under Jordanian jurisdiction. Lastly, it sought to evaluate the efficacy of extant consumer protection measures in safeguarding the rights and interests of consumers engaged in electronic transactions.

With meticulous and intricate endeavours dedicated to exploring electronic contracts, this study is poised to fulfil its primary objective of offering a concise and descriptive exposition of the comprehensive investigation into electronic contracts, particularly within the purview of Jordanian laws. This thorough exploration promises to provide legal entities and their affiliates with a succinct overview of the advantages, disadvantages, and associated nuances of electronic contracts. Furthermore, it aims to afford stakeholders involved in the pertinent contract law with enhanced clarity concerning their rights and responsibilities. From a theoretical standpoint, this study assumes a pivotal role in elucidating and enriching the understanding of empirical scholars regarding the multifaceted landscape of Jordan's electronic contract law. The subsequent sections of the paper have been structured to encompass a literature review, delineation of the adopted research methodology, presentation of results and subsequent discussion, with the concluding section summarizing the paper and offering implications and recommendations.

Literature Review

The electronic contract, while categorized among designated contracts, conforms to the fundamental principles governing conventional contracts in terms of composition, types, and content. It is thereby subjected to the overarching framework of general contract theory. Consequently, this chapter will commence by delving into the essence of electronic contracts, subsequently examining their defining characteristics, and ultimately discerning the distinguishing features that differentiate them from analogous contractual arrangements.

What is the Electronic Contract

Before delving into electronic contracts, it's crucial to grasp the general concept of contracts. Contracts entail legal agreements that establish obligations between parties, typically a creditor and debtor. While a universally applicable definition for all contracts proves elusive, civil legislation, such as Article 89 of the Egyptian Civil Law and Article 87 of the Jordanian Civil Law, offers guidance. These articles define a

contract as an agreement wherein one party makes an offer, the other accepts, and both agree, thus establishing reciprocal obligations.

Electronic contracts adhere to the structure and composition of traditional contracts outlined in general obligation theory. An electronic contract is defined as the creation, signing, management, and storage of contracts online, unrestricted by time and space, facilitated through electronic signatures and encryption based on certificates. This contrasts with traditional methods involving face-to-face interactions (Kim & Park, 2014).

In the realm of electronic contracts, the convergence of offers for goods and services with acceptances from individuals across multiple jurisdictions occurs through diverse technological mediums, including global internet networks. The objective is to formalize agreements, often referred to as "smart contracts" within the electronic contract domain. In this context, a contract emerges as the culmination of offer and acceptance facilitated via the expansive reach of the internet, employing electronic data interchange to establish contractual obligations (Wang & Xu, 2023).

Turning our attention back to the Jordanian Civil Law, we observe that this emergent form of electronic contract has been addressed, albeit without explicit reference to "electronic contracts" within the legal text. Article 102 of the Jordanian Civil Law pertains to contracts executed via telecommunications or similar channels when the contracting parties are not physically co-located. This legislative treatment has long been established, recognizing the establishment of electronic contracts through intermediaries. Similarly, Article 94/1 of the Egyptian Civil Law addresses the presentation of offers within a contractual gathering (Article 94/1 of the Egyptian Civil Code).

In the Jordanian Electronic Transactions Law No. 15 of 2015, Article 2 defines "transactions" as encompassing any action executed among one or more parties, leading to the creation of an obligation on one party or reciprocal obligations among multiple parties, irrespective of whether the action pertains to commercial, civil, or governmental affairs. Moreover, the same provision defines an "electronic document" as a document formulated, signed, and exchanged electronically (Article 2 of the Jordanian Electronic Transactions Law No. 15 of 2015).

Furthermore, the Federal Civil Transactions Law of the United Arab Emirates, Law No. 5 of 1985, Article 125 characterizes a contract as the manifestation of an offer by one party, followed by the acceptance of the other party, culminating in an agreement that impacts the subject matter of the contract and imposes obligations mutually agreed upon by both parties (Article 125 of the UAE Civil

Civil Transactions Law No. 5 of 1985).Despite the pervasive use of the term "electronic contract" and its recurrence in the discussions within the United Nations Commission on International Trade Law (UNCITRAL), there exists no precise definition for it. The term "electronic contract" typically denotes the recording of a contract through electronic communications, such as data messages. This concept is elucidated in Article 2 of the UNCITRAL Model Law on Electronic Commerce of 1996, which defines a "data message" as information generated, sent, received, or stored via electronic, optical, or analogous means (Sadual, 2021).

The committee responsible for drafting this law intended for this definition to encompass all electronic applications, including the formation of contracts and commercial transactions in their entirety. Accordingly, an electronic contract, as defined by this law, is a contract wherein the expression of intent between the involved parties is conducted using the means outlined in Article 2 (a) and (b), which are:

- Transferring data between computers based on a mutually agreed-upon standard.
- Exchanging electronic messages following general or standardized protocols.
- Transmitting texts electronically via the internet or other technologies such as telex and fax.

Some legal scholars assert that while the UNCITRAL Model Law on Electronic Commerce does not explicitly define an electronic contract, it does delineate the methods used to form such contracts (Khan & Kishore, 2023).

Directive 97/7/EC, enacted by the European Parliament on May 20, 1997, addresses distance contracts and consumer protection. It defines a distance contract as "any contract concerning goods or services concluded between a supplier and a consumer under an organized distance sales or service-provision scheme run by the supplier, who, for the contract, makes exclusive use of one or more means of distance communication up to and including the time at which the contract is concluded" (Steennot, 2013). Additionally, it defines means of distance communication as "any means which, without the simultaneous physical presence of the supplier and the consumer, may be used for the conclusion of a contract between those parties" (AlKhalidi, 2009). This directive explicitly includes electronic contracts within its scope of distance contracts, urging EU Member States not to obstruct electronically regulated contracts and to facilitate their conclusion without hindrance or the need for direct human interaction.

The definition of an electronic contract can be derived from the nature of the legal relationship between the parties involved. Some experts define it in technical or technological terms, referring to it as an intelligent agent. This agent demonstrates a high level of intellectual capability to adapt to and manage the complexity of electronic commercial transactions. Furthermore, it efficiently condenses extensive,

time-consuming contracts into simplified electronic transactions, maintaining a comprehensive record of all negotiations communicated and enforced throughout the contract (Ko lvart, Poola, & Rull, 2016).

The uniqueness and privacy of electronic contracts stem from their method of formation. The convergence of offer and acceptance in these contracts occurs between parties who are not physically co-located; instead, the contract is formed remotely. Modern technology facilitates the expression of intent, with the entire process integrated into the digital sphere, encompassing all aspects of the agreement (Hassan, 2008).

Consequently, an electronic contract, also referred to as a smart contract, is fundamentally an agreement where the parties exchange offers and acceptances via electronic means, eliminating the need for physical interaction and face-to-face communication. In this context, the technology itself plays a central role in the contract formation process (Karamanlıog lu, 2018). The various definitions, whether legal or jurisprudential, all emphasize the electronic exchange of intentions. This exchange is facilitated under specific conditions and within the framework of the electronic environment in which it occurs.

The Characteristics of an Electronic Contract

An Electronic Contract is Formed Remotely. This means the parties are not physically present in the same location when concluding the contract, exchanging offers and acceptances electronically over the internet. This type of agreement is often referred to as a "cyber forum" because it is formed between virtually absent parties. Through data exchange via electronic intermediaries, there is an opportunity to establish and verify the identities of the contracting parties (Hegazy, 2010). The international nature of electronic commercial transactions introduces various legal issues, such as the applicable law and the competent court for disputes. However, an electronic contract may still be considered domestic if it lacks international elements(Hassan, 2008).

Electronic Contract is Characterized by the Use of Electronic Means to Conclude the Contract over the Internet

This feature is a key aspect of the specificity of electronic contracts. Although electronic contracts align with the general provisions of ordinary contracts regarding the place of commitment and legal effects, they differ in requiring electronic tools for negotiations, communication, and the exchange of deliberate expressions through the internet. Consequently, electronic contracts cannot be formed without these methods, which facilitate the convergence of the contracting parties' intentions (Obaidat, 2021). The electronic environment, therefore, is both technically and legally conducive to the formation of

of electronic contracts (Hassan, 2008).

Often Electronic Contracts Exhibit a Commercial Consumer Nature

These contracts are commonly referred to as electronic commerce contracts because their nature, particularly in the online domain, is closely tied to electronic commerce activities. The concept of electronic commerce is indirectly defined in Article 1 of the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce, encompassing all commercial activities and related issues conducted, sent, or received through electronic means or similar methods (Khan & Kishore, 2023).

An electronic seller typically operates an electronic platform—a dedicated online space accessible at any time—where they display content related to their business activities. In this context, users, whether natural or legal persons, must act in good faith, with dealings conducted transparently and clearly.

In certain jurisdictions, such as under Article 12/8 of the French Consumer Protection Law issued by Decree No. 741/2001, professionals or business entities are required to provide consumers with all relevant identifying information, such as the company name and nature of the business. This transparency is crucial to protect consumers from fraud or deception by the other party (Al-Fawair, 2014).

Regarding Compliance

According to Al-Fawair (2014) Regarding compliance has significant positive relationship. Electronic payment methods have replaced traditional cash in transactions, reflecting advancements in e-commerce and the growing use of digital transactions (Albalawee, 2024). Prominent forms include electronic money transfers, where banks transfer funds between accounts via electronic clearing with automated customer approval. Electronic banking, including mobile banking, allows customers to conduct transactions using services like voice-based interactions and private PINs, enhancing the ease of digital money transfers (De Luna et al., 2019). Additionally, clearing services facilitate financial transaction settlements online, where customers provide account and payment details for execution through automated systems (AlMousawi & Al-Shammari, 2014).

Electronic Contracts Distinctive Basis from Other Contracts

The electronic contract, or e-commerce contract, is not the sole contract formed within the digital environment, as there are other agreements entered into within this sphere, often interconnected with the electronic contract. We will now examine the distinguishing features that set the electronic contract apart from other contracts.

Distinguishing Between the Electronic Contract and the Contract Concluded by Phone

Contracts can be oral or written, but when concluded via phone, they are typically oral due to geographical distance. This contrasts with electronic contracts, where the offer and acceptance are often in written form, electronically. Notably, this writing is electronic (Al-Sarayrah, 2009). However, oral agreements through technology (e.g., Skype, chat) are also possible. In e-commerce contracts, there is no traditional faceto-face meeting; the environment is virtual, without physical boundaries (Zennyo, 2020). Parties may be in different locations, even with a time difference between them. Contracting via phone involves parties present in terms of time but absent in terms of location, akin to remote contracts. In this sense, e-contracts are characterized by their virtual nature, unlike traditional contracts involving face-toface meetings (Dudin, 2006).

Distinguishing Between the Electronic Contract and Telex

Telex, an instantaneous communication method, provides substantial verification assurances, ensuring addressee identity, as well as information confidentiality and security. Telex produces printed paper outputs on specialized machines, allowing for document preservation, albeit without the capability to transmit graphics, images, and signatures (El-Tahami, 2008). Contracting via telex may share similarities with an electronic contract in its legal nature. However, a notable distinction lies in the fact that messages sent over the Internet or via email need not be printed for recipient comprehension. Such messages can incorporate images, audio files, or text (Dudin, 2006).

Distinguishing Between the Electronic Contract and Television Contract

In a television contract, there often exists a unilateral contract arrangement, devoid of direct interaction between the involved parties. The offeror conveys their intent to contract either through telephone communication or by dispatching a message to a designated address specified by the accepting party, primarily aimed at distributing the offered products, goods, and marketing services (Bawono, 2020).

Conversely, electronic or smart contracts are distinguished by the interactive engagement between the contracting parties within a virtual contractual domain facilitated through the Internet or online platforms (Nuredini & Dodevska, 2020).Contracting via television typically involves both parties being present concurrently in terms of time, with no temporal gap between the offer and acceptance. This mode of contracting is conducted remotely due to the absence of physical proximity between the parties. There exists a potential similarity between electronic contracts and television-based contracts when contracting occurs through a website, presenting goods via images, enabling consumers to make informed decisions.

Legal scholars posit that the principal distinction between internet-based contracting and television-based contracting lies in the manner of offer and acceptance. In internet contracting, both offer and acceptance occur through the same website, whereas in television contracting, an additional device is required to receive the acceptance (Alan, 2002).

Electronic Contracts Have an Absolute Peculiarity in the Domain of Evidence, Enforceability, and the Validity of Electronic Signatures

Electronic contracts present distinctive challenges regarding their evidential nature. They rely on electronic records, signatures, and documents as evidence of the parties' rights, unlike traditional contracts, which are based on physically signed written documents. Consequently, establishing the validity of electronic signatures is crucial (Wardani & Afriansyah, 2020).

In the realm of electronic contracts, the concept of writing has evolved from physical to electronic forms, with data messages playing a vital role in e-commerce transactions. Data messages serve as written communications stored electronically for proof and evidence purposes. This is articulated in Article 6 of the UNCITRAL Model Law on Electronic Commerce, which validates data messages as meeting the requirement for written information (UNCITRAL, 1996).

Moreover, Egyptian Law No. 15 of 2004 defines electronic writing in Article 1(a) as letters, numbers, symbols, or marks stored on electronic, digital, optical, or similar media, serving as evidence in electronic contracts.

Research Methods

This study adopts a descriptive approach to investigate electronic contract laws within Jordanian

legislation. It aims to provide a detailed exploration of electronic contracts, including their formulation, configuration, and associated legal obligations. The study relies on secondary descriptive data gathered from various sources such as books, websites, articles, and official sources. A simple content analysis technique is employed to analyse the collected data, with the main findings presented in the results and discussion section.

Results and Discussion

In this section, we will initially discuss the methods of electronic contract formation, followed by an examination of the structure of electronic contracts, and finally, their significant applications in both commercial and civil contexts.

Means of Electronic Formation

Participants engaging in electronic transactions and e-commerce necessitate a method that aligns with the dynamics of these transactions. The prevalent trend leans towards the utilization of email and electronic data interchange systems, which have become integral components within the domain of electronic transactions, particularly electronic contracts. The surge in electronic commerce post the digital revolution underscores the importance of adapting to the era of instantaneous communication, eradicating temporal and spatial limitations and enabling instantaneous contracting across various global locations. Consequently, the internet and computers have emerged as pivotal tools for conducting electronic business activities. Hence, we will explore the key electronic mechanisms contributing to the efficacy of transactions in electronic commerce, encompassing personal computers, telex, and fax.

Computer: The term "computer" denotes a configuration of electronic circuits engineered to manipulate data in an interconnected manner, facilitating rapid and precise information processing and retrieval. Under Article 2 of the Jordanian Electronic Transactions Law No. 15 of 2015, an "electronic information system" is defined as a collection of programs and tools designed for the electronic creation, transmission, delivery, processing, storage, management, or display of information. Through the utilization of personal computers connected to the internet, individuals can engage in electronic commercial transactions, thereby establishing legal obligations for both contracting parties.

Telex: This apparatus transmits information by printing and directly dispatching it to designated recipients. Notably, there may exist a temporal discrepancy between the sender and recipient, where the message is promptly transmitted but may not be immediately read or responded to. Intentions expressed

through telex are in written form, proving to be instrumental in facilitating commercial transactions, despite the temporal lag.

Fax: Fax machines transmit information as exact reproductions, whether handwritten or printed, to receiving fax devices. Here, the temporal disparity between sending and receiving communications is evident, and fax machines are renowned for their swiftness in document delivery and user-friendliness. It is noteworthy that online contracting parallels fax transmissions when documents are dispatched via computers, albeit with a slight variation in expressing intent. Through computers, the process is instantaneous, eliminating waiting times inherent in fax transmissions. This is corroborated by the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce (1996), General Assembly Resolution 51/162, paragraph 148, based on committee reports(Al-Ajouli, 2002).

Configuration of the Electronic Contract

The formation of an electronic contract necessitates the same elements as any other contract, comprising offer, acceptance, subject matter, consideration, and conditions stipulated by the liabilities of the contracting parties. Nevertheless, it distinguishes itself from traditional contracts by being established without the physical presence of the involved parties during its formation. Each party may reside in disparate geographic locations. In electronic contracting, the absence of physical proximity during contract formation implies that the parties are not assembled in a singular physical location.

Electronic Offer: An electronic offer parallels a traditional offer in requiring clarity, specificity, and irrevocability. The offeror's intention to engage in a contract must beevident upon the offeree's acceptance. If the offeror conditions their offer on nonbinding terms until acceptance, it constitutes an invitation to contract rather than a valid offer. Electronic offers are frequently directed towards specific individuals and commonly transmitted via email or other electronic communication platforms, particularly evident in e-commerce websites. The efficacy of an electronic offer hinges not solely on its issuance but also on its dissemination to the public via the Internet or electronic communication channels. Hence, an offer's validity is contingent upon its communication to the offeree. Electronic offers often transcend national borders, facilitated by electronic means across international telecommunication and information networks, leveraging the global accessibility and connectivity inherent in the Internet.

Electronic Acceptance: This component signifies the offeree's consent to the contract and is issued by the party to whom the offer was directed. It must be explicit, unconditional, and devoid of any stipulations (Adler, 2006). Electronic acceptance constitutes the second essential element in contract formation, representing a clear and irrevocable indication of the offeree's intention to embrace the offer, thereby establishing the contract. Electronic acceptance aligns with the traditional definition of acceptance, which entails the unequivocal manifestation of the offeree's intent. Typically executed through electronic means via the Internet, electronic acceptance adheres to the same principles and regulations governing traditional acceptance while possessing distinct attributes inherent to its electronic format (Basyouni, 2009).

Applications of Electronic Contracts in Civil and Commercial Matters

We will elucidate the paramount technological applications pivotal in delineating electronic contracts in both commercial and civil spheres, facilitating the realization of the parties' intended legal ramifications. Our examination will encompass contracting via websites on the Internet, contracting through email correspondence, and contracting via discussion forums and communication platforms.

Contracting through Websites on the Internet

The Internet serves as an expansive platform for information dissemination, interconnecting millions of personal computers worldwide. Through telephone lines or satellites, this network enables users to exchange information, engage in contracts, communicate, and foster connections. Various electronic communication methods, such as Electronic Data Interchange (EDI), email, fax, and Electronic Funds Transfer (EFT), facilitate interactions on the Internet. Renowned for its accessibility and inclusivity, the Internet operates on a cooperative principle, devoid of individual ownership, and open to all. Commonly known as the World Wide Web, this network allows users to explore diverse websites, access information, and engage in contractual agreements with merchants offering goods or services. Each website boasts a distinct address akin to a physical location, granting users entry upon modification of the address. Once accessed, users can navigate through different pages, gathering pertinent information and initiating contractual arrangements with vendors (Mujahid, 2000).

Contracting via Email (E-mail): Email, a prevalent electronic communication method, facilitates the exchange of written messages and documents among interconnected devices via the information network. It leverages the internet as a virtual mailbox, enabling users to send electronic messages, including files and images, to recipients worldwide swiftly and inexpensively.

Operating seamlessly around the clock, email records the time and date of messages sent and received, ensuring efficient communication without constraints of holidays. This technology allows users to express their intent to enter into contracts and receive similar communications from others, all within seconds. Accessible through email software installed on computers, email stands out as a widely utilized method for rapid, efficient communication in today's digital age.

Dialogue and Communication Forums (Chat and Video): Individuals utilize specific internet programs for chatting and discussions to engage in contracting discussions with others sharing similar interests or offering desired products or services. Through these electronic forums, users negotiate terms and conditions, eventually formalizing agreements once a consensus is reached. This method, commonly used for purchasing, selling, and entering civil and commercial contracts, facilitates direct conversations via cameras and real-time video, proving highly effective in business communication.

Regarding rescinding electronic commercial contracts, some argue that ecommerce legislation provides consumers the right to rescind contracts under certain conditions, allowing the consumer, considered the weaker party, to change their mind. This provision aims to establish a fair balance between consumers and merchants, granting consumers a reasonable period to terminate contracts if necessary.

Legal Obligations to Implement: E-commerce transactions conducted over the Internet frequently involve parties from diverse geographical locations, necessitating the application of the law intended by the parties involved, provided it does not compromise consumer protection rights guaranteed by the consumer's place of residence. This approach aims to maintain a fair balance between the parties.In contractual agreements, parties often pre-determine the governing law in case of disputes. International e-commerce regulatory bodies have endeavoured to establish model regulations to govern and streamline online commercial activities. Additionally, electronic arbitration, which eliminates the need for physical presence during dispute resolution, merits discussion. This method allows proceedings to be conducted via telecommunications channels, including phone or satellite, document exchange via email, and communication with experts through electronic networks.

Summary of the Study

This study has achieved its principal aim of elucidating electronic contracts within the framework of Jordanian law. Employing a descriptive approach, it collected secondary data from various sources to analyse the prevalence and impact of electronic commerce, particularly emphasizing the role of the Internet and email technology. The findings underscored the significance of electronic means in facilitating commercial transactions, wherein parties coordinate offers and acceptances electronically, either through written or verbal expressions using advanced electronic tools. This synthesis contributes both theoretically and practically to understanding electronic contracts, emphasizing their close association with the Internet and adherence to legislative protocols and formalities.

Implications and Contributions of the Study

Every research endeavour aims to yield valuable insights that contribute to both empirical understanding and practical application. Similarly, the exploration of electronic contracts within the legal framework of Jordan holds significant implications for the modernization of legal systems and adaptation to the digital age. As Jordan seeks to align its legal structures with international norms and embrace technological progress, a nuanced comprehension of electronic contracts becomes essential. Such comprehension not only informs policy formulation but also fosters innovation and legal predictability in electronic transactions, thereby stimulating commercial expansion and economic prosperity within the nation.

Furthermore, this study has unearthed certain limitations within Jordanian law that hinder its ability to fully encompass the multifaceted nature of electronic contracts. Addressing the temporal and spatial aspects of electronic contract formation within the Jordanian Electronic Transactions Law, rather than relying solely on general principles of civil law, is imperative. Additionally, concerted efforts from government and judicial authorities are required to conduct training courses and seminars for Jordanian judiciary members, ensuring they remain abreast of the latest advancements in various technological domains.

Limitations and Future Suggestions

In addition to the significant contributions made by this study, certain limitations offer avenues for future research to further enhance the breadth and depth of understanding in this area. Firstly, this study exclusively focused on electronic contract laws within the context of Jordanian legislation, neglecting the exploration of other countries' legal frameworks pertaining to electronic contracts. Future studies could overcome this limitation by investigating and comparing electronic contract laws across various jurisdictions.

Secondly, this study adopted a simple descriptive approach and relied solely on secondary data sources. To provide more comprehensive insights, future research could employ a more robust research methodology, such as exploratory or explanatory approaches, targeting specific populations of interest. This would offer new perspectives and deeper insights into electronic contracts in Jordan and other relevant jurisdictions.

Furthermore, future studies could explore innovative advancements and radical updates in judiciary and legislative regulations related to electronic contracts. By assessing these developments, researchers can contribute significantly to the empirical literature and provide valuable insights into the evolving landscape of electronic contract law.

R*eferences*

Adler, K. A. (2006). Intellectual Property Licensing: Forms and Analysis. Law Journal Press, New York.
Al-Ajouli, A. K. (2002). Online Contracting: A Comparative Study. Amman, Jordan, Legal Library.
Al-Fawair, A. M. (2014). E-Contracts, Willing Agreement. Dar Al-Thaqafa.
Al-Khalidi, I. (2009). E-Arbitration. Dar Al-Nahda Al-Arabia, Cairo.
Al-Mousawi, N. K. I., & Al-Shammari, I. K. M. (2014). A Legal System for Electronic Money. Babylon University Journal, 22(2), 264-285. https://www.iasj.net/iasj/article/88038
Al-Sarayrah, M. A. (2009). The Legal Framework of Contracts Concluded via Electronic Communication Means, A Study in Jordanian Legislation. Damascus University Journal of Economic and Legal Sciences, 25(2).
Al-Zawahreh, M. M., Alghathian, G. A., & Al-Lasasmeh, M. R. (2024). Consumer's Right of Withdrawal in E-Commerce Contracts: A Comparative Study of the Jordanian Civil Law. Pakistan Journal of Criminology, 16(2), 1081-1094. https://doi.org/10.62271/pjc.16.2.1081.1094
Alan, R. M. (2002). Expressing Will via the Internet and Proving E-Contracts. Law Journal, Kuwait University, 26(4), 229-294. https://doi.org/10.34120/0318-026-004-007
Albalawee, N. (2024). E-Contracting within Jordan's Legal Framework. Pakistan Journal of Criminology, 16(1), 331-343. https://doi.org/10.62271/pjc.16.1.331.343
Alsheyab, M. S. A. (2023). Legal Recognition of Electronic Signature in Commercial Transactions: A Comparison Between the Jordanian Electronic Transactions Law of 2015 and the United Arab Emirates Electronic Transactions and Trust Services Law of 2021. International Journal for the Semiotics of Law-Revue internationale de Sémiotique juridique, 36(3), 1281-1291. https://doi.org/10.1007/s11196-022-09967-6
Arabi, O. (2021). Studies in Modern Islamic Law and Jurisprudence. Brill. https://doi.org/10.1163/9789004480704
Basyouni, A. (2009). Online Sales and Leasing and Opening E-Stores. Ibn Sina Library, Cairo.
Bawono, B. T. (2020). The Validity of Electronic Contracts in Software Applications. Jurnal Akta, 7(1), 446407. https://doi.org/10.30659/akta.v7i1.10556
De Luna, I. R., Lie bana-Cabanillas, F., Sa nchez-Ferna ndez, J., & Mun oz-Leiva, F. (2019). Mobile payment is not all the same: The adoption of mobile payment systems depending on the technology applied. Technological Forecasting and Social Change, 146, 931-944. https://doi.org/10.1016/j.techfore.2018.09.018
Dudin, B. (2006). The Legal Framework of Contracts Made over the Internet (1st ed.). Dar Al-Thaqafa, Amman.
El-Tahami, S. (2008). Online Contracting - A Comparative Study. Legal Books.Hassan, A. A. H. (2008). Satisfaction in E-Contracts via the Internet. Dar Al Nahda Al Arabiya.
Hegazy, M. A. M. (2010). Expressing Will via the Internet and Proving E-Contracts. Dar Al-Fikr Al-Jamei, Alexandria.

Karamanlıog lu, A. (2018). Concept of smart contracts–A legal perspective1. Kocaeli Üniversitesi Sosyal Bilimler Dergisi, (35), 29-42. https://www.acarindex.com/pdfler/acarindex-1191-4899.pdf
Khan, B., & Kishore, K. (2023). Mandatory Uncitral Model Laws: An Anlysis. In Policies, Practices, and Protocols for International Commercial Arbitration (pp. 91-100). IGI Global. https://doi.org/10.4018/978-1-6684-4040-7.ch004
Kim, J.-N., & Park, J.-R. (2014). Study on the Electronic Contract. Journal of The Korea Society of Computer and Information, 19(6), 129-138. https://doi.org/10.9708/jksci.2014.19.6.129
Ko lvart, M., Poola, M., & Rull, A. (2016). Smart Contracts. In T. Kerikma e & A. Rull (Eds.), The Future of Law and eTechnologies (pp. 133-147). Springer International Publishing. https://doi.org/10.1007/978-3-319-26896-5_7
Mujahid, O. A. A.-H. (2000). Specifics of Online Contracting. Dar Al-Nahda Al-Arabia.Nuredini, B., & Dodevska, V. P. (2020). Legal Aspects of Electronic Contracts. UBT International Conference, 171. https://doi.org/10.33107/ubt-ic.2020.256
Obaidat, I. M. (2021). E-Commerce Regulations. Dar Al-Thaqafa for Publishing and Distribution, Amman, Jordan.
Sadual, M. K. (2021). Electronic Contracts: Legal Issues and Challenges. International Journal of Reserach and Analytical Review, 8(3), 793-798. https://www.ijrar.org/papers/IJRAR21C2209.pdf
Steennot, R. (2013). Consumer protection with regard to distance contracts after the transposition of the Consumer Rights Directive in Belgium and France. European Consumer Law Journal, (3-4), 415-458. https://biblio.ugent.be/publication/4233862/file/6807506
Toubat, H. S., Halim, R., & Magableh, N. (2020). The Impact of Technological Development on Legal Rules: A Case Study of Jordan. Journal of Critical Reviews, 7(8), 1574-1579. https://doi.org/10.31838/jcr.07.07.01
Van Veldhoven, Z., & Vanthienen, J. (2022). Digital transformation as an interactiondriven perspective between business, society, and technology. Electronic Markets, 32(2), 629-644. https://doi.org/10.1007/s12525-021-00464-5
Wang, X., & Xu, F. (2023). The value of smart contract in trade finance. Manufacturing & Service Operations Management, 25(6), 2056-2073. https://doi.org/10.1287/msom.2022.1126
Wardani, N. K., & Afriansyah, A. (2020). Indonesian legal challenges regarding electronic contracts in international trade. In 3rd International Conference on Law and Governance (ICLAVE 2019) (pp. 23-30). Atlantis Press. https://doi.org/10.2991/aebmr.k.200321.004
Yuri, T., Nikolai, K., Fatima, T., & Sayana, B. (2021). Law and Digital Transformation. Legal Issues in the digital Age, (2), 3-20. https://cyberleninka.ru/article/n/law-and-digital-transformation
Zennyo, Y. (2020). Strategic Contracting and Hybrid Use of Agency and Wholesale Contracts in E-commerce Platforms. European Journal of Operational Research, 281(1), 231-239. https://doi.org/10.1016/j.ejor.2019.08.02.

Digital Human Rights in Jordanian Legislation and International Agreement

Fahad Yousef Al-Kasassbeh1*
Faculty of Law, Amman Arab University
Sadam Mohammad Awaisheh2
Faculty of Law, Al-Ahliyya Amman University, Amman, Jordan
Mohammad Atef Odeibat3
Faculty of Law, Al-Ahliyya Amman University
Salah Mohammad Aboudi Awaesheh4
Student in Commercial Law at Ain Shams University, Cairo, Egypt
Lana Al-Khalaileh5
Faculty of Law, Applied Science Private University, Amman, Jordan
Manal Al-Braizat6
Women Police Command

ABSTRACT

In the contemporary era characterized by rapid advancements in digital technology, concerns about online security and hacking underscore the urgent need for an effective legal framework to address these threats. Consequently, the promotion of digital humanrights has become a priority for both national and international legislation, encompassing freedoms related to communication, knowledge sharing, opinion expression, privacy and data protection, and equitable access to communication infrastructure and services. Nevertheless, emerging challenges include the exploitation of personal data by major technology corporations and the monetization of data for commercial or security purposes. This study examines international agreements and domestic laws to uphold digital human rights, employing a legal qualitative approach with data sourced from online platforms and relevant legal texts, followed by content analysis. The findings from this study underscore that digital rights are integral to the broader spectrum of human rights and freedoms, and are fundamentally embedded in the digital realm. The concept of "digital rights" emerged concurrently with contemporary human rights discourse, with international organizations advocating for their recognition. It is incumbent upon governments to acknowledge, protect, and ensure these rights impartially. However, digital rights face complex challenges that span legislative, strategic, and technical domains. Regulatory mechanisms are crucial in upholding these rights while addressing societal concerns such as public order and morality.

Keywords: *Digital Rights, International Conventions, Protect Morals, Information Revolution.*

1. INTRODUCTION

The ongoing advancement of digital technology presents numerous transformation challenges for societies, impacting various facets of human life, including economic, social, and cultural domains. According to a report published in January 2024, approximately 5.44 billion people globally use the internet (Statista, 2024), underscoring the crucial role of digital technology in the contemporary era. This phenomenon has arisen from the current information revolution, driven by cutting-edge technology

in the contemporary era. This phenomenon has arisen from the current information revolution, driven by cutting-edge technology that facilitates the transfer and processing of information. Consequently, digital technology has become a pivotal and influential factor across all dimensions of social, economic, cultural, and scientific life, firmly integrating into our daily routines (WSIS, 2003).

Digital technology has significantly enhanced global human awareness by providing unprecedented access to knowledge and fostering scientific and cognitive advancements. This digital revolution has become a critical demand in the media landscape of the virtual space era. As of early 2020, global platforms have faced intense scrutiny due to escalating privacy concerns and increased advocacy for digital human rights (UN, 2004). In today's digital age, internet access is considered a fundamental human right, prompting various issues related to digital and human rights. Many countries have implemented legal frameworks to guarantee internet accessibility. For example, in 2020, the European Union outlined its five-year agenda with a focus on trust as a priority. This initiative aims to foster a secure technological environment, ensuring users can interact with data safely. Consequently, digital human rights have become essential in meeting the basic needs of individuals amidst the extensive openness in the "information and communication technology (ICT) sector."

In the contemporary digital era, the designation of the Internet as a human right underscores the significance of digital human rights, affirming that internet access is a legally protected right in various jurisdictions. Governments and regulatory bodies are committed to fostering a secure technological environment that facilitates user interaction with data. Consequently, digital human rights are integral to addressing fundamental needs in the context of the extensive advancements in information and communication technology (Gaitas, 2021). As the Internet has evolved into a global service, the issue of digital human rights has emerged as a recent and dynamic concern, evolving in tandem with ongoing technological progress. International human rights organizations play a crucial role in advocating for the protection of these rights and urging states to formally recognize digital rights. This advocacy is essential in the digital age to ensure the safeguarding of individuals' and users' digital rights.

The research problem is rooted in the novelty of establishing and grounding digital rights. This study emphasizes the importance of state and governmental recognition of digital rights, evaluating the alignment of international treaties with the approval of these rights in the digital age. Digital rights have evolved into a broad platform for expression and are now recognized as fundamental human rights, integral to modern human existence. The primary research question addressed is: What are the forms of digital rights individuals seek to obtain and their legal foundations? To answer this question, the research pursues several objectives: (a) To explore the legal basis for digital human rights in Jordan, (b) To

evaluate efforts contributing to the establishment of digital human rights, (c) To examine international agreements, treaties, and covenants that support and promote digital human rights, and (d) To investigate national legislation supporting digital rights and associated regulatory restrictions.This research holds both practical and theoretical significance. The theoretical importance stems from the crucial need to address human rights in the digital age. As digital technology offers substantial benefits and plays a pivotal role in human rights and development, its impact cannot be overlooked. The rapid advancement in human rights, particularly with the emergence of the fourth generation of human rights, highlights its integration into the international human rights legal framework. This research contributes to understanding how these evolving digital rights intersect with established human rights principles, underscoring their critical role in contemporary legal and social contexts. The practical significance of this research lies in addressing the relative scarcity of studies and research in the field of digital human rights. By advancing this research, we aim to provide valuable support to decision-makers in recognizing and protecting digital rights, both nationally and globally. This research seeks to inform policy development and implementation, ensuring that digital human rights are adequately safeguarded in the evolving technological landscape.

Literature Review

Gaitas (2021), in his study explored the concept of digital human rights, highlighting that the extensive use of the internet necessitates the development of crucial laws and regulations to protect users' data privacy rights. Building on this foundation, the current research delves into additional topics, including the restrictions on digital rights and the key factors contributing to the recognition of these rights. Kamal and Taha (2023) addressed digital rights, focusing specifically on privacy rights in the digital age and the mechanisms for protecting these rights through international conventions. In contrast, the present study aims to identify various types of digital rights, their legal foundations and characteristics, and the international efforts, agreements, and treaties that have advanced the recognition of digital human rights. Additionally, while Bashikh (2017) examined public rights and freedoms within the digital domain and the risks associated with internet misuse, the current study expands on this by also discussing international initiatives and legal frameworks that support the recognition of digital human rights.

The Theoretical Rooting of the Principles of Digital Human Rights

The theoretical framework for digital rights centres on defining their legal scope, identifying their characteristics, and establishing their legal basis. The evolution of the human rights movement has progressed from traditional intellectual and philosophical concerns to a broader focus. Various legal

frameworks and efforts at national, regional, and international levels have significantly contributed to the development and refinement of concepts related to fundamental human rights.

The Nature of Digital Rights

This topic is examined from two perspectives: the first addresses the linguistic meaning of digital rights, breaking down the term into its components—"digital" and "rights"—to clarify its definition. The second perspective explores the terminological concept of digital rights, providing a more nuanced understanding of the term in its specific context.

The Linguistic Meaning of Digital Rights

The term digital is defined as the use of a system for transmitting or receiving significant information represented as a series of zeroes and ones, indicating the presence or absence of an electronic signal. Conversely, right is defined as "a moral or legal claim to possess or obtain something or to act in a specific manner." According to Merriam-Webster, digital refers to "a thing of, relating to, or utilizing devices constructed or functioning by the methods or principles of electronics," while right is described as "something to which one has a just claim."

The Theoretical Definition of Digital Rights

Human rights are intrinsic entitlements that allow individuals to fully realize their qualities, intelligence, talents, and self-awareness while addressing their spiritual needs. These rights stem from the growing demand for a life where respect and protection for the inherent dignity and self-worth of every individual are assured. They represent universal legal safeguards designed to protect individuals and groups from actions or omissions that infringe upon basic freedoms, entitlements, and human dignity.

The literature on digital rights presents varied definitions, often reflecting the term's emerging nature. Fathy (2018) defines digital rights as the entitlement of every individual to access, use, create, and publish digital content without restriction. This definition associates digital rights with several fundamental rights and freedoms, including freedom of opinion and expression, privacy, the right to knowledge, development, and the freedom to disseminate information. In contrast, Al-Saadi (2019) defines digital rights as the rights to essential benefits derived from services provided by information networks at the international level. This definition emphasizes the need for user security and safety and the provision of basic requirements for accessing these services. However, it primarily focuses on the availability of digital rights, potentially overlooking foundational principles such as privacy, freedom of

expression, and the right to development, use, and innovation. Gaitas (2021) offers a more comprehensive definition, describing digital human rights as those that provide individuals with crucial capabilities for data and information circulation within their environment. This definition also encompasses the ability to communicate within this environment and highlights that digital rights are essential to contemporary life. According to Gaitas, states are obligated to secure and facilitate these rights while avoiding arbitrary impediments to access and use.

The UN Human Rights Council has affirmed that the rights people possess in the physical world are equally applicable in the digital realm. It asserts that these rights must be safeguarded online just as they are offline. Human rights are fundamental freedoms and entitlements that belong to all individuals universally and without discrimination. In a broader sense, the term digital refers to anything that exists in the form of data and encompasses the capacity to utilize technology and communications within cyberspace. Various terms related to digital include digital citizenship, digital transformation, and other concepts pertinent to cyberspace. Digital rights are defined as "those rights that individuals seek to enjoy effectively in the digital realm, facilitated by their knowledge of specific digital skills that enable their participation in the digital society, while ensuring these rights are recognized without undue oppression within this digital environment." The Arab Centre for the Development of Social Media and the Association for Progressive Communication characterize digital rights as an extension of human rights in the physical world, emphasizing that these are rights safeguarded and advanced by laws and international treaties. This research defines digital rights as the rights that enable individuals to connect to the Internet and ensure their protection while engaging with it, whether through sharing, creating, or receiving data.

Research Methodology

This study primarily examines the digital rights of individuals within the framework of Jordanian legislation and international agreements. To achieve this objective, an interpretivist philosophy was adopted due to its exploratory nature, complemented by an inductive approach. Additionally, a descriptive and analytical approach was employed, deemed most suitable for the study's objectives. This approach encompasses the extrapolation and interpretation of international agreements, followed by a detailed analysis after providing a general description. Consequently, a legal research study was conducted focusing on digital human rights within the context of Jordanian and international legislation. Secondary qualitative data for this study were collected from various laws, legislations, and treaties. Additionally, online legal databases and resources, such as WestLaw, LexisNexis, and others, were utilized to gather relevant information. The results are organized into three sections.

The first section addresses the legal foundations and characteristics of digital rights. The second section examines digital rights within international agreements and discusses international efforts that support their recognition, highlighting the most significant of these rights. The third section focuses on the incorporation of digital rights into national legislation and explores the limitations and restrictions affecting these rights.

Results and Discussion

The Legal Basis for Digital Rights and Their Characteristics

This basis is primarily divided into the following parts:

The Legal Basis for Digital Rights

The United Nations is credited with prioritizing the issue of digital human rights from the outset. It has incorporated a consistent principle in several documents that mandates the protection of internet freedom and communication, advocates for the recognition of digital rights by states, and encourages countries to implement effective measures to uphold these rights.

Human Rights Council Resolution of 2016

In 2016, the Human Rights Council formally recognized digital rights as human rights through a resolution adopted by the United Nations. This resolution affirmed that access to the Internet constitutes a fundamental human right. Although the resolution was supported by the majority of major powers, it faced opposition from Russia, China, Saudi Arabia, India, and South Africa. These countries contested a specific paragraph of the resolution addressing measures to intentionally prevent or disrupt online access and the dissemination of information (Al-Saadi, 2019). The resolution also advocated for the provision and expansion of Internet access, with a focus on addressing gender disparities and enhancing access for individuals with disabilities. It underscored the importance of involving civil society and the technical community in related processes. Furthermore, the resolution acknowledged that a universal and open Internet is crucial for achieving the United Nations' Sustainable Development Goals and its 2030 Agenda (Khalifah, 2012).

19th Article of the Human Rights' Universal Declaration

In its prior resolution, the Human Rights Council built upon an earlier United Nations statement regarding digital rights. This earlier affirmation emphasized the promotion, protection, and enjoyment of human rights on the Internet, asserting that the same rights individuals have offline must be upheld

online, particularly freedom of expression as enshrined in Article 19 of the Universal Declaration of Human Rights (HRC, 2014). It is important to note that such resolutions face significant challenges in passing and implementation. Effective action requires pressing the governments of opposing states and bolstering the credibility of human rights advocates to ensure the recognition and promotion of digital human rights, preventing actions such as internet access restrictions and violations of individual privacy.

The UN High Commissioner for Human Rights also called for the preparation of areport on bridging the digital gender divide from a human rights perspective, involving the participation of states, civil society organizations, and technical and industrial institutions. This report is to be submitted to the Human Rights Council at a later date. Consequently, it can be argued that digital rights have become recognized as fundamental rights by states and organizations, treated as integral to basic human rights. These UN resolutions legalize digital rights and provide the necessary legal foundation to justify their existence.

Characteristics of the Digital Rights

Digital human rights are characterized by several key features, namely:

- Digital Rights are Evolving Rights: Digital human rights are intrinsically linked to the digital revolution. As technology evolves and new applications and practices emerge on the Internet, corresponding digital rights must be identified, protected, and recognized to address these developments (Qashqush, 1992).
- Digital Rights are Legal Rights: Digital rights are classified as legal rights, which are formally adopted and recognized by the law. Legal rights are those established and sanctioned by legal systems, distinguishing them from natural rights. The latter are inherent and not contingent upon legal frameworks, while digital rights fall within the domain of legal rights, derived from and protected by statutory and regulatory measures (Al-Wafa, 1998).
- Digital Rights are Absolute and Unrestricted: Digital rights are inherently free and connected to the World Wide Web. Nonetheless, certain restrictions on digital rights may be imposed to balance the interests of others, uphold public order, or maintain public morals.
- Digital Rights are Newly Established Rights: Digital rights are characterized as part of the fourth and contemporary generation of human rights, emerging in response to the significant technological advancements occurring globally. These rights have become integral to human progress, encompassing both the material aspects of service provision that meet basic needs and the human dimensions related to rights, culture, and education (Al-Saadi, 2019).
- Digital Rights are Integrated Rights: They are not discrete or isolated rights but are interconnected. Access to the Internet enables individuals to obtain data and information, thereby facilitating the

exercise of various rights, including privacy.

● Digital Rights are Universal Rights: The association of digital rights with the World Wide Web has imparted a global dimension to these rights. The widespread availability of the Internet has simplified the fulfilment of human needs related to digital rights, such as communication, publishing, browsing, correspondence, creating blogs, and accessing information. This ease of access is facilitated by the Internet's pervasive reach across the globe.

● Digital Rights are Fundamental Rights: When the Human Rights Council endorsed digital rights, it underscored their fundamental nature, distinguishing them from mere leisure or secondary rights. This designation arises from the fact that digital rights now intersect with all aspects of daily life.

● Digital Rights are an Extension of Human Rights: These digital rights possess a dual nature: they not only support and enhance other human rights but also stand asrights in their own right. Consequently, digital rights have become prominent within the broader framework of human rights deployment, education, and training. They serve as a vital tool for monitoring, documenting, and exchanging data regarding international adherence to these rights.

● Digital Rights are Intrinsic Rights: By acquiring specific skills, individuals can effectively master the use and exercise of digital rights.

Digital Rights in International Conventions and National Legislations

International efforts have played a pivotal role in advancing the adoption of digital human rights, fostering an environment conducive to their development and recognition while maintaining national and global security. This section is organized into two key topics: the role of international agreements in shaping digital rights and the integration of digital rights within national legislation.

Digital Rights in International Conventions

Several factors have played a crucial role in supporting and formalizing digital human rights, contributing to their evolution and recognition as fundamental human rights. These factors include the activities of international organizations and bodies dedicated to information technology. Notably, the Office of the United Nations High Commissioner for Human Rights has acknowledged that the global electronic information network has transformed the human rights landscape. This transformation has enhanced freedom of expression and access to information, enabling individuals to form and voice their opinions and claim various rights, such as the right to a fair trial, freedom of religion, free elections, and decent living conditions.

Advancements in communications technology have significantly enhanced the exercise of freedom of expression, the articulation of opinions, and active engagement in the promotion and consolidation of rights related to thought and conscience. These innovations have created the necessary space for the expression of such rights, facilitating the realization of their underlying legal objectives. The information and technology revolution has also bolstered political rights by providing tools for individuals to engage with politics, monitor political developments within society, disseminate democratic values, and understand political systems that restrict free democratic thought. This has deepened awareness of political rights, including the right to participate in political processes, run for office, engage in political parties, and contribute to the improvement of electoral management, including the implementation of electronic voting systems for polling and counting (Al-Saadi, 2019). Moreover, digital human rights provide a crucial framework for monitoring and documenting violations occurring globally, thereby stimulating the international community to address these issues. The visibility and documentation of such violations through digital platforms can elevate them to matters of public concern, mobilizing global awareness and response.

Efforts and Conventions that Contributed to the Digital Rights Recognition

● The most prominent efforts that have contributed to the recognition of digitalrights include the following:

1. The holding of the "World Summit on the Information Society (WSIS)": The WSIS is recognized as a forum convened by global leaders committed to leveraging the digital revolution in Information and ICT to benefit humanity. Its primary objective is to foster a people-centred, inclusive, and development oriented society where every individual has the right to create, use, share, and access information, thereby advancing sustainable development and enhancing quality of life. Through its resolutions and initiatives, WSIS has played a pivotal role in laying the foundational principles of digital rights, elevating these rights on the international stage, and facilitating the integration of digital rights into the broader framework of human rights and freedoms.

2. In 2011, the United Nations appointed the "Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression," focusing on key aspects of digital rights. The report delivered to the Human Rights Council (HRC) was instrumental in recognizing digital rights and advancing their inclusion in international documents. The Special Rapporteur urged states to ensure the maintenance of internet access, highlighting the Internet's critical role in upholding human rights, addressing inequality, and fostering development.

3. The Creation of the Internet Governance Forum: The IGF aims to facilitate discussions among multiple stakeholders and promote the exchange of experiences and ideas on maintaining the stability of the Internet and ensuring secure and continuous access. The term "multi-stakeholders" refers to the collaborative involvement of various entities in technology issues, driving discussions toward consensus on critical matters related to digital human rights. The most prominent tasks of this forum include:

- Addressing public policy issues pertaining to key aspects of Internet governance to enhance its sustainability, robustness, security, stability, and development.
- Contributing to capacity-building in Internet governance within developing countries and optimizing the use of local knowledge and expertise.
- Assisting in the development of solutions to challenges arising from both the and misuse of the Internet.
- Facilitating dialogue among diverse entities involved in international public policies that impact various sectors related to the Internet.
- Engaging with pertinent intergovernmental organizations and other institutions on issues within their areas of expertise.
- Facilitate the exchange of information and best practices, leveraging the expertise of academic, scientific, and technical communities to enhance understanding and solutions.

The Most Prominent International Conventions and Treaties that Support Digital Rights

Digital human rights have garnered significant global attention, particularly following the Internet revolution and its rapid advancement since 2010. This period marked a profound qualitative leap in information technology. Initially restricted toacademic research, the Internet has evolved substantially, with software advancements and a dramatic increase in global users. The number of Internet users surged from 360 million in 2000 to approximately 2.7 billion by 2013, and further doubled to around 4.5 billion by 2020. Thus, the most significant international conventions that have advanced the recognition and promotion of digital human rights include the following:

APC Internet Rights Charter

The charter sought to advance seven key principles: ensuring universal access to the internet, facilitating access to knowledge, fostering creation and learning, enabling the sharing and communication of critical information, and promoting the effective use of the internet. These principles align with and support the human rights outlined in the Universal Declaration of Human Rights.

WSIS Declaration of Principles – 2003:

Under the auspices of the United Nations and recognizing the profound impact of the Internet and digital technology on various aspects of global life, a coalition of governments, international organizations, and civil society issued a declaration at the World Summit on the Information Society in 2003. This declaration expressed a unified commitment to building a people-centred, inclusive, and development oriented information society. It emphasized the importance of ensuring that every individual has the ability to create, access, use, and share information and knowledge. This declaration highlights the integral connection between the Internet and human rights, particularly as outlined in the Declaration of Principles of the World Summit on the Information Society, which underscores the importance of freedom of expression and the utilization of information technology.

The UN Human Rights Council Resolution No. (13) on the Promotion, Protection, and Enjoyment of Human Rights on the Internet (2012):

The resolution asserts that: (a) The Council acknowledges the global and open nature of the Internet as a catalyst for accelerating development in its various forms and encourages all states to facilitate and promote internet accessibility. International cooperation is also emphasized to support media development and other forms of communication across nations. (b) It is decided that states should be encouraged to promote and protect human rights, particularly integrating the right to freedom of expression on the Internet.

The UN Resolution on the Privacy Right in Current Digital Age (2014):

The resolution stipulates that arbitrary or unlawful surveillance of communications, which infringes upon individuals' privacy rights, undermines the values of a democratic society. Therefore, surveillance of digital communications must adhere to international human rights obligations and be conducted within a legal framework that is publicly accessible, transparent, precise, and free from discrimination.

Declaration of the Global Multi-Stakeholder Meeting on the Future of Internet

Governance "NETmundial" - São Paulo /Brazil 2014:

The meeting reaffirmed the human right to privacy, asserting that no individual should be subjected to arbitrary or unlawful interference with their privacy. It emphasized the right to legal protection against such intrusions and stressed the need to effectively address the challenges posed by modern technology and its rapid advancements, which may potentially lead to illegal or arbitrary violations of privacy rights.

Declaration of Digital Democracy – HRDO Institution (2017):

This declaration addressed ten fundamental rights, namely:

- The right to open internet access.
- The right to unrestricted communications.
- The right to strong social networks.
- The right to share digital TV.
- The right to privacy online.
- The right to use common radio frequencies.
- The right to devices and equipment free from obstructions.
- The right to software free from restrictions.
- The right to public websites/right to a public digital service
- The International Covenant on Economic, Cultural and Social Rights:

Article 15 emphasizes that states should prioritize the establishment of agreements recognizing every individual's right to participate in cultural life. This right includes benefiting from scientific progress, which facilitates the application of technology and other moral interests derived from literacy, as well as scientific and artistic achievements.

The African Declaration on the Freedom and Rights to use Internet (2014):

This initiative centres on establishing principles that guide legislative and policy frameworks related to freedom, governance, and internet rights within Africa. It aims to foster an effective online environment that upholds human rights, thereby contributing to economic growth. It is emphasized across all international conventions and treaties that individuals should fully enjoy their digital rights, free from interference or abuse by any party.

Types of Digital Rights Contained in International Conventions

Among the most prominent documents within this track is the "Declaration of Digital Democracy," published by the Centre for Digital Democracy. This declaration outlines the following digital rights:

The Right to Open Internet Access

The right to access the Internet is increasingly recognized as a fundamental human right, essential for the enjoyment of both offline and online human rights. The Internet serves as a crucial platform for sharing and acquiring knowledge, engaging in social networking, political organization, and participating in economic and developmental activities (Qashqush, 1992). This right ensures that all individuals can

benefit from communication and information technologies, by mitigating barriers related to distance, cost, and accessibility, thus enabling universal usability. The right to access the Internet encompasses two essential dimensions: the provision of necessary infrastructure and the availability of digital content. Governments are tasked with ensuring that internet access is universally available at minimal cost and free from discrimination based on race, colour, sex, religion, political opinion, national origin, or social status. The paper underscores the significance of open, highspeed internet connections and advocates for the principle of universal accessibility, rather than imposing restrictions on access.

Freedom of Expression and Information Rights

Article 19 of the International Covenant on Civil and Political Rights addresses the freedom of expression, stating: "Everyone shall have the right to hold opinions without interference. This right shall include freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing, or print, in the form of art, or through any other media of their choice" (UN Human Rights, 2002). Accordingly, the right to freedom of expression, opinion, and information encompasses the ability to request, receive, and disseminate information and ideas without interference or limitations, ensuring access to a broad range of sources. However, states and governments may impose restrictions on this right to protect the rights of others, as stipulated in Article 19(3) of the International Covenant on Civil and Political Rights. This article specifies that the exercise of these rights may be subject to limitations that are provided by law, particularly to respect others' rights and reputations, and to safeguard national security (UN Human Rights, 2002). The Human Rights Committee has clarified that the concept of public morals can vary across different traditions. Furthermore, the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression has emphasized that any restrictions on this right must adhere to the following criteria:

- To be Legal or Provided by the Law: Signifies that it should be a clearly defined rule, protected by legislation, and publicly accessible.
- Legitimacy: These restrictions must aim to achieve one of the purposes outlined in Article 19(3) of the International Covenant on Civil and Political Rights, which includes the protection of the rights or reputations of others, national security, public order, public health, or morals.
- Necessity and Proportionality: This means that the policies of intergovernmental organizations should allow for non-disclosure only when disclosure would likely cause harm to a legitimate interest.

Accordingly, restrictions on access to information may be imposed only when they satisfy the aforementioned three-part test. The researcher contends that internet users should be able to communicate freely and without obstacles with any device connected to the network, utilize any services, and transfer any data, all without unjustified restrictions imposed by the government.

The Right to Data Protection and Privacy

No one can deny that privacy is a fundamental human right, crucial for preserving human dignity and humanity by ensuring the confidentiality of all aspects of an individual's private life. However, the rapid development in the field of technology has increasingly threatened this right. Therefore, governments must intervene to protect and respect the right to digital privacy. The right to digital privacy is defined as an individual's right to be left alone (Al-Khursan, 2016). It also encompasses the freedom of individuals to choose how they express themselves, their desires, and their actions to others. While various terms may be used, they generally convey the same concept. When discussing the right to privacy, one refers to aspects such as private life, intimate life, or solitude and personal space (Afifi, 2013). This right includes the legal and moral protection of individuals from interference in their personal affairs, including their homes, correspondence, honour, and reputation through direct material means. The right to privacy is defined as "the protection bestowed upon a place, whether public or private, with the emphasis on the individual's state of enjoying legal protection." This concept has its origins in French law, which introduced the term "right to private life," based on the criterion of place, implying that private life occurs behind closed walls. Consequently, digital privacy can be described as the protection of personal data published and circulated through digital means. This encompasses email, bank accounts, personal photos, work information, and all data used during an individual's interaction with the internet.

According to Article 18 of the European Convention on Human Rights (ECHR) of 1950, the first paragraph guarantees respect for private and family life, home, and correspondence for every individual within the territory of any state party to the Convention. The second paragraph of Article 18 prohibits any intervention by public authorities in the exercise of this right by its owner, except as permitted by legislative texts of the respective countries and only to the extent necessary to achieve the purposes for which the intervention is allowed (Harris et al., 2023). The researchers contend that the right to digital privacy encompasses both physical protection, such as the inviolability of domicile and the sanctity of mail, and moral protection, such as the confidentiality of personal conversations and calls.

The Freedom of Association, Peaceful Assembly and Participation

The International Covenant on Civil and Political Rights, specifically in Articles 21 and 22, recognizes the rights to peaceful assembly and association. These rights extend beyond merely receiving and obtaining information and data; they also include the right to actively participate in the process of creating content, forming associations, and engaging in peaceful assembly online. This affirms the right of individuals to select any website, application, or tools they wish to use on the Internet. It also upholds the right to join or form online associations, which may include civil society organizations, religious or cooperative clubs, as well as political parties and trade unions. As previously discussed, it is permissible

to impose certain restrictions on the right to peaceful assembly and freedom of association, provided that these restrictions are justified. States and governments are not obligated to compensate individuals if these rights are restricted without proper justification.

The Right to Encryption

The right to encryption is closely related to the right to freedom of expression andopinion, as it serves as a fundamental tool for safeguarding freedom of expression in the digital age. Encryption ensures that communication data remains unintelligible to anyone other than the intended recipient. This right is defined as the use of symbols and codes not in common circulation, rendering phrases and sentences incomprehensible to unauthorized parties. This research posits that the right to encryption is intrinsically linked to ensuring cybersecurity, which is essential for protecting information and data within cyberspace.

The Right to Access Information

The positive aspect of the digital revolution is reflected in the seamless, crossborder availability of information and data without restrictions. Consequently, the right to access information has emerged as a result of the extensive development of computers, communication networks, and their connection to the World Wide Web (the Internet). This underscores the interconnected nature of digital rights, as it is essential to provide individuals with internet access to obtain information available online (Mathiesen, 2014).

The Right to Digital Security

Digital security is defined as "the set of tools and applications used to protect information on computers and the Internet." This encompasses measures to safeguard internet accounts and files from unauthorized access, interference, and intrusion by external users. Neglecting to provide such protection can result in severe consequences, including data theft, extortion, invasion of privacy, and other cybercrimes with potentially catastrophic effects.

The Right to Incognito (Invisibility)

Users of telecommunications networks have the right to choose whether to be visible during communication or to remain anonymous. This right is crucial for fulfilling personal preferences without disrupting the normal environment. It is widely practiced in electronic interactions conducted through virtual platforms that lack a physical presence. Digital rights, including digital identity, free software, television broadcasting, and common radio frequencies, are dynamic and continuously evolving. As technology progresses, so too do the rights within cyberspace (Rodgers, 2019). It is essential for states

and governments to consistently protect and recognize these rights, as the digital age necessitates increasingly diverse and sophisticated digital human rights.

Protecting digital human rights amidst rapid digital development poses a significant challenge due to the vast amount of information in the digital realm. While technology offers numerous benefits—such as bridging distances, facilitating communication, andreducing costs—these advancements also necessitate the protection of rights, ensuring individuals can effectively exercise them. The launch of the National Strategy for Human Rights in the Hashemite Kingdom of Jordan was a response to the changes imposed by the digital environment on both the theoretical and practical aspects of human rights, including the emergence of digital rights (Al-Khasawneh & Barakat, 2016). These digital rights have become integral to the hierarchy of human needs, reflecting the central role of digital applications in contemporary life.

National Legislation on Digital Rights

The following highlights the most significant local legislation related to digital human rights, even if not explicitly addressed in the legislation:

Jordan Personal Data Protection Law of 2021

This law primarily emphasizes the enhancement of constitutional freedoms and rights within the context of the Jordanian Constitution. It strengthens the Kingdom's position in relation to other nations concerning digital environment regulation and personal data protection (Jordanian News Agency, 1/31/2022). Additionally, the law aims to create a regulatory framework that balances individuals' rights to secure their data with the need for processing and retaining data and information in cyberspace. The Personal Data Protection Law addresses mechanisms for creating a secure and stable cyberspace environment. It outlines the obligations and duties of those responsible for handling and processing personal data, as well as the penalties and sanctions for violations of the law and its regulations (Nemer et al., 2023). This law is inferred to encompass digital rights such as the right to prior consent, the right to object, the right to be forgotten, and the right to conceal one's identity—essential rights for all technology users. Authors believe that this law enhances Jordan's position in the digital environment and represents a positive step forward.

The Jordan Cyber Security Law No. (16) of 2019

The pressing need to codify cybersecurity legislation arose due to the frequent occurrence of cyberattacks and the significant risks they posed across various sectors. Article 2 of the Cybersecurity

Law defines cyberspace as an environment encompassing interactions among information systems, telecommunication systems, data, individuals, and other related infrastructure. The same article also defines cybersecurity as "the measures taken to protect information systems and networks, as well as critical infrastructures, from cybersecurity incidents. This includes the ability to restore them to their operational state following unauthorized access, misuse, failure to follow security procedures, or exposure to deceptive practices that lead to such incidents."

The law aims to protect the Hashemite Kingdom of Jordan from cybercrimes, enhance national capabilities to address threats to information systems and infrastructure, and foster a secure investment environment (Al-Flaieh, 2024). It involves monitoring cyberspace, documenting incidents, implementing national cybersecurity policies, and coordinating efforts to improve security for institutions and individuals. Additionally, the law seeks to respond to cybersecurity incidents and mitigate the resulting damages. The Jordan National Council for Cybersecurity was established in early 2021 under Article 3(a) of Cybersecurity Law No. 16 of 2019 (Thai Netizen Network, 2019).

The Centre aims to build, develop, and organize an effective system to enhance cybersecurity and protect the Kingdom at a national level. The Centre is chaired by an individual appointed through a combination of members from the Ministry of Digital Economy and Entrepreneurship and a royal decree. Additionally, members include representatives from the Jordanian Armed Forces, the Directorate of Public Security,the Crisis Management Department, and the Intelligence Department (Al-Flaieh, 2024). The authors of this paper argue that the mere existence of legislation designed to protect cyberspace from attacks, intrusions, threats, and risks inherently provides special protection for citizens' digital rights. Furthermore, it serves as a tool for monitoring restrictions on digital rights, ensuring that such restrictions are not applied arbitrarily.

The Jordan Cybercrime Law No. (27) of 2015

The Jordanian legislator recognized the need to establish specialized legislation addressing electronic crimes in response to significant global technological advancements. Consequently, this law comprises 18 legal articles, with most of them specifying penalties for actions classified as electronic crimes that impact cyberspace and, consequently, infringe upon digital human rights (Abu-Taieh et al., 2018). Cybercrime is defined as “any act criminalized by laws that attacks material and/or moral conditions as a result, directly or indirectly, of the intervention of information technology.” Cybercrime is also defined as "every act or omission involving the use of technological means that is punishable by law.”

Types of cybercrimes include, for example, email fraud, identity theft, theft of financial data or prepaid card information, cyber-espionage, copyright infringement, and other similar offenses. It is important to note that these types of cybercrimes often involve violations and abuses of citizens' digital rights perpetrated electronically by criminals. Additionally, the Anti-Cyber Crime Unit, a governmental security organization, was established by the Public Security Directorate within the Criminal Investigation Department in 2008. It was subsequently developed in 2015 under the name "The Anti-Cyber Crime Unit." This unit aims to combat electronic crime and raise awareness about its dangers. It operates with a collaborative approach, working with international and local institutions, telecommunications companies, and civil society organizations. This law was enacted to organize and define actions considered electronic crimes, thereby safeguarding citizens' digital rights by criminalizing such behaviours and imposing penalties on any actions that infringe upon these rights, even if those rights are not explicitly enumerated.

The Telecommunications Law No 13 of 1995

This law comprises 93 legal articles that address the responsibilities of the Ministry of Communications, the Telecommunications Regulatory Authority, communication network licensing and renewal, and outlines significant crimes and corresponding penalties. According to Article 4 of Communications Law No., a Commission focusing on Telecommunications Regulations will be established to safeguard the interests and rights of users of communication networks and information technology. The Telecommunications Regulatory Commission is an independent juridical entity with financial and administrative autonomy, responsible for regulating telecommunications and information technology services (Economides, 1999). Its duties and responsibilities include.

:● The Commission regulates information technology and telecommunications services within the Kingdom. It aims to ensure the delivery of high-quality information technology and telecommunications services at reasonable prices,thereby promoting optimal performance in the associated sectors.

● It focuses on developing regulations for the IT sectors within the Kingdom.

● It specifies the minimum level of service quality that licensees must adhere to in order to meet the needs of beneficiaries.

● It protects the interests of beneficiaries and monitors the actions of individuals and licensed entities to ensure compliance with license conditions.

● It stimulates competition in the telecommunications and information technology sectors by leveraging market forces and regulating them to prevent or curtail illegal competitive practices.

The Commission's role is to protect the interests of beneficiaries, particularly those using communication networks. It reviews laws related to cyberspace and the World Wide Web, identifying the digital rights enjoyed by individuals in the Hashemite Kingdom of Jordan. These rights include the confidentiality of financial data, privacy and protection from espionage, copyright protection, personal data protection, and internet usage. Relevant laws include the Jordanian Press and Publications Law and the Jordanian Electronic Transactions Law.

Restrictions on Digital Rights

Governments may impose restrictions on digital human rights under specific circumstances or legal justifications, which can limit their enjoyment. These restrictions might pertain to national security or cybercrimes. Advances in communications technology have enhanced surveillance capabilities, enabling states and governments to intercept communications and collect data more efficiently. The Special Rapporteur on the right to freedom of expression and opinion has noted that the effectiveness of surveillance is no longer constrained by scope or duration. Consequently, digital technologies such as browsers, search engines, and social media are susceptible to mass surveillance and can facilitate such practices

Restrictions Imposed to Protect the National Security of the State

It is argued that the international communications network, the Internet, can be exploited in ways that threaten state security, such as by spreading extremist ideas, encouraging violence, inciting hatred, or exacerbating sectarian strife within societies. The Internet may also be used to discriminate against individuals based on race, religion, gender, colour, language, or cultural and social background. For instance, social media posts targeting the Rohingya community in Myanmar contributed to mass killings and rape in 2017. Human rights investigators have found that Facebook and its news-based algorithms played a role in the spread of hate speech and incitement to violence.

In India, the Information Technology Act of 2008 permits the interception of communications for reasons including, but not limited to, safeguarding the country's sovereignty and security, maintaining friendly relations with foreign nations, preserving public order, or investigating any crime (Halder, 2011). The freedom of information and data flow on the Internet can be exploited to spread rumours and misinformation on issues of public concern, potentially creating security gaps and destabilizing the national security situation. The fight against terrorism and theexploitation of Internet freedom by terrorist groups have led to increased control over these networks at both national and international levels.

The legal basis for these restrictions is grounded in the recognition that states have the right to limit certain rights and freedoms during exceptional circumstances, such as wars, natural disasters, and similar crises. This principle extends to digital rights when there are justifications that threaten national security. Consequently, states may impose greater restrictions on websites that disseminate harmful ideas, support adversarial states in conflict, or provoke civil unrest during periods of internal conflict or civil war.

Restrictions Imposed for Protecting from Cybercrimes

Lawrence Ayres, legal adviser to the European Court of Human Rights, highlights the challenges of digital human rights, noting that modern communication methods pose significant threats to societal security. He points out that the proliferation of internet-related crimes complicates law enforcement efforts to address and prevent criminal activities, underscoring the growing need for effective legal frameworks to safeguard digital rights while combating cybercrimes.

- Drug Trade.
- Money Laundering.
- Trafficking in Slavery, Women and Children.
- Extortion Crimes.
- Fraud, and Other Electronic Crimes

To mitigate and combat cybercrimes, states often assert their sovereignty over websites by implementing mechanisms and restrictions aimed at reducing the negative impacts and risks that threaten social, economic, and political life. Governments may find it necessary to block certain websites when they infringe upon public order and morals or are deemed criminal activities punishable under the Criminal Code. These measures are intended to address and prevent harmful content and activities while balancing the need to protect digital rights. However, there is a risk that these restrictions could be misused to unjustifiably limit individuals' digital rights, without a clear case of necessity. The Human Rights Council and the United Nations Rapporteur have emphasized that the right to freedom of opinion and expression should only be restricted in the narrowest scope and with legal justifications. Researchers argue that there must be regulatory frameworks governing digital rights to balance the public interest, such as preserving national security, with the individual's interest in respecting and exercising their digital rights. Properly delineating and adhering to the legal limits of each interest ensures that they do not conflict but rather complement one another.

Conclusion

The ongoing advancement in digital technology has significantly increased the use of the internet and related technologies. While these technologies have effectively bridged global distances, they have also introduced several challenges, including threats to data privacy and various online risks. Consequently, users have legitimate concerns about potential violations and breaches of their digital rights. This concern arises from the very technological revolution that has facilitated the existence of these rights. This situation has enabled governments to access websites more readily, while also posing growing challenges and imposing restrictions intended to protect national security, public order, public morals, and the rights of others—restrictions that can sometimes conflict with digital rights. One of the primary challenges in this digital age is the lack of comprehensive legal frameworks governing digital rights, given their evolving and interconnected nature. Jordanian legislation also grapples with these issues in ensuring the effective implementation of digital human rights.

Recommendations

This paper concludes with a set of recommendations, including:

- Reformulating digital rights more appropriately, highlighting and organizing them.
- More efforts by various human rights organizations to reduce violations of people's digital rights.
- Raise awareness of digital human rights, and include them in the curricula of schools as well as universities.
- Urging countries around the world to enact national laws on digital rights.
- Tightening control over restrictions and justifications for digital rights, and ensuring their legality.

Research Implications

This study highlights the significance of digital rights as an extension of established human rights and fundamental freedoms. Consequently, contemporary human rights research has increasingly incorporated the concept of digital rights, with international organizations dedicating efforts to supporting these rights. Nonetheless, governments face a substantial responsibility to recognize, respect, protect, and ensure these rights for all individuals without discrimination. This study has been instrumental in shedding light on these issues. However, various challenges persist in the realm of digital rights, encompassing legislative, strategic, and technical obstacles. Therefore, governments across nations can undertake critical measures to enhance the development and enforcement of effective digital human rights. This involves formulating specific legal provisions dedicated to the protection and

enforcement of these rights. Concurrently, policymakers should prioritize the creation and implementation of targeted policies designed to safeguard human rights in the evolving digital landscape.

Limitations and Future Research

This study was confined to an examination of Jordanian legislation concerning digital human rights, which limited its scope. Additionally, the study relied on secondary qualitative data to address its objectives due to constraints in resources. Furthermore, the research does not address the social impacts of online threats or privacy concerns, a limitation stemming from research bias. Future research could benefit from a comparative analysis between common law and civil law jurisdictions with respect to digital human rights. Additionally, collecting primary qualitative or quantitative data in alignment with the research objectives would provide more comprehensive insights. Emphasizing the social impacts of digital threats could further contribute to the advancement and protection of digital human rights.

References

Abu-Taieh, E., Alfaries, A., Al-Otaibi, S., & Aldehim, G. (2018). Cyber security crime and punishment: comparative study of the laws of Jordan, Kuwait, Qatar, Oman, and Saudi Arabia. International Journal of Cyber Warfare and Terrorism (IJCWT), 8(3),46-59. https://doi.org/10.4018/IJCWT.2018070104

Afifi, K. (2013). Cybercrimes, Copyrights and Artistic Works (in Arabic: Jarā'im AlKumpyūtar wa Ḥuqūq Al-Mu'allif wal-Muṣannafāt Al-Fanniyyah). Al-Halabi Legal Publications, Beirut – Lebanon.

Al-Flaieh, M. T. I. (2024). Cybercrime in Jordanian Law. Zarqa Journal for Research and Studies in Humanities, 24(1), 112-122. https://doi.org/10.12816/0061775

Al-Khasawneh, A. L., & Barakat, H. J. (2016). The Role of the Hashemite Leadership in the Development of Human Resources in Jordan: An Analytical Study. International Review of Management and Marketing, 6(4), 654-667. https://www.econjournals.com.tr/index.php/irmm/article/view/2666

Al-Khursan, M. (2016). A Series of Readings on the Violation of Individual Privacy in the Digital Age, 20. Al-Noor Center.Al-Saadi, W. N. I. (2019). Digital Rights and the International Protection Mechanisms Established for Them Within the Framework of International Law. In 4th International Legal Issues Conference-ILIC2019 (pp. 351-368). https://doi.org/10.23918/ilic2019.22

Al-Wafa, A. (1998). The Mediator in Public International Law (in Arabic: Al-Wasīṭ filQanūn Ad-Duwalī Al-'ām). Dār Al-Nahḍah Al-'Arabiyyah, Cairo.Bashikh, M. H. (2017). The Impact of Digital Surveillance on Public Freedoms [Doctoral dissertation, University of Djillali Liberties]. https://www.ccdz.cerist.dz/admin/notice.php?id=000000000000000863687000074

Economides, N. (1999). The Telecommunications Act of 1996 and its impact. Japan and the World

Economy, 11(4), 455-483. https://doi.org/10.1016/S0922-1425(98)00056-5

Fathy, N. (2018). Freedom of Expression in the Digital Age: Enhanced or Undermined? The Case of Egypt. Journal of Cyber Policy, 3(1), 96-115. https://doi.org/10.1080/23738871.2018.1455884

Gaitas, J. M. (2021). Human Rights in the Digital Age and the Information Society. In Forum: The Role of Information and Communication Technology in Supporting Democracy and Freedom of Expression and Opinion: Arab Experiences (pp. 77-92). Kuala Lumpur: Arab Administrative Development Organization. https://search.mandumah.com/Record/123842

Halder, D. (2011). Information Technology Act and Cyber Terrorism: A Critical Review. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.1964261

Harris, D. J., O'boyle, M., Bates, E., & Buckley, C. (2023). Law of the European Convention on Human Rights. Oxford University Press. https://doi.org/10.1093/he/9780198785163.001.0001

HRC. (2014). The right to privacy in the digital age : report of the Office of the United Nations High Commissioner for Human Rights. UN. Office of the High Commissioner for Human Rights. https://digitallibrary.un.org/record/777869

Kamal, B. M., & Taha, S. I. (2023). The Legal Nature of Digital Human Rights and Their Legal Framework. Tikrit University Journal for Rights, 7(3/1), 1-33. https://www.iasj.net/iasj/article/271830

Khalifah, A. A. (2012). International Human Rights Law (in Arabic: Al-Qānūn Al-Dawlī Li-Ḥuqūq Al-Insān).

Mathiesen, K. (2014). Human Rights for the Digital Age. Journal of Mass Media Ethics, 29(1), 2-18. https://doi.org/10.1080/08900523.2014.863124

Nemer, M., Khader, Y. S., Alyahya, M. S., Pirlot de Corbion, A., Sahay, S., & Abu-Rmeileh, N. M. (2023). Personal Data Governance and Privacy in Digital Reproductive,

Maternal, Newborn, and Child Health Initiatives in Palestine and Jordan: a Mapping Exercise. Frontiers in Digital Health, 5, 1165692. https://doi.org/10.3389/fdgth.2023.1165692

Qashqush, H. Ḥ. (1992). Cybercrimes in Comparative Legislation (Jarā'im Al-Ḥāsib AlIlktrūnī fil-Tashrī' Al-Muqāran). Cairo: Dar Al Nahda Al Arabiya.Rodgers, N. (2019). Technoethics and Human Rights: The Metaethical Implications of Crisismapping and the Right to Privacy in Post-Disaster, Post-Conflict Scenarios[Doctoral dissertation, Columbia University]. https://doi.org/10.7916/d8-d06hd475

Statista. (2024). Number of internet and social media users worldwide as of April 2024 (in billions). https://www.statista.com/statistics/617136/digital-populationworldwideThai Netizen Network. (2019). Cybersecurity Act (2019). https://thainetizen.org/wpcontent/uploads/2019/11/thailand-cybersecrutiy-act-2019-en.pdf

UN. (2004). United Nations Decade for Human Rights Education (1995-2004). OHCHR. https://www.ohchr.org/en/resources/educators/human-rights-educationtraining/united-nations-decade-human-rights-education-1995-2004

UN Human Rights. (2002). International Covenant on Civil and Political Rights. Annex VIII. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

WSIS. (2003). Declaration of Principles, Building the Information Society, a Global Challenge in the New Millennium. United Nations Publications, Publications Department, New York. https://www.itu.int/net/wsis/docs/geneva/official/dop.html.

Development and Evaluation on Cybersecurity Behaviour Measurement Instruments for Undergraduate Students

Pannika Ngamcharoen1
Srinakharinwirot University, Thailand.
Naksit Sakdapat2*
University of the Thai Chamber of Commerce, Thailand.
Duchduen Emma Bhanthumnavin3
National Institute of Development Administration, Thailand.

A B S T R A C T

*Technological advancements from past to present have ushered the world into an era of rapid information exchange, establishing a networked system that has transformed information systems and introduced a new realm known as the "cyber world." While this progression has rendered access to information more efficient and convenient, it has concurrently spurred a rise in cyber threats, which have evolved into a societal concern and contributed to other criminal activities. Assessing knowledge for adaptability and promoting cybersecurity awareness is, therefore, an imperative for all sectors. This quantitative research aims to develop and evaluate a cybersecurity behaviour measurement instrument. The sample comprised 820 undergraduate students, with sample size determination conducted via the G*Power programme. The measurement instrument, initially designed by the researchers, encompassed 100 items across four components: 1) Awareness of cyber threats, 2) Knowledge of cyber threats, 3) Experience with cyber threats, and 4) Self-protection against cyber threats. Following expert evaluation, 67 items remained, rated on a 6-point scale. The findings supported all three hypotheses, with 21 items meeting established criteria, enabling the instrument to explain 64.187% of cybersecurity behaviours among undergraduate students and achieving an average reliability score of 0.885. Additionally, the model demonstrated alignment with empirical data, meeting standard indices, including $\chi^2 = 94.392$, $df = 59$, p-value = 0.531, RMSEA = 0.044, CFI = 0.987, TLI = 0.986, and SRMR = 0.062. In conclusion, the researchers recommended potential applications for the instrument in developing social indices and proposed extending it to study causal and effect factors in future research*

Keywords:*Cybersecurity Behaviours, Measurement, Undergraduate Students*

1. INTRODUCTION

Technological advancements, particularly in communication technology, the internet, and wireless electronic devices, have profoundly impacted daily life. These innovations have enhanced convenience in daily activities, enabling clearer and faster communication, simplified access to research information, and seamless social media connectivity. Information and communication technologies have developed rapidly across borders, allowing universal access and benefits. The foundation of modern communication lies in the internet—a vast global network of interconnected systems that facilitates immediate interactions regardless of time or location. However, this infrastructure has also created opportunities for cybercrime, transforming the internet into a platform for criminal activities.

Cybercrime has evolved beyond traditional offences, exhibiting changes in methods, frequency, speed, and scale of impact, with incidents becoming increasingly severe and widespread.

Statistics from the Royal Thai Police on online fraud incidents between January and June 2024 reveal 50,781 cases, with total damages exceeding 40,475 million baht—an average of 224 million baht per day. Among these cases, 19.22% involved individuals aged 18–22, typically late teenagers or undergraduate students(Cheurprakobkit et al., 2023). These figures highlight the increasing impact of cybercrime on individuals' lives and property, with substantial financial losses. Undergraduate students are particularly vulnerable to online fraud due to two main factors: 1) teenagers and students are frequent internet users; and 2) a study by Watts et al. (2017) indicated that Problematic Internet Use (PIU), characterised by difficulties in controlling internet usage and resulting in stress, is more prevalent among students than other population groups.

As information technology advances swiftly to address user needs, it simultaneously gives rise to cybersecurity threats and attacks on information systems across all organisational tiers. The frequency of cyberattacks is escalating, encompassing activities such as hacking into information systems, data theft, social media account impersonation, identity theft for fraudulent purposes, and a range of other cyber threats. Undergraduate students represent a transitional phase into adulthood, with technology integrated into their daily lives. They quickly adapt to technological advancements, which encompass skills in information access, data retrieval, digital media production, and content sharing (Salubi et al., 2018). However, research by Yan et al. (2018) revealed that only 62% of the 462 surveyed students in the United States considered cybersecurity in their decision-making, highlighting aconcerning gap given the potential consequences. Additionally, statistics indicate that individuals aged 18–24, despite being skilled digital users, are more vulnerable to cyber threats than older age groups, such as those aged 25–40, who tend to be more cautious in managing privacy and security. This heightened awareness among older users stems from greater knowledge and experience in recognising digital risks. Furthermore, engaging in digital transactions increases exposure to cyber threats (Debb et al., 2020). Victims of cyber threats often face financial, emotional, and physical repercussions. Thus, individuals with cybersecurity training or previous experiences are generally more aware of these dangers. Ahmad et al. (2021)emphasised the importance of educating students to establish a foundation for future cybersecurity, enabling them to safeguard themselves against cyber threats.

In addition to existing threats, cyber threats have evolved, with cyber-attacks adapting their methods to exploit new vulnerabilities. These contemporary forms of attacks differ from traditional ones, often surprising internet users and hindering their ability to monitor or protect themselves as effectively as

before.

This evolution renders users susceptible to unforeseen harm or damage. Awareness of cybersecurity is essential for preparing and strategizing against such threats, enabling better selfprotection against various risks. Individuals with adequate knowledge are more likely to recognise and anticipate potential harms. Although cyber threats can impact anyone, they disproportionately target university students compared to other age groups. These students, having grown up alongside technological advancements and being accustomed to navigating the digital landscape, face a heightened risk of becoming victims of cybercrime.

A review of the research literature indicates a significant absence of internationally standardised instruments for measuring cybersecurity behaviour among undergraduate students. Consequently, the researchers are motivated to study and develop an instrument specifically designed to assess cybersecurity behaviour within this demographic. The objective is to create a robust assessment tool that undergoes rigorous validation in accordance with stringent academic standards, enabling a comprehensive evaluation of cybersecurity behaviours. Moreover, this instrument will facilitate the screening of students' cybersecurity behaviours, thereby enhancing individual awareness of cyber threats in the future.

Literature Review

Thailand has fully transitioned into a hyper-connected digital society, where electronic devices are essential for daily life, allowing continuous online engagement. The COVID-19 pandemic has accelerated this shift, establishing a new normal for global society. People have become accustomed to conducting various activities online, including work, education, communication, and financial transactions. A study by Bicen et al. (2011) revealed that over 32% of undergraduate students spend more than four hours daily on social media, while Jones et al. (2009) found that 97% of students use the internet for communication. The research also indicated that students seek information related to entertainment, education, and personal matters, with some engaging in illegal activities. Additionally, Sherman et al. (2000)highlighted that technology offers varying benefits based on users' backgrounds and interests; however, hidden dangers exist if users do not exercise adequate caution.

As society adapts to the new normal, many individuals continue to conduct transactions online, leading to an increase in electronic data storage and a heightened risk of data breaches from cyberattacks.

These digital threats, which involve unauthorized access to systems and data, can cause significant harm to individuals and organisations (Chaikin, 2006). With the growing volume and variety of online activities, including shopping and cloud data storage, understanding how to protect oneself from cyber threats has become essential (Zwilling, 2021). Cybersecurity awareness is crucial for compliance with security protocols. Research by Duzenci et al. (2023) indicates that individuals' decision-making processes significantly influence their cybersecurity compliance. Similarly, Quayyum et al. (2021) found that cybersecurity knowledge and awareness greatly affect individuals' preventive behaviours against cyber threats. Increased exposure to cybersecurity information leads to better understanding and safer online practices. However, studies have shown that many individuals, particularly students, often lack basic cybersecurity knowledge and neglect necessary precautions. Russo et al. (2023) noted that students using smartphones frequently ignore cybersecurity risks, while Kovac evic et al. (2023) highlighted that students typically lack awareness of how to protect themselves. A survey by Djeki et al. (2024) revealed low levels of cybersecurityawareness among students and faculty, indicating that foundational knowledge is a critical factor influencing cybersecurity behaviour (Quayyum et al., 2021).

Cyber threats can be categorised into eight distinct areas, as identified by Frisk et al. (2023). These categories include abusive content, which refers to the use or dissemination of false or inappropriate information aimed at damaging the credibility of individuals or institutions, resulting in unrest or the distribution of illegal content. Availability attacks target system functionality, leading to delays or making systems inoperable. Fraud encompasses attempts to gain advantages through deception or fraudulent practices, which may manifest in various forms, such as unauthorised system usage. Information gathering involves efforts to collect data from systems without proper authorisation. Intrusions denote successful unauthorised access to a system, resulting in control being taken by an unauthorised individual, while intrusion attempts are efforts aimed at breaching a system's security. Malicious code or malware refers to software designed to inflict damage on systems, posing a significant threat to information security. Finally, information security concerns the unauthorised access to or alteration of sensitive information.

The concept of cybersecurity encompasses the strategies and actions designed to prevent, mitigate, and minimise risks associated with cyber threats that may compromise the confidentiality, integrity, and availability of information and equipment within an information system. Inadequate cybersecurity measures can leave users vulnerable to harm and expose their personal data to malicious actors. Enhancing cybersecurity can be achieved through various methods, including the use of complex passwords and the installation of antivirus software (Florackis et al., 2023). This perspective aligns with Maslow’s Hierarchy of Needs, particularly the second level, which focuses on the need for safety and

security. In the contemporary context, this includes concerns related to internet safety and social media security; individuals who do not perceive themselves as secure are likely to prioritise safety before pursuing higher-level needs for personal development and well-being (Shi etal., 2021).

The concept of cyber threats encompasses any event or circumstance that poses a risk to the confidentiality, integrity, and availability of information systems or data belonging to individuals, organisations, or nations. These threats primarily stem from cybercriminals or state-sponsored actors (Rahman et al., 2023). Significant categories of cyber threats include ransomware and malware associated with email communications. The concept of cybersecurity is essential for preventing potential threats from cyber disruptions. As the internet is the primary communication channel today, users must adopt strategies to protect against malware, viruses, and other risks that could compromise personal information. Effective cybersecurity requires service providers to implement a comprehensive policy that encompasses network security, including measures to safeguard networks from intruders, maintain application security through regular vulnerability testing and updates, and protect sensitive information by enhancing security measures and restricting access(Azizi et al., 2023).

In the context of individual-level prevention against cyber threats, the protection of personal data and digital assets is crucial to avoid victimisation by cybercrime. Key recommendations for enhancing cybersecurity include: (1) regularly updating software and operating systems, (2) employing antivirus software, (3) creating complex passwords, (4) refraining from opening email attachments from unknown sources, (5) avoiding links from unfamiliar senders or websites, (6) consistently backing up data, and (7) steering clear of insecure Wi-Fi networks, which heighten the risk of cyber-attacks (Safitra et al., 2023).

In the event of a cyber-attack, the following guidelines should be observed: (1) Check for any unidentifiable financial transactions and review credit reports for the emergence of new accounts or loans; (2) Exercise caution against providing sensitive information on websites, via emails, or through social media; (3) If unusual activity is detected, promptly change all account passwords, disconnect all devices, and consult cybersecurity professionals to scan for and eliminate any harmful elements; (4) Report the cyber threat to the appropriate authorities; (5) Conduct a thorough scan of all computer devices to ensure they are free from viruses and operating efficiently; and (6) Disconnect all devices from user accounts and internet networks, and initiate a full system recovery (Darem et al., 2023).

A study conducted by Bidgoli et al. (2016) identified undergraduate students as a high-risk group for cybercrime, primarily due to their pervasive use of technology in daily activities. The research, which surveyed 222 students, found that approximately half had encountered at least one form of cybercrime, with malware, hacking, and scamming being the most prevalent. Additionally, the study indicated that students often learned protective measures and gained cybersecurity knowledge from peers or individuals who had previously been victimized. Complementing these findings,Biese et al. (2024) noted that student victims of cybercrime frequently lack a clear understanding of the extent of the damage and may normalize their experiences due to insufficient knowledge of information networks.

Based on the literature review, a framework for the development and evaluation of measurement instruments is illustrated in Figure 1.

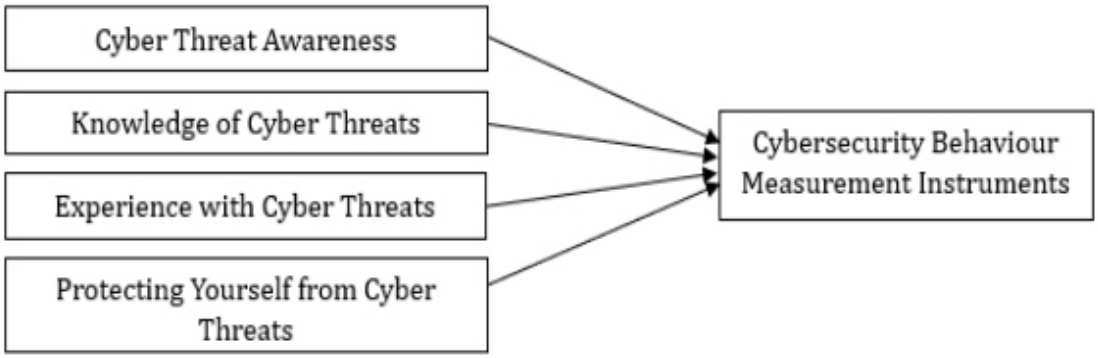

Figure 1: Conceptual Framework.

Methodology

Research Design

This quantitative research study seeks to develop and evaluate a robust measurement instrument for assessing cybersecurity behaviour. The methodology includes item quality testing, exploratory factor analysis, and second-order factor analysis. The results are further validated through confirmatory factor analysis to assess the model's fit with empirical data, employing SEM analysis. This research project has received ethical approval, as indicated by the certification number HREC-130.

Sample

The sample for this research comprises undergraduate students, with the sample size determined using G*Power software. The sampling process involves three stages:

1) Item Quality Testing, utilizing an effect size of 0.75 (medium effect), an alpha level of 0.05, and a power of 0.95 with an allocation ratio of 1. This results in a minimum required sample size of 96 participants based on a t-test for two independent samples;

2) Exploratory Factor Analysis; and

3) Confirmatory Factor Analysis. Following the ten-times rule (Hair Jr et al., 2017; Kock et al., 2018), the necessary sample size is approximately 600 participants. To account for potential incomplete responses, the researchers increased the sample size by 10%.

The researchers employed a multi-stage quota random sampling method to collect data, ensuring equal representation across a large sample (Burger et al., 2006). The process included:

1) random selection of university types, comprising 8 statesupervised and 8 privately supervised universities;

2) selection by faculty groups, including Business Administration, Humanities, Liberal Arts, Engineering, Science and Technology, and Health Sciences;

3) selection of undergraduate students by year—first-year through fourth-year; and 4) division by GPA, categorizing students into low GPAs (≤3.00) and high GPAs (>3.00) using a simple random sampling method. The minimum total sample size was set at 768 participants, with strict controls during data collection to minimize external influences on responses. In this study, data were collected from a total of 833 participants. After filtering for complete responses, the final sample consisted of 820 participants. Table 1 provides preliminary information on the sample utilized for data analysis across the various stages of the research.

Table 1: Preliminary Information of the Samples Used in Various Steps of Analysis.

Preliminary Information of the Samples						
Steps	1st step (n = 120)		2nd step (n = 300)		3rd step (n = 400)	
Analysis	Item Quality Testing		Exploratory Factor Analysis		Confirmatory Factor Analysis	
Samples	Undergraduate Students		Undergraduate Students		Undergraduate Students	
Gender	Male = 58 (48.33%)	Female = 62 (51.67%)	Male = 134 (44.67%)	Female = 166 (55.33%)	Male = 187 (46.75%)	Female = 213 (53.25%)
Average Age (Years)	20.72		20.95		20.81	
GPAX	3.09, SD = 0.21		3.14, SD = 0.27		3.10, SD = 0.23	
Year	1st Year = 12	1st Year = 16	1st Year = 29	1st Year = 30	1st Year = 40	1st Year = 48
	2nd Year = 14	2nd Year = 17	2nd Year = 35	2nd Year = 42	2nd Year = 45	2nd Year = 55
	3rd Year = 17	3rd Year = 16	3rd Year = 37	3rd Year = 46	3rd Year = 54	3rd Year = 61
	4th Year = 15	4th Year = 13	4th Year = 33	4th Year = 48	4th Year = 48	4th Year = 49
Sibling Status	Only Child = 52		Only Child = 138		Only Child = 176	
	Siblings = 68		Siblings = 162		Siblings = 224	
Accommodation	Living in a Dormitory Alone = 30		Living in a Dormitory Alone = 80		Living in a Dormitory Alone = 115	
	Living with Family = 42		Living with Family = 96		Living with Family = 108	
	Living with Friends = 22		Living with Friends = 35		Living with Friends = 76	
	Living with Relatives = 26		Living with Relatives = 89		Living with Relatives = 101	

Note: *Missing Value is Excluded.

Instruments

The development of measurement instruments is a vital aspect of knowledge advancement, as it enables researchers to gain a comprehensive understanding and analysis of individual behaviours. The significance of creating such instruments encompasses three essential components:

1) Validity and reliability ensure that the results derived from the measurement instruments are accurate and applicable in both research and practical contexts.

2) Standardization facilitates the comparison of results across different sample groups, promoting consistency and broader acceptance in research, thereby making them relevant to specific target populations.

3) Reflecting reality means that the instruments must accurately represent the real behaviours being examined, taking into account the evolving social and cultural contexts (Kimberlin et al., 2008).The process of developing measurement instruments involves seven critical steps, as illustrated in Figure 2.

1) The initial step entails a comprehensive review of relevant documents, theories, and prior research to define the variables, formulate hypotheses, and identify the components of the measurement instruments.

2) The next step involves constructing the instrument by designing a component map, ensuring that each component comprises at least 25-30 items, with a balanced representation of positive and negative questions. These items are derived from the document review conducted in the first step.

3) An expert review is then conducted, wherein at least three experts in behavioural science evaluate the content validity of the instrument. The questions are subsequently revised and reassessed for face validity to ensure alignment with the objectives, content, theory, and measurement standards(Kemper, 2020; Sireci, 1998).

4) Pilot testing follows, wherein the instrument is administered to a sample of 120 individuals who closely resemble the target group. The data collected during this phase are coded for statistical analysis to evaluate the instrument's quality.

5) Item quality testing is conducted using an independent-sample t-test with a criterion of 30%, requiring t-values to exceed 2.00 (Sedgwick, 2010), along with Pearson's correlation coefficient analysis, where R-values must be greater than 0.20 (Obilor et al., 2018). Items meeting these criteria should align with the variable definitions outlined in the instrument's map. In cases where insufficient items meet the criteria, priority is given to t-values, as R-values indicate alignment with other items but do not reflect discriminatory power.

6) Finally, exploratory factor analysis is performed using principal component analysis (PCA) and Varimax orthogonal rotation to evaluate five key criteria(Hair Jr et al., 2017) the Kaiser-Meyer-Olkin

measure of sample adequacy must be at least 0.600, 2) the chi-square statistic must be statistically significant, 3) eigenvalues for components must be at least 1.00, 4) factor loadings must meet a minimum threshold of 0.300, and 5) collectively, all components must account for at least 50% of the variance in the variables.

This facilitates the formulation of the first hypothesis, H1: Exploratory Factor Analysis (EFA) can effectively evaluate the cybersecurity behaviour measurement instrument, requiring a minimum of four items per component, a Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy of no less than 0.600 and a factor loading threshold of at least 0.600, which exceeds the conventional standard. Furthermore, the second hypothesis is articulated as H2: Exploratory Factor Analysis (EFA) can account for more than 60% of the variance in cybersecurity behaviour (Tucker et al., 1997).

7) Subsequently, Confirmatory Factor Analysis (CFA) is performed to conductsecond-order factor analysis, thereby assessing construct validity (Smith, 2005). Five criteria are employed to evaluate the fit between the model and the empirical data, referred to as fit measures: 1) Chi-square statistics (McHugh, 2013) Root Mean Square Error of Approximation (Browne et al., 2002)Comparative Fit Index, 4) Tucker-Lewis Index (Cai et al., 2023) Standardized Root Mean Square Residual (Pavlov et al., 2021).

This culminates in the formulation of the third hypothesis, H3: CFA will validate that the model satisfactorily fits the empirical data, as evidenced by the fit indices conforming to the five academic standards outlined previously

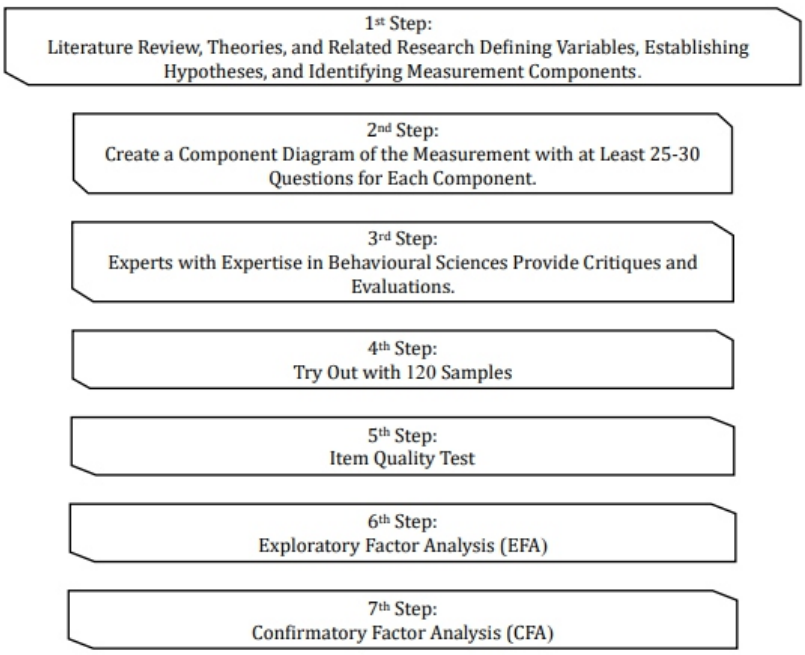

Figure 2: Steps in Developing the Cybersecurity Behaviour Measurement Instrument.

The measurement instrument utilized in this study is a cybersecurity behaviourquestionnaire comprising an initial pool of 100 items, developed by the researchers based on core concepts of cybersecurity. This tool encompasses four components, as detailed in Table 2: 1) Cyber Threat Awareness, 2) Cyber Threat Knowledge, 3) Cyber Threat Experience, and 4) Self-Protection from Cyber Threats. Each component features a balanced distribution of positively and negatively phrased statements. Respondents rate each item on a 6-point scale, employing the Summated Rating Method, with options ranging from "Most True" to "Not True at All." The overall reliability of the instrument is calculated to average 0.887 across 67 items. All itemsunderwent a comprehensive quality assessment following the seven key steps of measurement tool development, as illustrated in Figure 2.

Table 2: Components of the Cybersecurity Behaviour Measurement Instruments.

Cybersecurity Behaviour Measurement				
Code	A	B	C	D
Components	Cybersecurity Threat Awareness	Cybersecurity Behaviour	Cybersecurity Experiences	Cybersecurity Threat Self-Protection
Number of Initial Items	25 Items	25 Items	25 Items	25 Items
Positive Statements	13 Items	12 Items	12 Items	13 Items
Negative Statements	12 Items	13 Items	13 Items	12 Items
IOC Assessment Results	15 Items Remaining	18 Items Remaining	16 Items Remaining	18 Items Remaining
Average Reliability	0.889	0.892	0.884	0.884

Data Analysis

The research undertaken to develop and evaluate the measurement instrument employed three distinct types of statistical analyses. The first type involved statistics for assessing the quality of individual items, specifically utilizing Independent-Sample t-tests (Sedgwick, 2010) and Pearson's Correlation Coefficient Analysis (Obilor et al., 2018). The second type consisted of Factor Analysis aimed at exploring the dimensions or structures of specific characteristics of the items, which included both Exploratory Factor Analysis and Confirmatory Factor Analysis. The third type involved Inferential Statistics, with a particular focus on SEM Analysis (Stein et al., 2012).

Results

From the Index of Objective Congruence (IOC) assessment conducted by a panel of behavioural science experts, a total of 67 questions met the evaluation criteria. These questions underwent preliminary quality testing, where their discriminating power was evaluated using the Independent-Sample t-test (Sedgwick, 2010) and their correlation assessed through Pearson's Correlation Coefficient Analysis (Obilor et al., 2018). The analysis confirmed the presence of all four components, with 21 items meeting the criteria, thus supporting Hypothesis 1. The average reliability score was 0.885 (Table 3). The components that passed the criteria included: 1) Cybersecurity Threat Awareness (4 items), 2)

Cybersecurity Threat Knowledge (6 items), 3) Cybersecurity Threat Experience (5 items), and 4) Cybersecurity Threat Self-Protection (6 items).

Table 3: Preliminary Quality Assessment of the Cybersecurity Behaviour Measurement Instruments

Number	Code	Inferential Statistics: Parametric Statistics			
		T-test	R	Cronbach's Alpha	Communalities
		1st Component: Cybersecurity Threat Awareness			
1.	A14	3.708	0.264	0.890	0.673
2.	A7	2.661	0.272	0.887	0.617
3.	A11	2.190	0.240	0.890	0.649
4.	A1	2.969	0.285	0.889	0.514
		2nd Component: Cybersecurity Threat Knowledge			
1.	B14	2.850	0.281	0.887	0.704
2.	B11	3.259	0.349	0.890	0.652
3.	B7	5.236	0.492	0.888	0.590
4.	B13	3.199	0.321	0.893	0.664
5.	B5	2.703	0.327	0.892	0.779
6.	B9	3.242	0.289	0.894	0.562
		3rd Component: Cybersecurity Threat Experience			
1.	C14	4.779	0.471	0.882	0.739
2.	C11	3.655	0.383	0.881	0.724
3.	C3	6.076	0.514	0.882	0.675
4.	C9	2.946	0.478	0.882	0.666
5.	C7	5.663	0.496	0.884	0.755
		4th Component: Cybersecurity Threat Self-Protection			
1.	D12	5.602	0.577	0.876	0.816
2.	D13	3.477	0.442	0.880	0.643
3.	D10	4.289	0.503	0.877	0.588
4.	D15	4.765	0.525	0.884	0.634
5.	D6	3.346	0.493	0.883	0.649
6.	D4	3.653	0.455	0.884	0.539

Note: This Research Places Greater Emphasis on the T-Value than the R-Value, with the Selection Criteria Being a T-Value ≥ 2.00 and an R-Value ≥ 0.20.

The EFA using Principal Component Analysis and Varimax Orthogonal Rotation identified 21 items meeting the criteria, with factor loadings ranging from 0.608 to 0.871 and Eigenvalues exceeding 1 (Hair Jr et al., 2017)(Table 4). Communalities ranged from 0.514 to 0.816, and all factor loadings were statistically significant at the 0.05 level. The analysis explained 64.187% of the variance in cybersecurity behaviour among undergraduate students, thus supporting Hypothesis 2. The Kaiser-Meyer-Olkin Measure of Sampling Adequacy was 0.894, surpassing the minimum criterion of 0.600, while Bartlett's Test of Sphericity yielded a value of 6211.453, indicating strong correlations among the 21 items.

Table 4: Cumulative Percentage and Factor Loading of the Cybersecurity Behaviour Measurement Instruments

Code	Questions That Pass the Standard Criteria	Anti-Image	Factor Loading F1	F2	F3
	1st Component: Cybersecurity Threat Awareness				
A14+	Every time I use a banking application to transfer money, I make sure to log out once I finish using it.	0.287		0.793	
A7 +	I usually avoid connecting to public wireless networks (Wi-Fi) because I believe that my personal information could be accessed by others.	0.399		0.775	
A11+	I often think that disclosing personal identification on social networks can create security risks for individuals.	0.352		0.743	
A1 +	I always set complex passwords that are difficult for others to guess when accessing my information.	0.491		0.655	
	2nd Component: Cybersecurity Threat Knowledge				
B14+	I usually avoid opening or downloading files from unknown senders.	0.323		0.821	
B11+	I try to avoid using public computers, but if necessary, I ensure not to save any personal information.	0.352		0.783	
B7 -	I often set my phone to automatically connect to public wireless networks (Wi-Fi) because I prioritize convenience.	0.406		0.759	
B13+	I always read the privacy policy before confirming.	0.319		0.705	
B5 -	I tend to write down my passwords in places where they are easy for me to find.	0.275		0.701	
B9 +	I never save passwords or allow my information to be remembered on devices in public spaces.	0.418		0.611	
	3rd Component: Cybersecurity Threat Experience				
C14 -	I have experienced or know someone close who has been deceived by an individual impersonating someone else or using a fake profile.	0.305			0.830
C11 -	I have accessed or filled in personal information on a website that was created to scam and steal my personal data.	0.292			0.780
C3 -	I have disabled antivirus software on my computer to download files from a website.	0.344			0.748
C9 -	I think it is difficult to differentiate between legitimate websites and fake ones.	0.316			0.741
C7 -	I have been attacked by a computer virus because I wanted to watch movies or listen to music that were available for free download.	0.260			0.717

	4th Component: Cybersecurity Threat Self-Protection			
D12+	I will not post pictures or anything personal in public spaces because there is a risk that the information may be used for malicious purposes.	0.372	0.871	
D13+	I will set my privacy settings to avoid receiving spam or advertising messages.	0.398	0.787	
D10+	I do not share personal information with others unless I know their true purpose.	0.364	0.755	
D15+	Unless necessary, I usually do not use other people's communication devices and do not let others use my devices either.	0.436	0.724	
D6 +	I believe that installing tools or devices to prevent cyber-attacks helps protect me from cyber dangers.	0.358	0.661	
D4 +	I do not share my current location that can identify my identity on social media.	0.392	0.608	
Initial Eigenvalues			10.110	5.336 2.526
% of Variance			36.10719.058	9.022
Cumulative %			36.10755.16564.187	
Kasier-Meyer-Olkin Measure of Sampling Adequacy			0.894	
Bartlett's Test of Sphericity			6211.453	
df			51	

The results of the Confirmatory Factor Analysis indicate a good fit of the cybersecurity behaviour measurement model with the empirical data, thereby supporting Hypothesis 3, as the indices meet the standard criteria (Table 5 and Figure 3). The highest coherence was observed in Path D of the self-protection component ($\beta = 0.904$, $R^2 = 0.812$), followed by Path C of the experience component ($\beta = 0.865$, $R^2 = 0.857$), and Path B of the knowledge component ($\beta = 0.824$, $R^2 = 0.795$). Path A of the awareness component had the least influence ($\beta = 0.725$, $R^2 = 0.791$).

Table 5: Indices of Model Fit for the Cybersecurity Behaviour Measurement Instruments

Statistics	Criteria for Consideration	Statistics in the Model (Total Group)	Result of Consideration
Chi-Square Value	Not Statistically Significant	94.392	Accepted
Degrees of Freedom	Not Statistically Significant	59	Accepted
P-Value	Not Statistically Significant	0.531	Accepted
Root Mean Square Error of Approximation	≤ 0.06	0.044	Accepted
Comparative Fit Index	≥ 0.95	0.987	Accepted
Tucker – Lewis Index	≥ 0.95	0.986	Accepted
Standardized Root Mean Square	≤ 0.08	0.062	Accepted

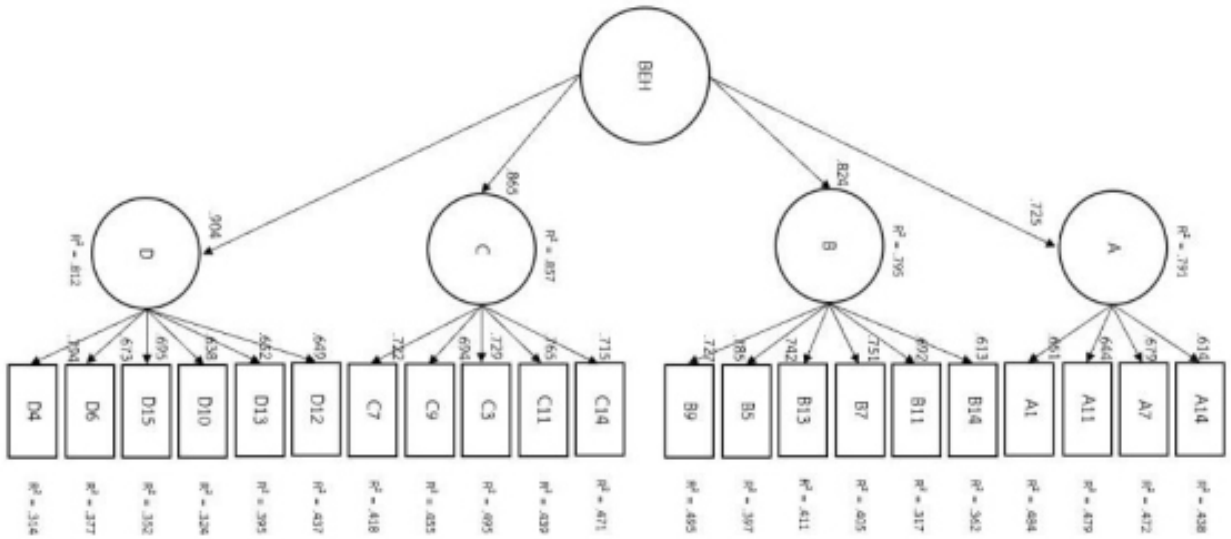

Figure 3: Fit of the Cybersecurity Behaviour Measurement Instrument Model with Empirical Data.

Discussion and Conclusion

This research identified 21 items that met the evaluation criteria across all four components, yielding an average reliability coefficient of 0.885. The measurement tool effectively explained 64.187% of the cybersecurity behaviour exhibited by undergraduate students. These findings are consistent with prior studies (Bidgoli et al., 2016; Djeki et al., 2024), which serve as a framework for research focused on developing and evaluating measurement instruments that incorporate the second level of Maslow's Hierarchy of Needs alongside cybersecurity concepts. Additionally, the results align with earlier investigations into cybersecurity issues among undergraduate students (Ahmad et al., 2021; Yan et al., 2018), thereby supporting all three hypotheses.

In examining each hypothesis, it was observed that the EFA required an adjustment in the factor loading threshold from 0.300 to 0.600. This adjustment enhanced the academic rigor of the items that met the criteria but potentially led to a reduction in the number of qualifying items. Consequently, Component 1, focusing on awareness of cybersecurity threats, was limited to four items, still satisfying the hypothesis requirement of a minimum of four questions. The Kaiser-Meyer-Olkin Measure of Sampling Adequacy remained within acceptable limits. Furthermore, CFA indicated a strong fit of the structural model, with all five indices meeting the established criteria, thus supporting Hypothesis 3 across all dimensions and demonstrating the clarity of the measurement instrument's components. The analysis conducted using this model constitutes a second-order factor analysis and provides robust evidence for construct validity (Smith, 2005).

Limitations

The cybersecurity behaviour measurement instrument developed in this study is specifically applicable to undergraduate students. To enhance its applicability, future adaptations should target other populations, such as school students or children. This approach would facilitate comparative analyses across diverse demographic groups,potentially uncovering significant variations in cybersecurity behaviours. Moreover, considering the dynamic landscape of cyber threats, it is imperative that the instrument's questions undergo regular updates to ensure their relevance to contemporary societal contexts.

Future Research Directions

For future research, it is advisable that the measurement instrument undergo an additional round of CFA to statistically validate any potential differences. The instrument could also be employed to investigate causal factors related to cybersecurity behaviour among undergraduate students. This may involve conducting causal-comparative research or examining cause-and-effect relationships by focusing on various independent or dependent variables to elucidate differences between groups. Furthermore, the tool could be adapted to assess students' cybersecurity readiness, potentially identifying at-risk groups who would benefit from targeted training. Additionally, the instrument could be refined to function as a social index, thereby raising awareness and guiding proactive prevention strategies, as cybersecurity continues to be a dynamic and critical issue. In this study, the researchers have already integrated the questionnaire into a mobile application that enables undergraduate students to self-assess and evaluate their understanding of cybersecurity issues. A handbook on cybersecurity knowledge has also been developed for interested individuals. Moreover, the findings from this research have been presented for further policy discussions, potentially contributing to strategic development plans.

References

Ahmad, N., Laplante, P. A., DeFranco, J. F., & Kassab, M. (2021). A cybersecurity educated community. IEEE Transactions on Emerging Topics in Computing, 10(3),1456-1463. https://doi.org/10.1109/TETC.2021.3093444

Azizi, N., & Haass, O. (2023). Cybersecurity issues and challenges. In Handbook of research on cybersecurity issues and challenges for business and FinTech applications(pp. 21-48). IGI Global. https://doi.org/10.4018/978-1-6684-5284-4.ch002

Bicen, H., & Cavus, N. (2011). Social network sites usage habits of undergraduate students: case study of Facebook. Procedia-Social and Behavioral Sciences, 28, 943-947. https://doi.org/10.1016/j.sbspro.2011.11.174

Bidgoli, M., Knijnenburg, B. P., & Grossklags, J. (2016). When cybercrimes strike undergraduates. 2016 APWG Symposium on Electronic Crime Research (eCrime), Biese, R., & O sterwall, G. (2024). "Cross Your Fingers and Hope You Don't Get Hacked" : A Qualitative Study on The Psychological Factors Behind Non-Compliance with Cybersecurity Recommendations [Student Thesis, https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1837432&dswid=1228

Browne, M. W., MacCallum, R. C., Kim, C.-T., Andersen, B. L., & Glaser, R. (2002). When fit indices and residuals are incompatible. Psychological methods, 7(4), 403–421.https://doi.org/10.1037/1082-989X.7.4.403

Burger, A., & Silima, T. (2006). Sampling and sampling design. Journal of public administration, 41(3),

, 65. htt6-668ps://hdl.handle.net/10520/EJC51475Cai, L., Chung, S. W., & Lee, T. (2023). Incremental Model Fit Assessment in the Case of Categorical Data: Tucker–Lewis Index for Item Response Theory Modeling. Prevention Science, 24(3), 455-466. https://doi.org/10.1007/s11121-021-01253-4

Chaikin, D. (2006). Network investigations of cyber attacks: the limits of digital evidence. Crime, Law and Social Change, 46, 239-256. https://doi.org/10.1007/s10611-007-9058-4

Cheurprakobkit, S., & Lerwongrat, K. (2023). Criminal justice officials' attitudes towards addressing computer crimes in Thailand: Difficulties and recommendations. Trends in Organized Crime, 1-21. https://doi.org/10.1007/s12117-023-09493-2

Darem, A. A., Alhashmi, A. A., Alkhaldi, T. M., Alashjaee, A. M., Alanazi, S. M., & Ebad, S. A. (2023). Cyber threats classifications and countermeasures in banking and financial sector. IEEE Access, 11, 125138-125158. https://doi.org/10.1109/ACCESS.2023.3327016

Debb, S. M., Schaffer, D. R., & Colson, D. G. (2020). A reverse digital divide: comparing information security behaviors of generation Y and generation Z adults. International journal of cybersecurity intelligence & cybercrime, 3(1), 42-55.https://doi.org/10.52306/03010420GXUV5876

Djeki, E., De gila, J., & Alhassan, M. H. (2024). West African online learning spaces security status and students' cybersecurity awareness level during COVID-19 lockdown. Education and Information Technologies, 29(12), 15557-15587. https://doi.org/10.1007/s10639-024-12472-x

Duzenci, A., Kitapci, H., & Gok, M. S. (2023). The Role of Decision-Making Styles in Shaping Cybersecurity Compliance Behavior. Applied Sciences, 13(15), 8731.https://doi.org/10.3390/app13158731

Florackis, C., Louca, C., Michaely, R., & Weber, M. (2023). Cybersecurity risk. The Review of Financial Studies, 36(1), 351-407. https://doi.org/10.1093/rfs/hhac024Frisk, I., Ruoslahti, H., & Tikanma ki, I. (2023). Cybersecurity Through Thesis in Laurea University of Applied Sciences. Proceedings of the 22nd European Conference on Cyber Warfare and Security,

Hair Jr, J. F., Matthews, L. M., Matthews, R. L., & Sarstedt, M. (2017). PLS-SEM or CB-SEM: updated guidelines on which method to use. International Journal of Multivariate Data Analysis, 1(2), 107-123. https://doi.org/10.1504/IJMDA.2017.087624

Jones, S., Johnson-Yale, C., Millermaier, S., & Pe rez, F. S. (2009). US college students' Internet use: Race, gender and digital divides. Journal of Computer-Mediated Communication, 14(2), 244-264. https://doi.org/10.1111/j.1083-6101.2009.01439.x

Kemper, C. J. (2020). Face Validity. In V. Zeigler-Hill & T. K. Shackelford (Eds.), Encyclopedia of Personality and Individual Differences (pp. 1540-1543). Springer International Publishing. https://doi.org/10.1007/978-3-319-24612-3_1304

Kimberlin, C. L., & Winterstein, A. G. (2008). Validity and reliability of measurement instruments used in research. American journal of health-system pharmacy, 65(23),2276-2284.

. https://doi.org/10.2146/ajhp070364

Kock, N., & Hadaya, P. (2018). Minimum sample size estimation in PLS-SEM: The inverse square root and gamma-exponential methods. Information systems journal, 28(1), 227-261. https://doi.org/10.1111/isj.12131

Kovac evic , I., Komadina, A., S tengl, B., & Gros , S. (2023). Light-Weight Synthesis of Security Logs for Evaluation of Anomaly Detection and Security Related Proceedings of the 16th European Workshop on System Security, Rome, Italy. McHugh, M. L. (2013). The chi-square test of independence. Biochemia medica, 23(2),143-149. https://doi.org/10.11613/BM.2013.018

Obilor, E. I., & Amadi, E. C. (2018). Test for significance of Pearson's correlation coefficient. International Journal of Innovative Mathematics, Statistics & Energy Policies, 6(1), 11-23. https://www.researchgate.net/profile/Esezi-Isaac-Obilor/publication/343609693_Test_for_Significance_of_Pearson's_Correlation_Coefficient_r/links/5f33ebbf458515b72918a25b/Test-for-Significance-of-Pearsons-Correlation-Coefficient-r.pdf

Pavlov, G., Maydeu-Olivares, A., & Shi, D. (2021). Using the standardized root mean squared residual (SRMR) to assess exact fit in structural equation models. Educational and Psychological Measurement, 81(1), 110-130. https://doi.org/10.1177/0013164420926231

Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. International Journal of Child-Computer Interaction, 30, 100343. https://doi.org/10.1016/j.ijcci.2021.100343

Rahman, M. H., Wuest, T., & Shafae, M. (2023). Manufacturing cybersecurity threat attributes and countermeasures: Review, meta-taxonomy, and use cases of cyberattack taxonomies. Journal of Manufacturing Systems, 68,196-208.https://doi.org/10.1016/j.jmsy.2023.03.009

Russo, E., Ribaudo, M., Orlich, A., Longo, G., & Armando, A. (2023). Cyber Range and Cyber Defense Exercises: Gamification Meets University Students Proceedings of the 2nd International Workshop on Gamification in Software Development, Verification, and Validation, San Francisco, CA, USA.

Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. Sustainability, 15(18), 13369. https://doi.org/10.3390/su151813369

Salubi, O. G., Ondari-Okemwa, E., & Nekhwevha, F. (2018). Utilisation of library information resources among Generation Z students: Facts and fiction. Publications, 6(2), 16. https://doi.org/10.3390/publications6020016

Sedgwick, P. (2010). Independent samples t test. Bmj, 340, 1-2. https://doi.org/10.1136/bmj.c2673

Sherman, D. A., Nelson, L. D., & Steele, C. M. (2000). Do messages about health risks threaten the self? Increasing the acceptance of threatening health messages via self-affirmation. Personality and Social Psychology Bulletin, 26(9), 1046-1058.https://doi.org/10.1177/01461672002611003

Shi, F., Ning, H., & Dhelim, S. (2021). A Tutorial of Cyber-Syndrome viewed from CyberPhysical-Social-Thinking Space and Maslow's Hierarchy of Needs. arXiv preprint arXiv:2111.02775. https://doi.org/10.48550/arXiv.2111.02775

Sireci, S. G. (1998). The construct of content validity. Social indicators research, 45, 83-117. https://doi.org/10.1023/A:1006985528729

Smith, G. T. (2005). On construct validity: issues of method and measurement. Psychological assessment, 17(4), 396-408. https://doi.org/10.1037/1040-3590.17.4.396

Stein, C. M., Morris, N. J., & Nock, N. L. (2012). Structural Equation Modeling. In R. C. Elston, J. M. Satagopan, & S. Sun (Eds.), Statistical Human Genetics: Methods and Protocols (pp. 495-512). Humana Press. https://doi.org/10.1007/978-1-61779-555-8_27

Tucker, L. R., & MacCallum, R. C. (1997). Exploratory factor analysis. Unpublished manuscript, Ohio State University, Columbus, 1-459. https://www.ffzg.unizg.hr/psihologija/phm/nastava/Book_Exploratory%20Factor%20Analysis.PDF

Watts, L. K., Wagner, J., Velasquez, B., & Behrens, P. I. (2017). Cyberbullying in higher education: A literature review. Computers in human behavior, 69, 268-274.https://doi.org/10.1016/j.chb.2016.12.038

Yan, Z., Robertson, T., Yan, R., Park, S. Y., Bordoff, S., Chen, Q., & Sprissler, E. (2018). Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment? Computers in Human Behavior, 84, 375-382.https://doi.org/10.1016/j.chb.2018.02.019

Zwilling, M. (2021). The Influence of COVID-19 Outbreak on the Readiness of Firms to Cyber Threats. In Responsible AI and Ethical Issues for Businesses and Governments(pp. 165-178). IGI Global. https://doi.org/10.4018/978-1-7998-4285-9.ch009.

Civil Protection of Trade Secrets in Cyberspace:Jordanian Legislation and International Agreements

Ahmad Mahmoud Al Masadeh 1 , Mohammad Assaf Al salamat 2 , Mohammad Tawfik Abdelfattah Batta3, Ahmed M. Khawaldeh4
Amman Arab University
Mohammad Alian Mafleh Al-Dahammsheh5
Private Law

A B S T R A C T

In the digital era, laws safeguarding trade secrets face increasing threats from cyber risks, posing significant challenges to legal frameworks worldwide. This research aims to assess the effectiveness of Jordanian legal provisions in protecting trade secrets within the technological domain. Utilizing a normative approach, the study examines the existing Jordanian legislation and relevant international agreements that address the civil protection of trade secrets in cyberspace. The findings reveal that, despite Jordan's efforts to protect trade secrets, emerging challenges persist, particularly concerning cross-border cyber-attacks and the rapid pace of technological advancements. The study offers practical recommendations to strengthen legislation, thereby enhancing the protection of trade secrets in Jordan's cyberspace. These insights are valuable for policymakers and legal scholars, providing guidance on improving the safeguarding of intellectual property in the digital environment.

Keywords: *Trade Secrets, Jordanian Legislation, International Agreements, Cyberspace, Protection.*

INTRODUCTION

The protection of trade secrets within firms and organizations has become increasingly complex due to the intensification of globalization and technological advancements (Põld, 2023). The integration of technology within organizational operations has heightened the likelihood of cybercriminal activities and unlawful penetrations (Saeed et al., 2023). It is very easy to steal trade secrets through computers. This includes private formulas and methods. Also, information technology is always changing, which lets hackers get around the defences that are already in place (Ubaydullaeva, 2024). The purpose of this paper is to investigate the civil protection of trade secrets on Jordan's internet in more depth. It will also investigate relevant international law treaties. This article gives a thorough look at the national laws and rules that protect trade secrets in cyberspace. It also talks about court decisions and how these laws are used in real life. The purpose of this article is to show the pros and cons of the present system by looking at these factors. The study also aims to find ways to make trade secret protection work better in Jordan's increasingly digital world. These are the reasons why the study sets the following research goals:

• the purpose of this study is to conduct an analysis of the legal framework that governs the protection of trade secrets within the setting of cyberspace in Jordan, including the laws, rules, and court precedents

that are pertinent information.

• This project aims to propose policy remedies and legislative changes meant to increase the effectiveness of trade secret protection on Jordan's cyberspace.

• for the purpose of investigating international agreements concerning the safeguarding of commercial secrets in their digital form.This paper provides a comprehensive analysis of the current legal framework for trade secret protection on the internet in Jordan, benefiting both legal practitioners and enterprises significantly. This renders the study considerably beneficial in return. It offers essential information for legislators aiming to modify the business environment and enhance intellectual property (IP) regulations, thereby informing the policymaking process.

Furthermore, underlined in the report is the need of trade secret protection and its part in promoting creativity and a basis for economic development. This study raises awareness of intellectual property rights, especially in developing countries, therefore contributing to the larger conversation on intellectual property and its absorption into the worldwide economy. For growing countries especially, this is quite crucial.

Literature Review

US Legislation Regarding Protection of Trade Secrets in Cyberspacethe Computer Fraud and Abuse Act addresses illegal access of any kind on computer systems of any kind. Sharing cybersecurity data also entails the distribution of data used to stop hostile operations directed against trade secrets(Soullier, 2024). that this facilitates information sharing between private enterprises and the government, especially in safeguarding trade secrets against cyber-attacks. Del Rosso and Bast's 2020 research indicate that the Electronic Communications Privacy Act regulates the interception ofelectronic communications and prohibits the unlawful acquisition of trade secrets stored in electronic formats (Nweke & Wolthusen, 2020). The saved Communications Act also pertains to the privacy of data held by electronic communication services (Del Rosso & Bast, 2020). offering enhanced protection for critical corporate information saved online(Elustondo, 2022).

Legislation in China regarding Protection of Trade Secrets in Cyberspace

Numerous essential legislative instruments constitute the legal foundation for trade secret protection in cyberspace in China. The primary legislation relating to the theft of trade secrets through digital networks is the Anti-Unfair Competition Law(Zhang, Lou, & Cai, 2021).

The Cybersecurity Law, enacted in 2017, imposes extensive obligations on organizations to secure their networks, aiming to protect sensitive data such as trade secrets from cyber threats (Vecellio Segate, 2020b). The Data Security Law of 2021 further enhances the protection of critical information by implementing cybersecurity measures (Creemers, 2022). Additionally, the Chinese Civil Code includes provisions related to the protection of trade secrets, particularly concerning the online dissemination of confidential information (Cai & Chen, 2022).

Legislation in the United Kingdom regarding the Protection of Trade Secrets in Cyberspace

As in many other countries, the UK has several key laws that protect trade secrets in cyberspace. The UK Trade Secrets Regulations 2018 implement the EU Trade Secrets Directive, establishing rules for civil action related to trade secret protection in digital environments (Vecellio Segate, 2020a). The Computer Misuse Act 1990 criminalizes unauthorized access to computers and data, including trade secrets (Wilson, 2019). Additionally, the Data Protection Act 2018 strengthens these protections by regulating the processing and safeguarding of personal data, indirectly supporting the protection of trade secrets through its focus on confidentiality(Walters, Trakman, & Zeller, 2019).

Legislation in India regarding Protection of Trade Secrets in Cyberspace

In India, the protection of trade secrets in cyberspace is governed by several key legal frameworks. The Information Technology Act of 2000, along with its subsequent amendments, includes provisions related to cybersecurity, data protection, and the safeguarding of trade secrets within the realm of information technology (Chander & Kaur, 2022). Cybercrimes are addressed in the Indian Penal Code, which includes provisions against illegal access to computer systems and data theft (Boruah, 2020). The Data Protection Bill of 2021, anticipated to be enacted, aims to safeguard sensitive data, thereby enhancing the protection of trade secrets kept in cyberspace(Kovacs, 2021).

Methodology of the Study

This study uses a normative research approach, which helps it to reach its goals and handle found problems. The first part is a thorough reading of all the current material, including legal documents, scholarly publications, and reports on the protection of trade secrets in cyberspace, both inside Jordan and abroad. This is subsequently succeeded by an analysis of Jordanian laws and regulations pertinent to trade secrets in cyberspace, along with relevant judicial rulings. The report also examines the legislative frameworks of countries recognized for their strong protection of trade secrets in cyberspace. Content

analysis will be conducted to analyse the acquired data.

Findings

Jordanian Legislation for the Civil Protection of Trade Secrets in Cyberspace

The following is a list of some of the most important laws in Jordan that pertain to the protection of trade secrets contained within cyberspace:

The Cybercrime Law of Jordan (Law No. 27 of 2015)

This piece of legislation makes some cyber-related actions illegal, therefore safeguarding commercial secrets. Among these transgressions include data theft, illegal computer system access, and data deletion. It enables companies facing cyber dangers to their personal data to take legal action by tackling behaviours including hacking, data breaches, and malware trafficking. the legislation imposes fines on individuals and businesses that are involved in illegal acts of this nature, which results in an increase in the level of protection afforded to personal information that is held in computer systems.(Toubat, Halim, & Magableh, 2020).

Jordanian Law No. 17 of 2023

Furthermore, according to this law, any person who unlawfully gets access to an information network or information system is considered to have committed an infraction. This infraction is subject to imprisonment for a duration of one week to three months, a fine between 300 and 600 Jordanian Dinars, or both penalties. The enactment of this regulation strengthens the safeguarding of trade secrets in cyberspace(Sadek, 2023).

Electronic Transactions Law of Jordan (Law No. 85 of 2001)

This law governs electronic communications and transactions, covering issues related to digital signatures and electronic documents. Although the law primarily addresses electronic transactions, encompassing their admissibility and security, it also contributes to the safeguarding of trade secrets within cybersecurity by ensuring the confidentiality of electronic messages and information (Toubat et al., 2020).

International Agreements for the Civil Protection of Trade Secrets in Cyberspace

Due to the extensive utilization of computer systems for storing and transmitting business information, it is essential to implement steps to safeguard trade secrets within the context of international law in today's corporate landscape. the rising utilization of the internet and digital media is associated with an increasing array ofthreats, including hacking, unauthorized access, and espionage. Trade secrets are more vulnerable to these risks. (Abd Jalil et al., 2020). Consequently, the subsequent international agreements pertain to the civil safeguarding of trade secrets in cyberspace:

Budapest Convention on Cybercrime

The Budapest Convention on Cybercrime is a significant international initiative regulated by the Council of Europe, although accessible for ratification by nonEuropean governments. Though the agreement mostly concerns computer crimes, it is directly pertinent to the safeguarding of trade secrets within computer systems. The agreement provides a structure for worldwide cooperation in spotting and punishing cybercrimes, including trade secret theft accomplished using computer programs (Nguyen & Golman, 2021). One of the most important clauses in the agreement is the ban on illegal access to computer systems, which hackers usually use to get trade secrets. Under the framework of globalization and the widespread influence of the internet worldwide, this clause is essential for improving cooperation among law enforcement authorities throughout many countries in safeguarding trade secrets. As established by the treaty, nations that have signed the deal could cooperate to monitor and identify hackers involved in the theft of significant corporate data (Spiezia, 2022).

Comprehensive and Progressive Trans-Pacific Partnership

Moreover, emphasized by this specific agreement is the protection of commercial secrets online. Focusing mainly on protecting trade secrets from being exploited online, this trade agreement comprising countries throughout the Pacific Rim includes clauses especially addressing trade secrets. Both civil and criminal actions are required to be taken against the unauthorized acquisition, disclosure, or use of trade secrets, notably through the use of cyber theft, as indicated under the agreement. The rules that it contains on digital trade are reflective of the modern dynamics of the global economy. These clauses underline the need of cybersecurity and the defines of rights in the framework of this environment. Furthermore, the agreement requires members to create appropriate legal remedies for trade secret exploitation on cyberspace. This promotes a more coordinated strategy to handle digital risks (Keitner & Clark, 2019).

General Data Protection Regulation

The primary objective of this rule is to protect personal data; nevertheless, it also has implications for the protection of trade secrets located in cyberspace. As a result, it enforces stringent data protection measures, such as encryption and safe storage, which can assist in preventing illegal access to important corporate information (Jackson, 2020). As a result of the regulation's imposition of significant costs for inadequate data protection, enterprises are being compelled to build sophisticated cybersecurity solutions that safeguard both personal and business information. In spite of the fact that it is primarily concerned with data protection, it offers insights into the ways in which privacy regulations and trade secrets interact in the digital environment, which frequently involves the combination of personal and corporate data (Markopoulou, Papakonstantinou, & de Hert, 2019).

US-China Economic and Trade Agreement (2020)

Signed in 2020, this agreement has clauses meant especially to guard intellectual property—including commercial secrets—from cybercrime. China has promised under this agreement to tighten its legal framework for trade secret protection and to raise fines for cybercrime (Abbott, 2021). At the bilateral level, this agreement is especially important since it guarantees that nations involved in high levels of digital commerce connections follow strict cybersecurity and trade secret protection criteria (Beconcini, 2021).

Organisation for Economic Co-operation and Development

This company has established cybersecurity and privacy policies due to its recognition of the critical necessity to protect trade secrets from internet threats (Carvalho et al., 2023). The directives for the Security of Information Systems and Networks require member nations to formulate policies aimed at bolstering the safeguarding of digital information, including trade secrets, against cyber threats. These guidelines are pertinent to any government aiming to establish robust security systems in response to escalating cyber threats (Radoniewicz, 2022).

Conclusion

This study project examines the civil protection of trade secrets in cyberspace under Jordanian law and international agreements, yielding some notable insights and findings. Every goal of the research was met brilliantly. The study underlined the need of strong trade secret protection and its importance in

promoting creativity and preserving a competitive advantage in many different fields. This study adds to the more general conversation on cyberspace trade secret civil protection. Practically, it also affects legislators, legal attorneys, and business entities running in Jordan.

Implications

Theoretical Implications

There is a noticeable lack of research on the topic of trade secret protection in cyberspace according to Jordanian law in the existing literature. This is particularly true in relation to regional efforts to combat digital threats. Academic studies examining the relationship between Jordanian civil law and cyber risks and international data breaches are severely lacking (Sadek, 2023; Toubat et al., 2020). While there has been some research on trade secret protection in general, very little on Jordanian civil law has been conducted. By looking into Jordan's current legal structure and how it has been adjusted to the digital environment, this research aims to solve these gaps. It sheds light on the methods in which developing nations safeguard their IP from cyber threats and offers a regional viewpoint on trade secret protection.

Practical Implications

In this paper, we'll look at some of the most important issues related to protecting trade secrets. It examines possible ambiguities and inconsistencies within the nationallegal framework that could hinder efficient protection. The research provides practical insights into the enforcement of trade secret rights in cyberspace, highlighting issues associated with court processes and remedies. The research assesses the conformity of Jordanian laws with international norms and agreements, emphasizing areas for enhancement. Additionally, it investigates the understanding and practices of Jordanian enterprises regarding the protection of trade secrets in the digital domain.

Policy-Related Implications

The study offers several key managerial implications:

• It advises Jordanian policymakers to strengthen enforcement mechanisms by implementing clearer guidelines for courts on issuing injunctions and calculating damages. Such measures would improve the protection of trade secrets in cyberspace. Additionally, establishing specialized intellectual property courts could expedite and streamline trade secret litigation.

• The study recommends that Jordanian policymakers continue to align the trade secret protection

framework with international standards and foster international cooperation to address cross-border trade secret misappropriation. Active participation in international forums and agreements would facilitate the exchange of best practices and enhance legal harmonization.

• Policymakers should promote innovation by offering incentives for businesses to invest in the protection of trade secrets. Moreover, providing legal advice and resources to small and medium-sized firms will foster a competitive and innovative business landscape.

Limitations

This study has several flaws. It only addresses Jordanian law, thereby limiting the relevance of its findings to other countries with different legal systems. The study uses secondary data sources and eliminates original data gathered from legal professionals' interviews. Due to the swiftly changing landscape of cyberspace and its related concerns, the legal framework may evolve, thereby impacting the significance of the study's conclusions. Moreover, the study's focus on civil protection omits the examination of criminal law elements that may potentially pertain to trade secret safeguarding.

Future Research Directions

Prior studies have primarily concentrated on conventional legal frameworks, intellectual property systems, and safeguarding strategies pertaining to tangible and commercial trade secrets. Although current research has examined the efficacy of legal frameworks for safeguarding trade secrets in national contexts and their interplay with neoliberal globalization, there is a significant lack of literature focusing on cyberspace and the civil protection of trade secrets from cyber threats. Future research should therefore investigate the dynamics of cyber threats, assess the adequacy of legal provisions for combating cross-border data theft, and explore how emerging technologies such as blockchain and artificial intelligence may impact the protection of trade secrets.

References

Abbott, F. M. (2021). Technology Governance in a Devolved Global Legal Order: Lessons from the China-USA Strategic Conflict. In A New Global Economic Order (pp. 197-226). Brill Nijhoff. https://doi.org/10.1163/9789004470354_006

Abd Jalil, J., Hassan, H., Abd Rahman, N., Ali, R. B. R. M., Mohamed, D., & Najib, A. (2020). Business under Threat: The Criminal Liability of Trade Secret Theft in Malaysia? International Journal of Business & Society, 21(S1), 49-65. https://www.ijbs.unimas.my/images/repository/pdf/Vol21-S1-paper4.pdf

Beconcini, P. (2021). The State of Trade Secret Protection in China in Light of the US-China Trade Wars: Trade Secret Protection in China Before and After the US-China Trade Agreement of January 15, 2020. UIC Review of Intellectual Property Law, 20(2), 2.https://repository.law.uic.edu/cgi/viewcontent.cgi?article=1490&context=ripl

Boruah, J. (2020). Cyber Crimes and Its Legal Challenges in India. The Journal of Legal Methodology Policy and Governance, 2(1). https://ssrn.com/abstract=3819497

Cai, P., & Chen, L. (2022). Demystifying Data Law in China: A Unified Regime of Tomorrow. International Data Privacy Law, 12(2), 75-92. https://doi.org/10.1093/idpl/ipac004

Carvalho, S., Carvalho, J. V., Silva, J. C., Santos, G., & Bandeira, G. S. (2023). Concerns about Cybersecurity: The Implications of the use of ICT for Citizens and Companies. Journal of Information Systems Engineering and Management, 8(2), 20713. https://doi.org/10.55267/iadt.07.13226

Chander, H., & Kaur, G. (2022). Cyber Laws and IT Protection. PHI Learning Pvt. Ltd. https://www.phindia.com/Books/BookDetail/9789391818463

Creemers, R. (2022). China's Cybersecurity Regime: Securing the Smart State. Available at SSRN 4070682. https://doi.org/10.2139/ssrn.4070682

Del Rosso, C., & Bast, C. M. (2020). Protecting Online Privacy in the Digital Age: Carpenter v. United States and the Fourth Amendment's Third-Party Doctrine. Catholic University Journal of Law and Technology, 28(2), 89-132. https://scholarship.law.edu/jlt/vol28/iss2/5

Elustondo, J. (2022). The Stored Communications Act and the Fourth Circuit: Resolving the Section 2510 (17)(B) Circuit Split in Hately v. Watts. Federal Communications Law Journal, 74(2), 223-249. http://www.fclj.org/wp-content/uploads/2022/09/98dc09e5-07dc4c2d-a505-b6da56aad004.pdf

Jackson, B. W. (2020). Cybersecurity, Privacy, and Artificial Intelligence: An Examination of Legal Issues Surrounding the European Union General Data Protection Regulation and Autonomous Network Defense. Minnesota Journal of Law, Science & Technology, 21(1),169-206. https://scholarship.law.umn.edu/mjlst/vol21/iss1/6

Keitner, C. I., & Clark, H. (2019). Cybersecurity Provisions and Trade Agreements. Harvard Business Law Review Online, 10, 1. https://journals.law.harvard.edu/hblr/wp-content/uploads/sites/87/2019/11/Cybersecurity-Provisions-in-Trade-Agreements_FINAL.pdf

Kovacs, A. (2021). Cybersecurity and Data Protection Regulation in India: An Uneven Patchwork. In L. Belli (Ed.), CyberBRICS: Cybersecurity Regulations in the BRICS Countries(pp. 133-181). Springer International Publishing. https://doi.org/10.1007/978-3-030-56405-6_4

Markopoulou, D., Papakonstantinou, V., & de Hert, P. (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. Computer Law & Security Review, 35(6), 105336. https://doi.org/10.1016/j.clsr.2019.06.007

Nguyen, C. L., & Golman, W. (2021). Diffusion of the Budapest Convention on cybercrime and the

development of cybercrime legislation in Pacific Island countries: 'Law on the books' vs 'law in action'. Computer Law & Security Review, 40, 105521. https://doi.org/10.1016/j.clsr.2020.105521

Nweke, L. O., & Wolthusen, S. (2020). Legal Issues Related to Cyber Threat Information Sharing Among Private Entities for Critical Infrastructure Protection. In 2020 12th International Conference on Cyber Conflict (CyCon) (Vol. 1300, pp. 63-78). IEEE.https://doi.org/10.23919/CyCon49761.2020.9131721

Põld, L. (2023). Beyond traditional intellectual property: The necessity and possibilities of strengthening the protection of trade secrets through its integration into the modern intellectual property system. International Comparative Jurisprudence, 9(1), 123-138.https://doi.org/10.13165/j.icj.2023.06.009

Radoniewicz, F. (2022). International Regulations of Cybersecurity. In K. ChałubińskaJentkiewicz, F. Radoniewicz, & T. Zieliński (Eds.), Cybersecurity in Poland: Legal Aspects(pp. 53-71). Springer International Publishing. https://doi.org/10.1007/978-3-030-78551-2_5

Sadek, G. (2023). Jordan: New Anti-Cybercrimes Law Enacted. Law Library of Congress.https://www.loc.gov/item/global-legal-monitor/2023-09-27/jordan-new-anticybercrimes-law-enacted

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. Sensors, 23(15), 6666. https://doi.org/10.3390/s23156666

*Soullier, B. A. (2024). Decriminalizing Trivial Computer Use: The Need to Narrow the Computer Fraud and Abuse Act (CFAA) After Van Buren. Federal Communications Law Journal, 76(2), 239-269. http://www.fclj.org/wp-content/uploads/2024/01/76.2.2_*

Decriminalizing-Trivial-Computer-Use-The-Need-to-Narrow-the-Computer-Fraud-andAbuse-Act-CFAA-After-Van-Buren.pdfSpiezia, F. (2022). International cooperation and protection of victims in cyberspace: welcoming Protocol II to the Budapest Convention on Cybercrime. ERA Forum, 23(1), 101-108. https://doi.org/10.1007/s12027-022-00707-8

Toubat, H. S., Halim, R., & Magableh, N. (2020). The Impact of Technological Development on Legal Rules: A Case Study of Jordan. Journal of Critical Reviews, 7(8), 1574-1579.https://repo.uum.edu.my/id/eprint/31192

Ubaydullaeva, A. (2024). Know-How and Trade Secrets in Digital Business. International Journal of Law and Policy, 2(3), 38-52. https://doi.org/10.59022/ijlp.162

Vecellio Segate, R. (2020a). Litigating Trade Secrets in China: An Imminent Pivot to Cybersecurity? Journal of Intellectual Property Law & Practice, 15(8), 649-659. https://doi.org/10.1093/jiplp/jpaa092

Vecellio Segate, R. (2020b). Securitizing Innovation to Protect Trade Secrets Between "the East" and "the West": A Neo-Schumpeterian Public Legal Reading. Pacific Basin Law Journal, 37(1), 59-126. https://doi.org/10.5070/P8371048804

Walters, R., Trakman, L., & Zeller, B. (2019). Data Protection Law: A Comparative Analysis of Asia-Pacific and European Approaches. Springer Singapore. https://doi.org/10.1007/978-981-13-8110-2

Wilson, K. (2019). Computer (mis) use and the law: what's wrong with the CMA? [Doctoral Dissertation, University of Oxford]. https://ora.ox.ac.uk/objects/uuid:f44d4182-a52f4842-aee0-28faa8b2acc8

Zhang, H., Lou, Y., & Cai, K. (2021). Research on the Dilemma and Improvement of Legal Regulation for Unfair Competition Related to Corporate Data in China. Computer Law & Security Review, 42, 105582. https://doi.org/10.1016/j.clsr.2021.105582.

Instructions for Authors

Essentials for Publishing in this Journal

1 Submitted articles should not have been previously published or be currently under consideration for publication elsewhere.

2 Conference papers may only be submitted if the paper has been completely re-written (taken to mean more than 50%) and the author has cleared any necessary permission with the copyright owner if it has been previously copyrighted.

3 All our articles are refereed through a double-blind process.

4 All authors must declare they have read and agreed to the content of the submitted article and must sign a declaration correspond to the originality of the article.

Submission Process

All articles for this journal must be submitted using our online submissions system. http://enrichedpub.com/ . Please use the Submit Your Article link in the Author Service area.

Manuscript Guidelines

The instructions to authors about the article preparation for publication in the Manuscripts are submitted online, through the e-Ur (Electronic editing) system, developed by **Enriched Publications Pvt. Ltd**. The article should contain the abstract with keywords, introduction, body, conclusion, references and the summary in English language (without heading and subheading enumeration). The article length should not exceed 16 pages of A4 paper format.

Title

The title should be informative. It is in both Journal's and author's best interest to use terms suitable. For indexing and word search. If there are no such terms in the title, the author is strongly advised to add a subtitle. The title should be given in English as well. The titles precede the abstract and the summary in an appropriate language.

Letterhead Title

The letterhead title is given at a top of each page for easier identification of article copies in an Electronic form in particular. It contains the author's surname and first name initial .article title, journal title and collation (year, volume, and issue, first and last page). The journal and article titles can be given in a shortened form.

Author's Name

Full name(s) of author(s) should be used. It is advisable to give the middle initial. Names are given in their original form.

Contact Details

The postal address or the e-mail address of the author (usually of the first one if there are more Authors) is given in the footnote at the bottom of the first page.

Type of Articles

Classification of articles is a duty of the editorial staff and is of special importance. Referees and the members of the editorial staff, or section editors, can propose a category, but the editor-in-chief has the sole responsibility for their classification. Journal articles are classified as follows:

Scientific articles:

1. Original scientific paper (giving the previously unpublished results of the author's own research based on management methods).

2. Survey paper (giving an original, detailed and critical view of a research problem or an area to which the author has made a contribution visible through his self-citation);

3. Short or preliminary communication (original management paper of full format but of a smaller extent or of a preliminary character);

4. Scientific critique or forum (discussion on a particular scientific topic, based exclusively on management argumentation) and commentaries. Exceptionally, in particular areas, a scientific paper in the Journal can be in a form of a monograph or a critical edition of scientific data (historical, archival, lexicographic, bibliographic, data survey, etc.) which were unknown or hardly accessible for scientific research.

Professional articles:

1. Professional paper (contribution offering experience useful for improvement of professional practice but not necessarily based on scientific methods);
2. Informative contribution (editorial, commentary, etc.);
3. Review (of a book, software, case study, scientific event, etc.)

Language

The article should be in English. The grammar and style of the article should be of good quality. The systematized text should be without abbreviations (except standard ones). All measurements must be in SI units. The sequence of formulae is denoted in Arabic numerals in parentheses on the right-hand side.

Abstract and Summary

An abstract is a concise informative presentation of the article content for fast and accurate Evaluation of its relevance. It is both in the Editorial Office's and the author's best interest for an abstract to contain terms often used for indexing and article search. The abstract describes the purpose of the study and the methods, outlines the findings and state the conclusions. A 100- to 250-Word abstract should be placed between the title and the keywords with the body text to follow. Besides an abstract are advised to have a summary in English, at the end of the article, after the Reference list. The summary should be structured and long up to 1/10 of the article length (it is more extensive than the abstract).

Keywords

Keywords are terms or phrases showing adequately the article content for indexing and search purposes. They should be allocated heaving in mind widely accepted international sources (index, dictionary or thesaurus), such as the Web of Science keyword list for science in general. The higher their usage frequency is the better. Up to 10 keywords immediately follow the abstract and the summary, in respective languages.

Acknowledgements

The name and the number of the project or programmed within which the article was realized is given in a separate note at the bottom of the first page together with the name of the institution which financially supported the project or programmed.

Tables and Illustrations

All the captions should be in the original language as well as in English, together with the texts in illustrations if possible. Tables are typed in the same style as the text and are denoted by numerals at the top. Photographs and drawings, placed appropriately in the text, should be clear, precise and suitable for reproduction. Drawings should be created in Word or Corel.

Citation in the Text

Citation in the text must be uniform. When citing references in the text, use the reference number set in square brackets from the Reference list at the end of the article.

Footnotes

Footnotes are given at the bottom of the page with the text they refer to. They can contain less relevant details, additional explanations or used sources (e.g. scientific material, manuals). They cannot replace the cited literature.
The article should be accompanied with a cover letter with the information about the author(s): surname, middle initial, first name, and citizen personal number, rank, title, e-mail address, and affiliation address, home address including municipality, phone number in the office and at home (or a mobile phone number). The cover letter should state the type of the article and tell which illustrations are original and which are not.

Notes: