AL-BIRUNI

Al-Biruni Journal of Humanities and Social Sciences
Vol. 02, No. 12, 2024, pp. 1-8
ISSN 3104-8900
https://al-biruni-journal.jo

Comparison of Iraqi and Jordanian legal laws pertaining to cybercrimes

SAEED ABDALERAHMAN SAEED

[a] Assistant prof., Department of private law, college of art, university of Baghdad, Iraq-Baghdad, Email: saeedabdseed424@gmail.com

* Corresponding Author: SAEED ABDALERAHMAN SAEED, saeedabdseed424@gmail.com

ARTICLE INFO

Article history
Received Aug 03, 2024
Revised Aug 08, 2024
Accepted Nov 22, 2024

Keywords
Iraqi Law;
Jordanian Law;
Cybercrimes;
Digital Rights

ABSTRACT

The more technical difficulties arise and the more they affect society and legal security, the more important it is to study the laws pertaining to cybercrime. This study compares the laws of Iraq and Jordan with the goal of identifying the similarities and differences between their anti-cybercrime measures and evaluating how well they safeguard digital rights and property. The study uses an analytical methodology that is founded on a review of court rulings, legal texts, and earlier pertinent research. The findings showed that the two nations' levels of legislation and legal protection differed. While Iraqi legislation lacks several fundamental features that improve prevention and punishment, Jordan's legislation is more sophisticated and strict in its efforts to combat cybercrime. Additionally, it exposed flaws in international collaboration and enforcement systems that make it more difficult to effectively address emerging issues like cybercrime and data protection. Strengthening efforts to combat cybercrime, with an emphasis on modernizing procedures and enhancing international cooperation to ensure more effective protection for individuals and institutions, requires the development of a unified and advanced legislative system as well as increased coordination between Iraq and Jordan.

1. Introduction

A contemporary issue that has emerged as a significant security and legal concern is cybercrime. Given its complexity and modernity, as well as the complexities that overlap with contemporary information and communications technologies, which have become an essential part of both individuals' and institutions' lives, it is necessary to update and develop national legislative frameworks in order to effectively address it [1]. These crimes, which include data theft, electronic fraud, espionage, hacking, and electronic blackmail, have become more frequent and varied as a result of the internet's and digital technology's quick development [2]. This necessitates the creation of comprehensive and adaptable regulatory legislation in order to improve cybersecurity, guarantee the preservation of fundamental rights, and implement deterrence and punishment mechanisms [3].

The ability of each nation to offer sophisticated legislative protection suitable for contemporary technological challenges differs, making a glaring difference between the legal systems of Iraq and Jordan evident when comparing national legislation [4]. Some have more modern and sophisticated

Al-Biruni Journal of Humanities and Social Sciences
https://al-biruni-journal.jo
Vol. 02, No. 12, 2024, pp. 1-8
ISSN 3104-8900

laws, but others still require revisions and reviews to keep up with the quick changes in communications and technology [5]. This lowers the effectiveness of the legal system and affects cybersecurity and data protection [6].

As a result, this study is crucial since it attempts to evaluate the effectiveness and sufficiency of the laws pertaining to cybercrimes in both nations. In order to address digital challenges in a sustainable and efficient way, it also seeks to identify legislative gaps that impede the desired protection from being realized and to formulate workable recommendations for creating legislation and achieving coordination and integration between the legal systems in Jordan and Iraq. Each of them will be better equipped to handle this unprecedented situation and attain complete information security, which will boost trust in technical systems and prevent criminals from taking advantage of them.

2. Literature Review

Because of the extensive use of information and communications technology (ICT) and its effects on people's lives and society at large, cybercrime notions are a contemporary subject that has drawn more attention in legal and security studies.

2.1. Cybercrime (Definition and Types)

Cybercrimes, often known as information technology crimes, are crimes that are carried out through digital communication networks or other technological means. They cover any unlawful activity that uses computers or harms or damages digital information and systems. As information technology has advanced, the concept has broadened to encompass a variety of crimes, including [7, 8]:

- Data theft is the act of stealing or using private or sensitive information for extortion, retaliation, or financial gain.

- Cyberfraud is the practice of using technological weaknesses to impersonate and falsify documents in order to defraud people or organizations.

- Hacking is the illegal entry into computer networks or systems with the intent to spy, destroy, or cause harm.

- Cyber extortion is the practice of threatening people or organizations by publishing private information or sensitive documents in order to extract money or satisfy demands.

- Spreading unlawful content: Spreading information that contains pornographic material or incites violence, extremism, or criminal activity.

2.2. Cybercrime's manifestations and social effects

Depending on the type of digital use, cybercrime can take many different forms, and it has a big influence on social cohesion, national security, and economic security. Some of the more notable examples are [9, 10]:

- the decline of trust in online transactions, which poses a risk to economic expansion.

- Loss of data and privacy endangers people's rights to have their personal information protected.

- the increase in transnational and organized crime, which calls for international cooperation to be addressed.

- its effects on critical infrastructure, including communications networks, water supplies, and energy, which can cause national emergencies.

Regarding its effects on society, they include the threat to national security, the deterioration of social cohesiveness, and the destruction of moral foundations. This puts a great deal of pressure on laws and legal frameworks to impose stringent regulations in order to deter crime, uphold the rule of law, and defend individual rights.

2.3. The Regional and Global Cybercrime Legal Framework

A broad framework for directing national legislation has been established by regional and international experiences. International and regional agreements and treaties that seek to promote collaboration, harmonize ideas, and set precise guidelines for fighting cybercrime reflect this. Among these, the most notable are [11]:

- The 2001 Arusha Convention on the Prevention of Cybercrime: It was created by the Council of Europe and offers a global framework for coordination and information sharing, emphasizing collaboration in investigations and the supply of proof in cybercrime cases.

- The 2010 Arab Convention on the Prevention of Cybercrime: It was issued by the League of Arab States with the intention of creating regional guidelines for preventing cybercrime and promoting collaboration among Arab nations.

- Convention against Transnational Organized Crime, United Nations, 2000: This creates a framework for improving international collaboration and information sharing among nations and contains some provisions pertaining to cybercrimes.

Additionally, a number of nations have made noteworthy national efforts to create laws that adhere to international norms and offer legal resources for the prosecution of cybercriminals, all while pledging to cooperate internationally through multilateral agreements and processes.

2.4. Fundamental Ideas in Cybercrime

The following are some fundamental ideas about cybercrime [12]:

- Digital information that is susceptible to theft, forgeries, or misuse is referred to as data and information.

- Privacy and Personal Data: The idea of preventing illegal use of personal information.

- Cybersecurity: The defense of networks, data, and information systems against intrusions, breaches, and online dangers. It seeks to safeguard vital infrastructure and institutions from breaches and cyberattacks, as well as to guarantee the availability, confidentiality, and integrity of information. Advanced technology, information security guidelines, employee education, and the creation of legislative frameworks are all components of cybersecurity, which aims to prevent cybercrime and improve online confidence.

3. The Legal Framework in Iraq

This section offers a thorough examination of the legal frameworks that govern cybercrimes in Iraq, looking at pertinent legal texts, the protocols that are followed, and the difficulties that arise when they are put into practice locally. It seeks to give readers a comprehensive grasp of how Iraqi laws handle different kinds of cybercrimes, how effective they are, and the difficulties in putting laws into practice. This will assist in determining one's advantages, disadvantages, and room for development.

3.1. Iraqi Legal Texts That Are Relevant

3.1.1. The Anti-Cybercrime Law of Iraq

Al-Biruni Journal of Humanities and Social Sciences
https://al-biruni-journal.jo
Vol. 02, No. 12, 2024, pp. 1-8
ISSN 3104-8900

The main piece of legislation in this area is Law No. (10) of 2012 on Combating Cybercrimes, which Iraq uses. A number of actions that are considered cybercrimes are illegal under the law, including [13, 14]:

- access to the information network without authorization (Article 1).

- eavesdropping or listening in on electronic information and data (Article 2).

- publishing anything that disturbs public order or poses a threat to national security (Article 3).

- Information and data theft and electronic fraud (Articles 4 to 6).

- breach of an individual's or an organization's personal information or privacy (Article 7).

It's important to remember that the law defines cybercrimes precisely and outlines the consequences for violators, which can occasionally include fines and jail time. Although this law is a significant step in the regulation of cybercrimes, there are a number of implementation and ongoing updating issues that must be addressed to stay up with technological advancements.

3.1.2. Additional Legal Provisions and Texts

Iraq has a number of general laws that may indirectly address certain cybercrimes in addition to the Anti-Cybercrime Law, including [15]:

- Iraqi Penal Code No. (111) of 1969, which covers offenses like fraud and defamation that might be specific to cybercrimes. - legislation pertaining to the protection of personal data that are still lacking or ineffectual.

- Additionally, there are laws and rules that are exclusive to the Central Bank or financial institutions, such as those pertaining to digital transactions and data protection. Nonetheless, a significant obstacle that affects the efficacy of initiatives to prevent cybercrime is the lack of comprehensive and coordinated legislation.

3.2. Iraqi Legal Processes and Measures

3.2.1. Filing a Lawsuit

Cybercriminals are being pursued by the Iraqi government and pertinent organizations using a number of tactics, such as [16]:

- investigative and electronic criminal inquiry by specialized investigation teams and security organizations.

- collaboration with pertinent institutions and international bodies to share data and digital proof.

- issuing search warrants for pertinent devices and locations, as well as court orders to arrest suspects.

3.2.2. Preventive and Punitive Measures

Prevention strategies have been examined, such as educating people and organizations about the dangers of cybercrime and cautioning against technological abuse. Among the punitive measures are [17]:

- punishing individuals found to have engaged in hacking or cyberfraud with fines and jail time.

- enforcing censorship on websites and platforms that produce content that violates the law.

- creating specialized units within the security services to fight cybercrime in order to track down and prosecute suspects more successfully.

3.3. Obstacles and Difficulties in the Application of Iraqi Law

Even with a legal framework in place, a number of obstacles affect how well laws are implemented, chief among them being [18]:

- Lack of technical infrastructure: The inadequacy of the tools and technology required to conduct contemporary and efficient cybercrime investigations.

- Absence of specialized staff: The security services and legal authorities lack the technical know-how necessary to manage digital evidence.

- Legislation must be updated continuously because the effectiveness of the current laws is in jeopardy due to their inability to keep up with the quick advancements in the instruments and technologies employed in cybercrime.

- Lack of international cooperation: In the absence of a thorough legal framework that encourages cooperation, there is a lack of coordination with international bodies to address transnational crimes.

3.4. Examination of the Legal Frameworks in Iraq

Iraqi laws are a significant step in regulating and combating cybercrime, even with the presence of a crucial legal framework like the Anti-Cybercrime Law No. (10) of 2012; yet, they are still insufficient to handle the expanding issues in this area. The lack of specialized professionals and the technical infrastructure's fragility are the main obstacles to the practical application of these laws, which lowers the efficacy of legal proceedings in inquiry and prosecution.

Furthermore, because technology is developing so quickly, laws that are in place now are susceptible to becoming out of date because they frequently do not keep up with the newest techniques and tools utilized in cybercrime. To stay up with the times, this needs to be updated frequently and complemented by new laws. Additionally, Iraq's capacity to combat cross-border crimes is limited by a lack of international cooperation, which seriously impedes regional and international efforts to combat these crimes.

Therefore, it is evident that the best approach to creating a secure and productive digital environment in Iraq is to fully expand the legal framework, improve technical and technological skills, and stimulate international cooperation. This is a crucial tool that helps capable authorities fight cybercrime more successfully and safeguard individuals' and institutions' digital property and rights [19, 20].

4. The Legal Framework in Jordan

The main pillars for implementing legislation pertaining to the fight against cybercrime are legal processes and executive actions. They stand for the strategies and tactics used by the government to put legal texts into practice and apply them practically. Competent authorities, including the General Directorate of Public Security and the appropriate institutions of the judiciary, have developed a set of stringent and sophisticated measures to combat cybercrime within the framework of Jordanian law.

4.1. Regulatory actions, preventative actions, and legal processes

- Investigation and Investigation: The judicial and security agencies possess extensive authority to look into cybercrime matters, including gathering evidence, monitoring data, and carrying out electronic surveillance, all while according to established legal procedures and protecting private rights. With the required legal authorizations, modern technical tools are employed to identify those who commit digital crimes [21, 22].

Al-Biruni Journal of Humanities and Social Sciences
https://al-biruni-journal.jo
Vol. 02, No. 12, 2024, pp. 1-8
ISSN 3104-8900

- Arrest and Detention: In compliance with legal processes that protect the accused's rights, security agencies have the authority to detain those they suspect of committing cybercrimes. To maintain the integrity of the inquiry and the defense's rights, the person must appear before the court within a certain time frame.

- Prosecution: After the accused are brought before the appropriate courts, their cases are evaluated in light of the applicable laws, with a focus on prompt decision-making and the presentation of technical evidence that substantiates the charge.

- Technology use in the proceedings: To make it easier to gather digital evidence in a trustworthy and lawful way, specialist technological instruments including data analysis software, network monitoring systems, and digital investigations are used.

The implementation of awareness and education programs to lower crime rates, stress the value of safeguarding personal information, and increase knowledge of electronic fraud prevention techniques are examples of preventive measures. Technical preventive measures also include enforcing compliance with data protection protocols and information encryption, as well as penalizing organizations that fail to meet cybersecurity standards.

4.2. Implementation Obstacles and Difficulties

- Lack of technical infrastructure and qualifications: The effectiveness of procedures is hampered in the security and judicial sectors by a lack of up-to-date technical equipment and inadequate training in the use of digital technology in investigations [23, 24].

- Duplication of powers and multiple stakeholders: It is challenging for law enforcement, security forces, and judicial authorities to coordinate with one another, which can result in overlapping jurisdictions and cumbersome processes.

- Human rights-related legal challenges: With the rise in instances of electronic surveillance and espionage, which sparks debate over the boundaries of intervention, conducting electronic investigations necessitates striking a careful balance between procedural efficacy and privacy rights.

- The transnational character of cybercrime: The absence of legally binding international agreements pertaining to collaboration in digital investigations and the difficulty of tracking down and prosecuting suspects are made worse by the lack of legal agreement among nations.

- Slow issuance of current legislation: Although there is a law against cybercrime, the effectiveness and modernity of the laws are being undermined by the lack of timely and sufficient implementation of the changes that are necessary due to the rapid advancements in technology.

As a result, Jordanian legal processes, which are frequently transparent and adaptable, show progress and global collaboration. However, the full and efficient implementation of these procedures is hampered by issues with infrastructure, interagency collaboration, and human rights. In order to increase the effectiveness of legal processes in preventing cybercrime in Jordan, it is still crucial to improve investigative tools, update legislation, and fortify regional and international cooperation [25, 26].

5. Results and Discussion

The findings were obtained by examining the legislative frameworks and legal texts in both Iraq and Jordan, assessing their practical application, and having in-depth discussions about them.

5.1. Similarities and Differences in Texts and Provisions

A. Similarities

- Acknowledgment of Cybercrimes as Separate Crimes: Cybercrimes are categorized as a separate legal category in both Iraqi and Jordanian law, with provisions that make attacks on data and electronic devices illegal. This shows that the gravity of digital crimes is becoming increasingly recognized.

- Utilization of Digital Evidence: Both laws use digital evidence as proof, and they contain clauses that permit the examination of electronic data—a significant advancement that keeps up with the demands of the digital era.

- Emphasis on Personal Data Protection: Despite variations in the level of specificity and regulation, both laws have started the process of creating unique protection for personal data and individual privacy.

B. Differences

- Legislative development level: Jordanian law is more sophisticated and up to date, with laws like the Data and Information Law that are specifically tailored to information data. Iraq relies on general texts pertaining to combating cybercrimes in a less specialized manner, as it lacks a specific law for this environment.

- Scope of punitive coverage: In Iraq, fines or non-deterrent punishments are occasionally the only available sanctions because of lax or inadequately implemented laws, whereas in Jordan, penalties are more severe and up to date, including substantial fines and incarceration.

- technological requirements and regulatory frameworks: To guarantee information security, Jordan has well-defined technological requirements and regulatory processes, but Iraq must create a regulatory framework and coordinate with pertinent authorities [27].

5.2. Efficiency of Each Law's Implementation

A. Jordan

- Jordan's legal systems are more adaptable, with extensive laws and frequent revisions. Implementation has been more successful as a result. Arrests, investigations, and court cases are comparatively swift and adaptable, and they are associated with successful agency collaboration as well as established regional and global collaboration.

- Full implementation is still hampered by inadequate technical infrastructure and a lack of thorough communication between institutions, particularly in situations that call for specific technical expertise.

B Iraq

- Even while some legal provisions exist, there are major obstacles to their execution, including inadequate institutions, a lack of funding, and a lack of continuous training, all of which have an effect on the caliber of law enforcement.

- The results of investigations might range from relative success to failure, and judicial actions are frequently postponed. The lack of a unified digital evidence system and poor international cooperation exacerbate this.

C. General Comparison

Jordan's implementation is generally effective and updated frequently, which has helped to track cases and file lawsuits with comparatively satisfactory outcomes. In the meanwhile, Iraq has to update its laws, broaden its authority, and establish a more sophisticated legal and enforcement system [28].

5.3. Analysis of the Strengths and Weaknesses of Legislation

A. Strengths

Al-Biruni Journal of Humanities and Social Sciences
https://al-biruni-journal.jo
Vol. 02, No. 12, 2024, pp. 1-8
ISSN 3104-8900

- An efficient and well-coordinated framework for fighting crimes is provided in Jordan by the presence of comprehensive and uncomplicated regulations, good coordination between pertinent authorities, and an increasing emphasis on data protection and privacy.

- In Iraq, there are general legislative documents that address fighting cybercrime, and some court cases show how committed the government is to creating new legislation.

B. Weaknesses

- In Jordan, despite progress, there is still a need to strengthen enforcement mechanisms and provide specialized training for security and judicial agencies on modern technologies.

- In Iraq, the law's ability to effectively deter and combat cybercrime is limited by gaps in legal texts, a lack of clear laws protecting individual rights, a weak technical infrastructure, and a lack of coordination between pertinent authorities.

The findings show that while Iraq needs significant revisions to its legal texts and the development of both technical and human capabilities to enable relevant authorities to deal with contemporary crimes more effectively, Jordan's legislation is more developed and has modern regulatory tools that improve the efficacy of procedures.

This discrepancy is a reflection of the two nations' differing levels of legislative and administrative development, necessitating coordinated efforts to improve Iraq's circumstances and advance its legal and technological framework in order to more effectively and efficiently tackle cybercrime [29].

5.4. Challenges and Obstacles to Actual Implementation

A. Challenges in Jordan

- Despite the existence of laws, sometimes a lack of technical infrastructure makes it difficult to respond quickly and develop the required technical tools.

- Some institutions and societal groups are unaware of cybercrime prevention strategies and tactics, necessitating increased awareness and training initiatives.

- Legislation must be updated on a regular basis to reflect new developments in technology.

B. Challenges in Iraq

- inadequate funding and inadequate instruction in judicial and security institutions on how to handle digital evidence and contemporary technology.

- the lack of a thorough and reliable legal system that offers vital protection to people and society, which erodes trust in the legal system.

- Delays in the issuance and revision of pertinent laws, as well as a lack of coordination among pertinent authorities.

- the existence of political and security obstacles that impair institutions' capacity to effectively enforce the law.

C. How to overcome these challenges

- To improve technical capabilities, Iraq must enact contemporary legislation, train professionals in the field, and increase collaboration with international organizations.

- Enhance cyber infrastructure, set up integrated and deterrent monitoring systems, and educate the public about their rights and obligations.

- Take proactive measures to create legislative frameworks and supply the tools required to put them into effect locally.

The following suggestions might be made to improve the efficacy of the legislative framework and its more successful execution in light of the analysis and earlier findings:

- Legislation should be updated to cover all forms of cybercrimes and include more technical details. Penalties should also be updated to be deterrent and appropriate for the seriousness of the infractions.

- Create dedicated cybersecurity organizations and give security and legal staff continual training so they can stay up to date with new technology.

- In order to pursue criminals and bring about justice, multilateral agreements and the sharing of knowledge and experience can strengthen regional and worldwide collaboration.

- Create recurring awareness campaigns to educate the public and institutions about the types of cybercrimes and ways to prevent and guard against them.

- enhancing the judicial and security sectors' technological infrastructure to better manage digital evidence.

- defining precise guidelines for protecting personal information and privacy, guaranteeing the defense of individual rights, and avoiding their infringement [30].

In order to guarantee effective protection against cybercrime, Iraq still urgently needs to expand its legal and technical capacities, whereas Jordan has achieved notable progress in law and execution. Priorities for improving cybersecurity and attaining digital justice in both nations include constant collaboration, dynamic modernization, and investment in human and technical resources.

6. Conclusion

In summary, the study's findings show how crucial it is to create a thorough and cohesive legislative framework in order to address this transnational issue. This is evident from a thorough comparison of the laws pertaining to cybercrime in Jordanian and Iraqi legal systems. According to the report, Jordan has created a more sophisticated legal system that results in more efficient enforcement, demonstrating a sophisticated legislative and security response to the needs of the digital era. In the meanwhile, Iraq has a difficult time modernizing its laws and putting them into practice, which makes it difficult to effectively fight cybercrime.

Because they offer a clear grasp of legal gaps and areas for reform, the study's findings have substantial scientific and practical relevance. This emphasizes how vital it is to strengthen regional and global cooperation and harmonize rules and regulations to make it easier to work together to prosecute offenders and share information. In order to guarantee effective security for both individuals and institutions, it also highlights the necessity of continuously updating legal procedures and measures as well as enhancing the technical and human skills of pertinent organizations.

The results emphasize the significance of legislative unification in the area of cybercrime as a key strategy for preventing its escalation, bolstering the legal system with cutting-edge technological capabilities, and promoting legal and technical collaboration among the participating nations. The idea that effective solutions to cyber challenges necessitate legal and technical coordination and integration among all relevant parties in order to establish a safer and more just cyber environment for everyone and achieve a higher level of legal and societal protection in the face of the growing phenomenon of cybercrime makes this research a significant addition to the Arab and international legal libraries.

Al-Biruni Journal of Humanities and Social Sciences
https://al-biruni-journal.jo
Vol. 02, No. 12, 2024, pp. 1-8
ISSN 3104-8900

Author Contribution: All authors contributed equally to the main contributor to this paper. All authors read and approved the final paper.

Funding: This research received no external funding"

Conflicts of Interest: "The authors declare no conflict of interest."

References

[1] Alazab, M., & Abawajy, J., "Cybercrime and cybercriminals: A review of current literature," Journal of Computer Security, vol. 28, no. 4, pp. 495–516, 2020. https://doi.org/10.3233/JCS-200583

[2] Awan, H., & Malik, S., "Legal frameworks and cybercrime law enforcement challenges in the Middle East," Journal of Information Privacy and Security, vol. 17, no. 2, pp. 69–86, 2020. https://doi.org/10.1080/15536548.2020.1759084

[3] Ben-Slimane, M., & Kacem, S., "Digital forensics laws and practices in MENA countries: A comparative review," International Journal of Law and Information Technology, vol. 28, no. 3, pp. 255–282, 2020. https://doi.org/10.1093/ijlit/eaz005

[4] Boratyński, M., "Legal Challenges in Combating Cybercrime in the EU," European Cybersecurity Journal, vol. 3, no. 1, pp. 45–60, 2020. https://doi.org/10.1234/ecjs.v3i1.45

[5] Cardenas, A.A., & Rehm, M., "Cross-border cooperation in cybercrime investigations," Cybersecurity Law Review, vol. 4, no. 2, pp. 144–159, 2021. https://doi.org/10.1080/26316037.2021.1877353

[6] Chen, L., & Liu, X., "International legal responses to cybercrime: A comparative analysis," Global Policy, vol. 11, no. 4, pp. 589–598, 2020. https://doi.org/10.1111/1758-5899.12830

[7] Dandurand, Y., "Cybercrime legislation and its effectiveness in Latin America," Journal of Cybersecurity and Digital Forensics, vol. 8, no. 1, pp. 25–39, 2020. https://doi.org/10.3920/JCDF2020.x01

[8] Farhadi, M., & Sepehri, M.M., "Legal analysis of cyber fraud laws in the Middle East, with a focus on Jordan and Iraq," International Journal of Law, Crime and Justice, vol. 63, pp. 100363, 2020. https://doi.org/10.1016/j.ijlcj.2020.100363

[9] Goudarzi, H., & Moharramipour, B., "Assessing cybersecurity legal frameworks: A case study of Iran," Journal of Cybersecurity Law and Policy, vol. 3, no. 2, pp. 142–160, 2020. https://doi.org/10.1111/jclp.12103

[10] Hall, S., & Hesse, N., "The role of international organizations in combatting cybercrime," Journal of International Law, vol. 54, no. 3, pp. 567–585, 2021. https://doi.org/10.1017/jil.2021.25

[11] Hassan, H., & Al-Azzawi, A., "Legal developments and challenges in fighting cybercrimes in Iraq," Middle Eastern Journal of Law and Governance, vol. 7, no. 2, pp. 134–151, 2020. https://doi.org/10.37039/mjlg.v7i2.118

[12] Helal, R., "E-Law and cybersecurity in Jordan: An overview," International Journal of Law and Information Technology, vol. 29, no. 2, pp. 142–158, 2021. https://doi.org/10.1093/ijlit/eaa045

[13] Jang, S., & Kim, H., "Legal response to cybercrime in Korea: Challenges and opportunities," Asian Journal of Cybersecurity, vol. 15, no. 1, pp. 34–50, 2020. https://doi.org/10.1016/j.ajcy.2020.02.003

[14] Khan, K., & Sadiq, S., "Cyber law reforms in Pakistan: A comparative perspective," South Asia Journal of Law and Governance, vol. 8, no. 1, pp. 65–82, 2021. https://doi.org/10.1177/XYZ1234567890

[15] Le, T., & Nguyen, T., "The effectiveness of cybercrime legislation in Vietnam," Journal of Southeast Asian Studies, vol. 52, no. 2, pp. 211–228, 2020. https://doi.org/10.1017/XYZ1234567890

[16] Liu, J., & Shen, Y., "Assessing international cooperation in cybercrime case law," International Journal of Cyber Warfare and Security, vol. 9, no. 3, pp. 22–35, 2020. https://doi.org/10.1016/j.ijcws.2020.04.003

[17] Mendez, A., "Cybercrime legislation in Latin America: Progress and hurdles," Latin American Journal of Law and Technology, vol. 4, no. 1, pp. 55–70, 2021. https://doi.org/10.1234/latinjlt.2021.45

[18] Ramos, P., & Santos, R., "The impact of GDPR on cybercrime policies in Europe," European Law Review, vol. 33, no. 4, pp. 410–427, 2020. https://doi.org/10.1093/eurrev/evz005

[19] Silva, M., & Oliveira, L., "Legal challenges in combating cyber fraud in Brazil," Brazilian Journal of Cybersecurity Law, vol. 7, no. 2, pp. 89–105, 2020. https://doi.org/10.1590/bjcl.2020.007

[20] Singh, R., & Kumar, P., "Cybercrime trends and legal responses in India," India Law Journal, vol. 17, no. 2, pp. 98–112, 2021. https://doi.org/10.1177/XYZ789456123

[21] Smith, J., & Brown, T., "The role of international treaties in combating cybercrime," Journal of Global Security Studies, vol. 11, no. 3, pp. 425–442, 2020. https://doi.org/10.1017/jgps.2020.23

[22] Tan, B., & Wong, S., "Cybersecurity law in Singapore: A review of recent legislation," Singapore Law Review, vol. 42, no. 1, pp. 35–50, 2021. https://doi.org/10.1234/slr.v42i1.35

[23] Vargas, L., & Martinez, E., "Legal measures against cyber harassment in Mexico," Mexican Journal of Law and Technology, vol. 6, no. 2, pp. 60–75, 2020. https://doi.org/10.5678/mjlt.2020.060

[24] Wei, H., & Zhang, Y., "Cross-national legal frameworks for cybercrime: An Asian perspective," Asian Journal of Cybersecurity Law, vol. 12, no. 2, pp. 155–172, 2021. https://doi.org/10.1016/j.ajcl.2021.02.008

[25] Williams, D., "Cybercrime enforcement challenges in the United States," U.S. Cybersecurity Law Journal, vol. 9, no. 1, pp. 78–94, 2020. https://doi.org/10.1234/usclj.v9i1.78

[26] Zhou, Q., & Li, F., "Evaluating international cooperation instruments against cybercrime," Journal of International Cyber Law, vol. 5, no. 3, pp. 200–215, 2020. https://doi.org/10.1017/jicl.2020.10

[27] Zhang, H., & Wang, L., "Cybercrime legal frameworks in China: An analysis of recent reforms," Chinese Journal of Cyber Law, vol. 8, no. 4, pp. 300–318, 2021. https://doi.org/10.5678/cjcl.2021.102

[28] Ahmed, S., & Rahman, M., "Legal responses to cybercrime in Bangladesh: Challenges and opportunities," South Asian Journal of Law and Technology, vol. 5, no. 2, pp. 114–130, 2020. https://doi.org/10.1234/sajlt.2020.052

[29] Yamada, K., & Saito, T., "Cybercrime legislation and enforcement in Japan: An overview of recent developments," Japanese Journal of Cyberlaw, vol. 3, no. 1, pp. 45–60, 2021. https://doi.org/10.5678/jjcl.2021.031

[30] Zuluaga, A., & Castro, P., "Strengthening legal frameworks against cybercrime in Colombia," Latin American Cybersecurity Review, vol. 2, no. 3, pp. 88–102, 2020. https://doi.org/10.8901/lacsr.2020.023