Cybercrime Laws in Iraq: Addressing Limitations for Effective Governance

Nashwan Mohammed Suleiman[1]*
Al-Noor University College, Bartella, Iraq

Ahmed Hatim[2]
Al-Farahidi University, Iraq

Mohamed Amer Alseidi[3]
Al-Hadi University College, Baghdad, Iraq

Karrar Shareef Mohsen[4]
Al-Ayen University, Iraq

Wesam Khalid Abd Al Aali[5]
Mazaya University College, Iraq

Alaa Hussein Abdulaal[6]
Ashur University College, Iraq

Mustafa Asaad Rasol[7]
National University of Science and Technology, Iraq

Abdulnaser Khalid Hamzah[8]
AL-Nisour University College, Iraq

Khudr Bary Freeh Alsrray[9]
Al-Esraa University, Iraq

[1] Department of Law, Al-Noor University College, Bartella, Iraq.
Email: nashwan.mohammed@alnoor.edu.iq
[2] College of Law/ Al-Farahidi University/Iraq.
[3] Al-Hadi University College, Baghdad, 10011, Iraq. Email: dr.mohamed.alseidi@huc.edu.iq
[4] Information and Communication Technology Research Group, Scientific Research Center, Al-Ayen University, Thi-Qar, Iraq.
[5] Mazaya university college Iraq. Email: ww1983ww83@mpu.edu.iq
[6] Medical device engineering/ Ashur University College/Baghdad/ Iraq.
email: alaa.hussein@au.edu.iq
[7] National University of Science and Technology, Dhi Qar, Iraq.
Email: mustafa.a.rasol@nust.edu.iq
[8] Department of Medical Laboratories Technology, / AL-Nisour University College/ Baghdad/ Iraq. Email: abdulniser.kh.eng@nuc.edu.iq
[9] College of Arts, Department of Media/ Al-Esraa University, Baghdad/ Iraq
* Corresponding Author Email: nashwan.mohammed@alnoor.edu.iq

Abstract

Developing countries like Iraq have embraced digitalization and technology without proper legal measurement and implementation concerning the adverse outcomes, which has entangled Iraq in a crucial stage to take immediate actions against the negative aspect, i.e., cybercrimes. To address the current status of this issue, the study has investigated the legislative and administrative laws of cybersecurity to explore its limitations and provide suggestions for effective governance. This study has collected data qualitatively from the legislative experts of Iraq. The data was analyzed through NVIVO software, and transcription and thematic analysis were run. The analysis divided the data into four themes of different concepts. The findings have concluded several limitations prevailing and existing in the current laws. The theoretical and practical implications of the study have been discussed in the study.

Keywords: Cybercrime Legislative; Administrative Laws; Iraq; Governance; Limitations

1. Introduction

Cybercrime impacts consumers and sellers and is a rising concern for nations at all stages of growth. Law enforcement organizations and prosecutors face an enormous obstacle due to the changing nature of cybercrime and associated shortages of skills, particularly when it comes to international prosecution (Unctad, 2021). Iraq's digital industry is currently ungoverned, making it one of the most open and vulnerable in the world. Due to the country's political and security environment, more effort will be required to establish the organizational, technological, authorized, and capacity-building foundations necessary to offer effective cybersecurity for its people, enterprises, and government (Jawad, 2017). The Iraqi government hardly ever releases information on the sorts of cybercrime that occur there. However, past studies published by the Iraqi government reveal the most typical forms of cybercrime in Iraq, which have probably become more prevalent over time. There is presently no particular cybercrime legislation in existence in Iraq. Cybercrime is currently far from having a clear definition. Because cyber actions are not constrained by physical boundaries, the majority of countries have laws in place to address these issues (Nehme, 2020). Nonetheless, the underlying crime actually differs from situation to situation. This makes these crimes all the more complex and confusing. The basis upon which societies and enterprises are constructed is now made up of the online world, digital devices, and technologies. Digital consumption has also evolved into a measurement and indication of progress.

Despite the House of Representatives having filed a bill on cybercrimes for consideration, there is no specific law in Iraq that deals with it. Inadequate current governing systems in Iraq have made it difficult to generally enhance governance. Iraqi administrations have faced severe sectarian hostility since the invasion by the United States in 2003 (O'Driscoll, 2018), which has resulted in situations that are almost civil war-like and are heightened by self-imposed issues like bribery and insufficient transparency. The anti-cybercrime draught bill has been challenged by the Iraqi civil rights community because it does not adhere to both international and Iraqi legal requirements. Nevertheless, Iraq rejected the anti-cybercrime law's adoption in its existing version because it was overly broad and limited its rights to

free expression (AbdulAmeer et al., 2022). In the age of technology, cybercrime has become a widespread problem that creates serious problems for governments and society all around the world, including Iraq. As technologies develop, so do the techniques and complexity of cybercriminal operations, demanding strong governmental and administrative structures to tackle cyber threats successfully. Nevertheless, Iraq's current cybercrime legislation and administrative procedures may have limitations in dealing with the constantly changing cyber threat landscape, necessitating an in-depth study of these legal and administrative issues. The aim of this study is to explore the cybercrime legislative and administrative laws within Iraq, with a focus on identifying limitations and gaps in the existing framework. The objectives of this study are:

1. To assess the current cybercrime legislative framework in Iraq
2. To explore the adequacy and effectiveness of administrative measures in mitigating cybercrime risks within Iraq
3. To identify potential limitations in the current cybercrime laws in Iraq

The study's findings and recommendations can help Iraq improve its cybersecurity governance. The findings can help policymakers and authorities develop focused initiatives to improve cybercrime prevention, detection, and response processes by highlighting gaps in the current legislative and administrative framework. Critical infrastructure, governmental organizations, and people are all at serious risk from cybercrimes. In order to better protect Iraq's digital landscape and residents from cybercriminal tasks, regulations, and administrative measures may be developed as a consequence of an understanding of the weaknesses in the current cybersecurity protocols.

2. Literature Review

2.1 Role of Cybercrime Legislations in Preventing Cybercrimes

Over the last decade, there has been observed an alarming increase in cybercrimes, which has caused hindrance in the positive impression and working of technology and the internet. The whole world has indulged in internet usage and technological addiction, and this has facilitated cybercriminals in every corner of the world, and the trend of cybercrimes had gained more rising rate during the covid times when every person was bound to house boundaries (Rakhimova, 2020). The speed in the growth of cybercrimes has been mentioned as faster than the legislation and regulations to prevent this serious crime, and some studies have explored the past content available in the literature that has provided suggestions for practitioners and policymakers to implement and combat cybercrimes. Khan et al. (2022) have conducted an extensive literature review focusing on the legislation in both technology and legal framework; they have found the need for cybercrime legislation to be enhanced, strengthened, and to be made up to date with the rapidly evolving technologies and the growing rate of crimes comes with it.

The Council of Europe's Convention on Cybercrimes has been named the leading international instrument for cybercrime control, comprised of four sections based on topics (Urbas, 2015). After this, the global law regarding cybercrimes has been established, which has been seen as a countermeasure for implementing legal norms in different countries. This legal framework has been connected with foreign policy to minimize the rate of cybercrimes all over the world (Siregar & Sinaga, 2021).

Cybercrimes have a high rate in developing regions like Asia, where the Budapest convection has been observed to be moderately aligned with South Asian countries' laws, but actions have been required to raise awareness about cybercrimes and the pupation of Budapest laws according to the latest cybercrimes (Chang, 2020). Despite the worldwide application of the Budapest convention of the Council of Europe's Convention on Cybercrimes, still, countries haven't properly converted this law into action; like Pacific Island Countries [PIC] still have this law in their books, not in the enforcement of their existing law capacity (Le Nguyen & Golman, 2021).

The Council of Europe's Convention on Cybercrimes has benefits and accuracy in prevention but still has some limitations. Tosoni (2018) has argued about the privacy policy and concerns provided in the Council of Europe's Convention on Cybercrimes laws and has drafted an additional convention that has been pointed before to fail in providing adequate privacy and maintaining privacy protection. In China, strict laws and legal actions like administrative laws, content filtering, and monitoring have been implemented to tighten the circle of cybercrimes (Li, 2015). Due to these laws' applications, China has no prominent need for cyber police, investment in cyber security, and surveillance of internet users.

From the business perspective, studies have analyzed the relationship between cybercrime laws, business laws and their influence on the business and prevention of cybercrimes. Business laws have a prominent impact on the performance of organizations, and companies should implement cybercrime laws in their administration for smooth business practices and customer confidence (Hasbullah, 2022). Businesses have been observed to report cybercrimes in their setup very often, and most companies report their cyber issues based on the nature and intensity of cybercrime and the companies' mindset for the protection against cybercrimes (Kemp et al., 2021). In Iraq, there has been illustrated weak judicial system for the patent and other intellectual rights for the companies, and a study (Mohameed et al., 2022) has demonstrated the significance and importance of proper legislative and administrative systems for the safety of business patient rights.

2.2 The Impact of Cybercrime Legislative and Administrative Laws on Effective Governance

Cybercrime laws and regulation has a positive role in the effective governance of companies, and the literature has knowledge, information, and guidance for the significance of this relationship. A study has emphasized the concept of organized cybercrimes and has explored it as a profit-driven crime (Lusthaus, 2013), and they have illustrated the challenges associated with organized crimes; violence, issues of territory, and enforcement. Data-driven government has its significance by the quality delivery of information and knowledge to the nation using different technologies, which has the alarming aspect of cybercrimes.

In this context, a study (Oni et al., 2019) has investigated the government's adoption of digitalization in Nigeria, and they indicated a substantial danger in the implementation of digitalization for government information delivery. Another study has investigated the role of legal and administrative laws for cybersecurity, they compared Budapest laws with the existing running laws in Nigeria, and they gained insight into the acute need for the domestication of Budapest conventions in the legislations and administrations of the Nigerian judicial system for controlling the

cybercrime activities. These studies have reflected Nigeria's current judicial status and the need for the proper action of the Budapest Conventions to eliminate cybersecurity. A developing country like Iraq has been reviewed from the perspective of the rate of cybercrimes (Aboud, 2012); it has revealed the high rate of cybercrimes among high school student scholars with the rate of 62.7%, reflecting an alarming situation for Iraq to focus on the education department to reduce this frightening aspect of cybercrimes in students. After passing so long, several recent studies have still explored, tested, and discussed the falling laws and legislations in Iraq for the control of cybercrimes, and they have provided the reasons and drawbacks that exist in the running legislation and judicial system.

2.3 Cybercrime Legislation in Iraq

In Iraq, laws and regulations have been implemented against cybersecurity, but still, there have been demonstrated several challenges in the reformation of existing laws, including a lack of cybercrimes concept, extensive access to technology, lack of surveillance, and no defined age to accuse for cybercrimes (Mahmood, 2020). In Iraq, media and other information technology communication sectors have forced the government and the judicial bodies to pass an act or legal framework that should cover the concept of cybercrimes and relevant terms to it, and as a consequence of this protest, Iraqi governing bodies have taken some steps by enforcing laws against cybercrimes in Iraq.

A study (Baeewe, 2021) has overviewed the particular act of cybercrime law designed by the legislative bodies, its concept, which is providing legal protection to the individuals using technological devices, and the maintenance of their security from any misuse through the technology, amendments, and the aspects it covered and highlighted the deficiencies in the law.

The academia in Iraq has focused on the awareness of cybersecurity among the students; in this perspective step, a study investigated the impact of cyber education, cyber training, internet applications, creative behavior, and information security on digital awareness, and they have found a significant correlation between all the factors and reflected the importance of courses to improve the literacy about cybercrimes and to prevent the youth from this crime (Tarrad et al., 2022). A systematic review collected data about the cybersecurity status in Iraq, and they have highlighted the prevailing risk associated with the current cybersecurity, the need for decisive legislative actions, and policy developments to overcome the arising risk of new trends in cybercrimes (Abdullah et al., 2022).

Another study has provided a thorough knowledge about the aspects Iraq must focus on to match the cybercrime rate with developed countries and overcome the political and economic challenges of cybercrime prevention (Shubbar, 2022). The main improvements Iraq should focus on were policy changes, international agreements, innovative technologies implementations, combining national CERT with the cyber agency, increasing investments, and developing the digital commerce sector. From the governance perspective, a study has evaluated the impact of hatred speech forms and causes on the behavior and approach of individuals (Bajraktari, 2023), and they have manifested that by good governance of a favorable legal and judicial system and the control over the hatred speech and negativity by the constitution of government can overcome the negative cause of hate speech.

The studies from the literature have illustrated the current status of laws and regulations in Iraq, the drawbacks in their existing laws for cybersecurity, the lack of awareness, the need for political and policy reforms, and the low rate of investment against cybersecurity. And the researcher has found, as such, no empirical evidence concerning the administrative rules for the organizations to prevent them from the hazards and damages of cybercrimes highlighting a significant gap and factor hidden from the eyes of researchers and practitioners. The knowledge from the literature can be summarized in one line Iraq has a very weak legislative system against cybercrimes, and there has been no considerable focus on the administrative regulations for the cybersecurity and protection of the organizations.

Considering all these collected points, this study has focused on the legislative and administrative cybercrime laws and has explored the limitations and further expending of effective governance within Iraq.

3. Method

3.1. Research Philosophy

This chapter will analyze the research methodologies and techniques that could be useful to determine and obtain generalized results that would effectively satisfy the objectives of the current study. Research philosophy is an investigator's basic research paradigm before proceeding through the data collection procedure. Based on the literature review and the research framework, the researcher has utilized the interpretivism philosophy to pursue the methodological procedure for the present investigation. It has been observed that interpretivism philosophy utilizes the formulation and analysis of norms and perceptions and understands the experiential and social aspects of the research (Junjie & Yingxin, 2022). However, this investigation has focused on understanding the applicability of cybercrime laws in Iraq from the legislative and administrative perspectives, and the research objectives will be explicitly fulfilled by applying the interpretivism philosophy.

3.2. Research Methodology

This research has utilized qualitative research methodology to determine the recent legislative frameworks thus implemented in Iraq regarding cybercrime, analyze the administrative measures that have been implemented in Iraq to lessen the cybercrime risks in the country along with their effectiveness and adequacy and determine the limitations of the imposed cybercrime laws in Iraq. The reason behind utilizing qualitative methodology is that the researcher wants an in-depth analysis of the research objectives, and qualitative methodology will be the most appropriate methodology for the present study, as it involves a detailed analysis of the data thus gathered from the research respondents. Moreover, it has utilized the inductive research approach and interpretivism philosophy, which provides the foundation for implementing qualitative research methodology for the present investigation, enabling the investigator to focus effectively on the purpose of the research.

3.3. Sampling Strategy and Unit of Analysis

The sampling strategy that has been utilized within the context of Iraq is the purposive sampling technique. Because purposive sampling technique will allow

choosing the correct research sample that will help gather authentic responses from the chosen sample regarding the laws thus executed in Iraq to avoid any risks from cybercrime at the administrative and legislative level, and it will support the aim of enhancing the depth of the gathered knowledge (Campbell et al., 2020).

Unit of analysis refers to the population the researcher has focused on for collecting data regarding the perspectives of particular research. The population thus targeted as the focus group of the present study is legal experts from Iraq, and the research respondents will be provided with a briefing regarding the scope of the research and purpose of the study because it is a necessary attribute so that the research respondents could effectively understand the research application and perspectives and scope and can easily proceed through the data collection procedure. The chosen research methodology, researcher has chosen a sample size of 8 legal experts from Iraq. The sample size is small because of the qualitative methodology and to avoid any thematic saturation in the responses.

3.4. Data Collection Instrument

Based on the qualitative methodology, the current research has focused on analyzing the laws for controlling cybercrime in Iraq to address their limitations and expand their perspective to achieve effective governance within the country. To collect the data from the research respondents, the prime tool that the researcher has used is semi-structured interviews where the interview contains qualitative questions regarding the application of legislative and administrative laws for mitigating cybercrime in Iraq which will be useful for identifying the challenges faced by the country regarding the execution of these laws, determine their shortcomings, and understanding the measures that could be feasible for enhancing the governance in Iraq.

3.5. Data Analysis

For collecting the data, the most appropriate research sample has been chosen by the researcher that could provide effective and required answers for the asked questions within the interview, and the data thus collected from the research respondents will be utilized for further analysis based on the NVivo software for codification and to achieve generalized and desirable results. In addition, NVivo is primarily utilized to configure the data regarding the qualitative methodology, which is why this software was chosen. After that, the gathered data will be utilized further for thematic analysis because it has helped the researcher analyze the data effectively and avoid repetition in the responses.

4. Results

After gathering the edited transcription, thematic analysis was conducted, and important themes and subthemes were formulated to address the proposed research objectives. These themes are discussed below:

- Theme I: Cybercrime Challenges
- Theme II: Cybercrime Legislation in Iraq
  - Theme IIa: Limitations
  - Theme IIb: Administrative Measures

- Theme III: Updated Cybercrime Legislation
  - Theme IIIa: Role of Government and Law Enforcement Agencies
  - Theme IIIb: Cybercrime Governance
- Theme IV: Improvement in Cybercrime Legislation

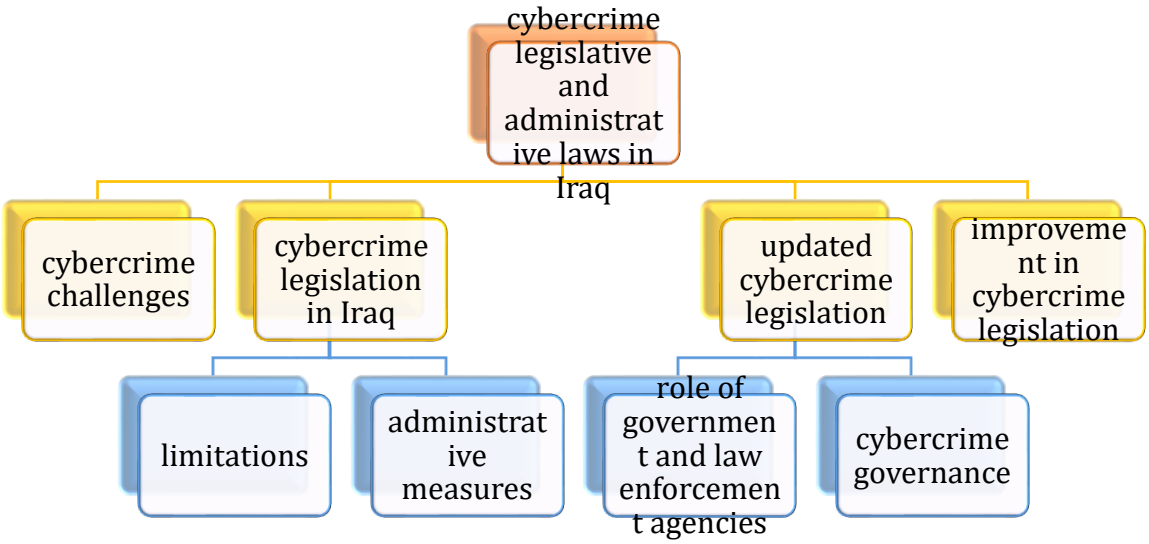

Figure 1. Mind map of thematic analysis

- *Theme I: Cybercrime Challenges*

According to 3 participants, different cybercrime challenges have been observed from the legal perspectives in Iraq. These respondents believed that the law enforcement agencies in Iraq lack effective resources, expertise and training to investigate cybercrimes, negatively impacting the safety of the associated individuals and companies. The government of Iraq is also unable to take important measures to prevent or reduce cybercrimes, leading to ineffective outcomes. In this regard, one of the participants stated:

"Due to limited resources and investments, Iraq cannot implement effective cybersecurity measures, providing various opportunities for cybercriminals to carry out illegal activities."

- *Theme II: Cybercrime Legislation in Iraq*

Five participants highly criticized Iraq's legislative framework concerning cybercrimes. According to them, Iraq's laws and regulations are outdated and not updated according to the continuously evolving cyber threats and technology. As a result, the country cannot effectively protect its people against cybercrimes. However, no particular legislation regarding cybercrime has been implemented in Iraq, which also worsens the situation for the people or companies suffering from cybercrimes. In support of this argument, one of the participants stated:

"There is no specific legislation regarding cybercrimes in Iraq, and the judiciary implements the provisions of Iraqi Civil Code No. 40 of 1951. This prevents an effective investigation of cybercrimes in Iraq."

- *Theme IIa: Limitations*

Different limitations are observed in the cybercrime legislation in Iraq, which prevent effective implementation of cybercrime law and regulation. Four participants stated that no specification concerning the cybercrime laws is presented in the legislative framework of Iraq, which also prevents effective international coordination for dealing with cybercrimes. Moreover, the provisions in the associated legislation are also outdated, impacting the efficiency of the cybercrime investigations in Iraq. Within this context, one of the participants stated:

"Inadequate penalties are presented in the Penal code for cybercriminals, which negatively impact the overall legislative framework of the country, leading to insignificant outcomes."

- *Theme IIb: Administrative Measures*

According to three participants, a multi-faceted approach is required to mitigate the cybercrimes in Iraq. For this purpose, the collaboration between the law enforcement agencies, government, public and private sectors is crucial. Therefore, different administrative measures must be taken to mitigate cybercrimes in Iraq. Many participants have also supported this argument, as one of them said:

"Developing an effective national cybersecurity strategy is crucial to deal with cybercrimes in Iraq."

- *Theme III: Updated Cybercrime Legislation*

The cybercrime legislation is needed to be amended to keep pace with the evolving cybercrime technology and threats. Six respondents believed that cybercrime legislation and administrative laws in Iraq do not address the technological advancements in cybercrimes which lack an effective implementation of a cybercrime legislative framework in Iraq. However, in 2020, a "new anti-cybercrime bill" was passed by the "Iraqi Council of Representatives." This bill highlights different cybercrime acts and also presents penalties for such acts. However, the council members focused on maintaining a balance between cybercrimes and imposed penalties. In this regard, one of the respondents said:

"The new 2020 anti-cybercrime bill was also unable to incorporate important amendments in association with the continuously advancing cybercrime technology, which can create various hurdles for the associated agencies to carry out effective investigations concerning cybercrimes in Iraq."

- *Theme IIIa: Role of Government and Law Enforcement Agencies*

Four of the participants emphasized the role of the government of Iraq and law enforcement agencies to develop and implement effective laws and policies to reduce and prevent cybercrimes in Iraq. They believed that the lack of effective resources and manpower prevent the law enforcement agencies in Iraq from taking important measures to prevent cybercrimes. In this regard, one of the participants said:

"In my opinion, the government of Iraq has been unable to protect its individuals and companies from cybercrimes due to limitations in the cybercrime legislative. Additionally, the lack of effective funds and investments also impacts the role of law enforcement agencies in reducing cybercrimes in Iraq."

- *Theme IIIb: Cybercrime Governance*

Six of the participants emphasized on Penal Code for cybercrime governance in Iraq. They believed that Penal Code includes specific provisions that can be applied within the context of cybercrimes, including data theft, online fraud and unauthorized accessibility to computer systems. However, the lack of particular cybercrime provisions resulted in various challenges for prosecuting cybercriminals in Iraq. Three participants also highlighted the "E-Signature Law of Iraq no. (78) of 2012" implemented for electronic transactions to prevent online fraud. In this regard, one of the participants stated:

"Even though there is no specific provision concerning cybercrimes in Iraq, the E-Signature Law of Iraq no. (78) of 2012 is utilized for electronic transactions."

- *Theme IV: Improvement in Cybercrime Legislation*

When asked about the suggestions for improving cybercrime legislative and administrative laws to reduce or prevent cybercrimes in Iraq, four participants emphasized the development of specific cybercrime legislation in Iraq to highlight different penalties within the context of associated cybercrimes. However, two of the participant also encouraged the international collaboration between Iraq and other international organizations to combat cybercrimes in the country. In this regard, one of the participants stated:

"I believe specific cybercrime provisions must be made to ensure effective investigation of cybercriminals by associated agencies. This approach can be effective in reducing cybercrimes in Iraq."

Figures 2 and 3 show the treemap and project map for the conducted thematic analysis.

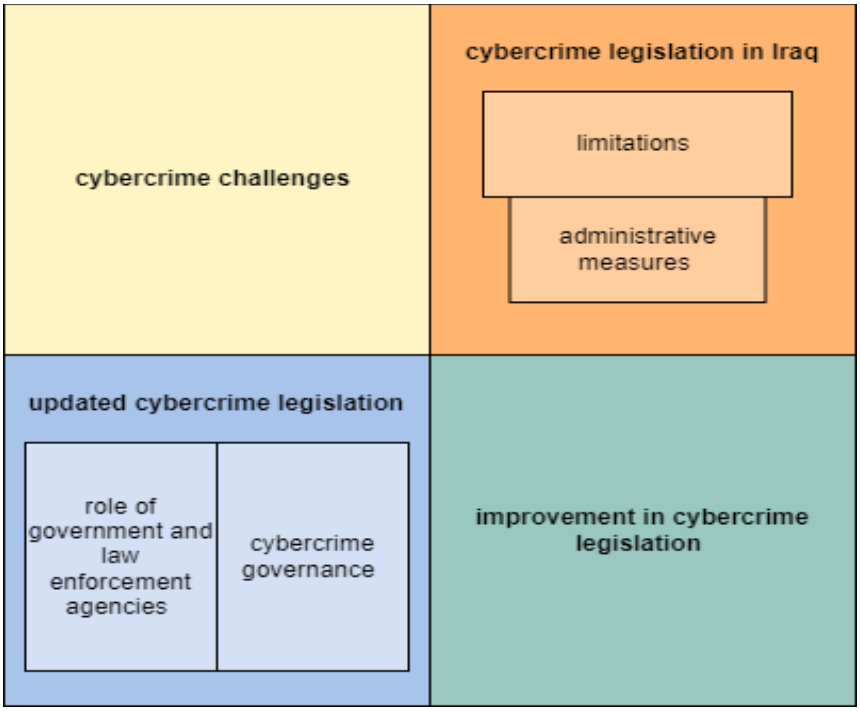

Figure 2. Treemap of thematic analysis

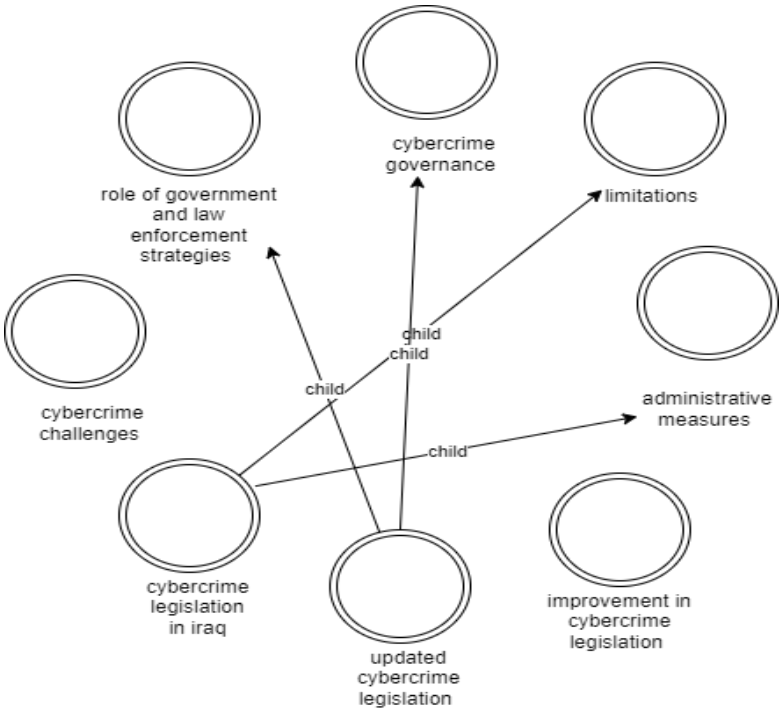

Figure 3. Project map of thematic analysis

5. Discussion

This study aimed to investigate the role of cybercrime's administrative laws, explore the associated limitations, and provide suggestions for the effective governance of Iraq. This study has collected data qualitatively through interviews from 8 legislative experts and questioned different concepts regarding the current administrative legislations of Iraq, and they provided various significant perceptions and suggestions. The collected data after thematic analysis were summarized into four themes; the first theme reflected the challenges regarding the cybercrimes prevailing in Iraq, highlighting the lack of effective strategies for cyber-control, weak investigation system, and the inability of the government to take effective measures because of lack of resources, these challenges have been highlighted by (Tarrad et al., 2022), providing the empirical support for our explored concept. The second theme has highlighted the ineffectiveness of the implemented cybercrime legislation and no proper idea of cybercrimes and the provisions about its concerned concepts causing a positive increase in cybercrimes, and literature, a study (Baeewe, 2021) has contended about the absence of any particular act concerning the cybercrimes and its prevention and the failure of their laws developed a long time ago. The third theme has been comprised of different sub-themes, mainly reflected on the lack of governance and effective agencies for the control of cybercrimes, and they provided the ideology of E-signature law for electronic transactions but not covering the concept of cybercrimes and security under its head. Past studies have also mentioned the need for the government to take considerable actions by making different laws mainly concerning cybersecurity (Abdullah et al., 2022); the concept aligned our findings with the literature knowledge. Another study has investigated the cybersecurity level in private banks, and they have narrated the lack of trust of

customers while using online services because of low-security maintenance and limited policies implemented governed and regulated by the government for this purpose. The foremost developed theme has asked about the upgradation of the current legislative acts against cybercrimes, and the participants have dropped some suggestions considered and acted on by the government for the improvement of effectivity of existing judiciary laws. They said the government should construct a separate and fully owned governing agency for the proper law and order implementation and its maintenance against cybercrimes, should collaborate with international agencies and with different countries by different contracts for the improvement of existing legislations against cybercrimes, and make new laws mainly highlighting the construct of cybercrimes, cybersecurity, penalties, and the related concerned matters regarding these concepts. The researcher has explored the literature for the empirical support of these concepts and found a study (Jarjees Al-Tae, Al-Dhalimi, & Jabbar Al-Shaibani, 2020) that has discussed the need for adequate defensive measures against cyberspace and to increase the security for the safety of political, social, and economic interests. Another study has contributed a significant and comprehensive analysis of the current strengths and weaknesses related to the existing cybersecurity directory bodies and has proposed a strategy for the applications in the current laws and a checklist that has covered all the internal and external factors influencing the current legislative and administrative regulations (Al-Wasiti & Alazzawi, 2021).

6. Conclusion

This study has analyzed the legislative and administrative law's limitations and provided suggestions for effective governance. This study has concluded four different themes after the transcription of the collected data and has compiled the results and discussed the empirical supports for its findings. This study has revealed several limitations in the Iraqi legislative system. The results of the opinions of legal experts have contended the lack of proper and specific laws related to cybercrimes and their related terms, inadequate government policies, lack of resources, ineffective working of agencies, no appropriate separate working agency body against the cybercrimes and security, need of training of cybersecurity directors, more human resources to control the cyber-activities, the urgency to collaborate with different countries and cybersecurity agencies for the implementation of effective laws against cybercrimes and the strict maintenance of cybersecurity for the eradication of the cybercrimes from Iraq, public awareness about cybercrimes, and the particular definition of rules and penalties against the cybercrimes. All these limitations have been highlighted by this study to improve the governance against cybercrimes and security.

7. Implications

This study has targeted the administrative and legislative laws regulating Iraq and has concluded various significant findings in its discussion and result. This study has come up with different constructive practical and theoretical implications. This study has contributed a comprehensive knowledge about the legislative laws governing Iraq, the current status of these laws, the drawbacks and critical points of lagging and

need improvement, and several findings of the limitations existing in these laws. This study has enlightened future researchers about the current judicial status of Iraq from the perspective of Iraq and the critical points from the improvement of governance perspective.

This study also possesses some practical implications for policymakers and practitioners. This study has provided a deep view of the limitations prevailing in the current legislation against cybersecurity. The findings of this study will help the practitioners to have a better understanding of the reasons for the ineffective working of the administrative laws and the loopholes existing in the current legislative laws. This study has also been acquainted with the possible solutions that policymakers and practitioners should follow to improve cybercrime laws and to protect the nation and economy from the hazards of this issue.

8. Limitations and Future Research

Every research winds up with its discussion having some limitations in it, so this research also has its boundaries as limitations. This study has targeted only the legislative and administrative laws, mainly focusing on the concept of cybercrimes, and has not considered other civil laws under observation. This study has collected data qualitatively through interviews, and it has compiled its results based on a limited amount of data, but there was no quantitative data collection for the generalizability of these concepts from a broad spectrum of people. This study was conducted in the Iraqi sector only, so it has provided information on the current legislation on cybercrimes in Iraq.

This study has noticed some potential areas of research that can become a significant focus and the main crux of future studies. Future researchers can use the same idea of this study and can investigate it qualitatively in any other country; furthermore, they can target the same country by using a quantitative approach and can contribute to the generalizability of this study's concept. In the future, a comparative analysis can also be performed targeting two or more countries and can provide the most efficient legislation and administrative laws in one of the targeted countries.

References

AbdulAmeer, S. A., Saleh, W. R., Hussam, R., Al-Hareeri, H., Alghazali, T., Mezaal, Y. S., & Saeed, I. N. (2022). Cyber Security Readiness in Iraq: Role of the Human Rights Activists. *International Journal of Cyber Criminology, 16*(2), 1–14. https://doi.org/10.5281/zenodo.4766563

Abdullah, M. M., Ahmed, H., Hasan, A. A., Ali, D. B., Al-Maeeni, M. K. A., Gdheeb, S. H., & Salman, S. D. (2022). Designing Predictive Models for Cybercrime Investigation in Iraq. *International Journal of Cyber Criminology, 16*(2), 47–60. https://doi.org/10.5281/zenodo.4766566

Aboud, S. J. (2012). An overview of cybercrime in Iraq. *The Research Bulletin of Jordan ACM, 2*(2), 31-34. https://www.researchgate.net/publication/261876935

Al-Wasiti, Y. S. S., & Alazzawi, F. R. Y. (2021). Requirements of Formulating a National Strategy for Developing the Cybersecurity System in Iraq According to GCI. v4 (2019) Index. *Geographical Education (RIGEO), 11*(4), 49-71. https://doi.org/10.33403/rigeoo.800625

Baeewe, S. S. (2021). Cybercrime under the New Iraqi Draft Cybercrime Law. *Journal of the College of Basic Education, 2*(SI), 123-141. https://doi.org/10.35950/cbej.v2iSI.5724

Bajraktari, H. (2023). Human Rights and Good Governance to Identify Hate Crimes on Social Networks. *Corporate Law & Governance Review, 5*(1), 151–157. https://doi.org/10.22495/clgrv5i1p13

Campbell, S., Greenwood, M., Prior, S., Shearer, T., Walkem, K., Young, S., Bywaters, D., & Walker, K. (2020). Purposive Sampling: Complex or Simple? Research Case Examples. *Journal of research in Nursing, 25*(8), 652-661. https://doi.org/10.1177/1744987120927206

Chang, L. Y. (2020). Legislative frameworks against cybercrime: The Budapest convention and Asia. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 327-343). Palgrave Macmillan. https://doi.org/10.1007/978-3-319-78440-

Hasbullah, M. A. (2022). Identifying the Effects of Cybercrime on Business Laws: Implications for Businesses and Consumers. *International Journal of Cyber Criminology, 16*(2), 119-130. https://doi.org/10.5281/zenodo.4766569

Jarjees Al-Tae, A. K., Al-Dhalimi, H. A.-H., & Jabbar Al-Shaibani, A. K. (2020). Relationship of Cybersecurity and the National Security of the Country: Iraq Case Study. *Systematic Reviews in Pharmacy, 11*(12), 469-476. https://www.sysrevpharm.org/abstract/relationship-of-cybersecurity-and-the-national-security-of-the-country-iraq-case-study-67372.html

Jawad, H. (2017). *Cybercrime Legislation in Iraq*. Al Tamimi & Company. https://www.tamimi.com/law-update-articles/cybercrime-legislation-iraq/

Junjie, M., & Yingxin, M. (2022). The Discussions of Positivism and Interpretivism. *Online Submission, 4*(1), 10-14. https://doi.org/10.36348/gajhss.2022.v04i01.002

Kemp, S., Buil-Gil, D., Miró-Llinares, F., & Lord, N. (2021). When Do Businesses Report Cybercrime? *Criminology & Criminal Justice, 23*(3), 468-489. https://doi.org/10.1177/17488958211062359

Khan, S., Saleh, T., Dorasamy, M., Khan, N., Tan Swee Leng, O., & Gale Vergara, R. (2022). A Systematic Literature Review on Cybercrime Legislation. *F1000Research, 11*, 971. https://doi.org/10.12688/f1000research.123098.1

Le Nguyen, C., & 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

Li, X. (2015). Regulation of cyber space: An analysis of Chinese law on cyber crime. *International Journal of Cyber Criminology, 9*(2), 185-204. https://doi.org/10.5281/zenodo.56225

Lusthaus, J. (2013). How Organised is Organised Cybercrime? *Global Crime, 14*(1), 52-60. https://doi.org/10.1080/17440572.2012.759508

Mahmood, I. S. (2020). Are Cyberbullying Interventions and Criminal Law Prevention Effective?(A Review of Cyberullying Legislation in Iraq). *PalArch's Journal of Archaeology of Egypt/Egyptology, 17*(7), 16983-16998. https://archives.palarch.nl/index.php/jae/article/view/8899

Mohameed, D. A. A.-H., Shaker, R. M., AlRashidi, W. B., Al-Maeeni, M. K. A., Alghazali, T., Dawood, I. I., Al-Muttar, M. Y. O., & Mousa, M. Y. (2022). Violation of Patent and Intellectual Property in Iraq: A Perspective of Cybercrimes. *International Journal of Cyber Criminology, 16*(1), 70–88. https://doi.org/10.5281/zenodo.4766557

Nehme, T. (2020). Impasse of Cyber Laws: Iraqi Case. *Defence Magazine, 112*. https://www.lebarmy.gov.lb/en/content/impasse-cyber-laws-iraqi-case

O'Driscoll, D. (2018). *Governance and Development in Iraq*. Institute of Development Studies. https://opendocs.ids.ac.uk/opendocs/handle/20.500.12413/13862

Oni, S., Berepubo, K. A., Oni, A. A., & Joshua, S. (2019). E-Government and the challenge of cybercrime in Nigeria. In *2019 Sixth International Conference on eDemocracy & eGovernment (ICEDEG)* (pp. 137-142). IEEE. https://doi.org/10.1109/ICEDEG.2019.8734329

Rakhimova, U. (2020). Cybercrime subject and limits of proof. *TSUL Legal Report International electronic scientific journal, 1*(1), 1-110. https://legalreport.tsul.uz/index.php/journal/article/view/17

Shubbar, H. (2022). *Constructing an Interinstitutional and interministerial effort on Cyber Security in Iraq*. Al-Bayan Center for Planning and Studies. https://www.bayancenter.org/en/wp-content/uploads/2022/03/87tr6tdf.pdf

Siregar, G., & Sinaga, S. (2021). The Law Globalization in Cybercrime Prevention. *International Journal of Law Reconstruction, 5*(2), 211-227. http://dx.doi.org/10.26532/ijlr.v5i2.17514

Tarrad, K. M., Al-Hareeri, H., Alghazali, T., Ahmed, M., Al-Maeeni, M. K. A., Kalaf, G. A., Alsaddon, R. E., & Mezaal, Y. S. (2022). Cybercrime Challenges in Iraqi Academia: Creating Digital Awareness for Preventing Cybercrimes. *International Journal of Cyber Criminology, 16*(2), 15–31. https://doi.org/10.5281/zenodo.4766564

Tosoni, L. (2018). Rethinking Privacy in the Council of Europe's Convention on Cybercrime. *Computer Law & Security Review, 34*(6), 1197-1214. https://doi.org/10.1016/j.clsr.2018.08.004

Unctad. (2021). *Cybercrime Legislation Worldwide*. Unctad. https://unctad.org/page/cybercrime-legislation-worldwide

Urbas, G. (2015). *Cybercrime Legislation, Cases and Commentary*. Lexis Nexis. https://store.lexisnexis.com.au/products/cybercrime-legislation-cases-and-commentary-skucybercrime_legislation_cases_and_commentary

Appendix

Interview Questions

1. In your experience, what challenges are faced by Iraq in dealing with cybercrimes from a legal perspective?
2. In your opinion, how does the legislative framework in Iraq address cybercrimes? What limitations are observed in this regard?
3. According to your experience, what administrative measures can be taken to mitigate cybercrime risks within Iraq?
4. How can the cybercrime legislation in Iraq, be updated to keep pace with the evolving cybercrime technology?
5. In your opinion, what is the role of government and other law enforcement agencies in preventing cybercrimes in Iraq?
6. In your opinion, are there any provisions in the cybercrime legislation in Iraq which impact cybercrime governance? If yes, how can they be improved?
7. Can you provide any suggestions for the improvement in cybercrime legislative and administrative laws to reduce or prevent cybercrimes in Iraq?