

Criminalizing data breaches in Iraq and KRI: Proposing Legal solutions

Mahdi Nooruldeen

Bayan University

DOI: <https://doi.org/10.31918/twejer.2584ELI.13>

Published:2/11/2025

Abstract

As our world becomes more digitized, the connection between law, security, and data privacy has become a significant concern. Criminals are using digital technology for committing crimes. This paper investigates the developing landscape of legal security and data privacy and electronic crimes. It covers the impact of developing technologies on the privacy of individuals and society, the developing regulations of digital law and international agreements related to the future of data crimes and privacy protection, the requirements of practical legal strategies, and measures to protect privacy and prevent illegal digital actions. It also studies the ethical and criminal use of data privacy. Furthermore, data breaches and privacy violations are occurring daily. This paper also provides suitable solutions and best practices that describe the future of legal security and data privacy. As the nature of crimes changes, law, and digital regulations must be ready for this new challenge. Criminals are using the digital era illegally to obtain private interests, which is why European Governments and UK police and authorities take necessary steps to protect individual and public sector data privacy. This work will provide a law proposal for criminalizing data breach.

Keyword: Data Breach, Criminal Law, Privacy Violations, Digital Age, Cybersecurity.

Introduction:

Digital age, has brought many advantages and disadvantages to the new world. online security is becoming a necessary structure for Governments and individuals. With the increase of depending on digital tools by people, businesses, banks, and nations, cybersecurity has become more popular and serious than ever. However, using technology has also led to increase a significant issue regarding of cyber threats that can led to committing different type of crimes. It is important to take cybersecurity extremely serious and implement applicable measures to safeguard sensitive information. Worldwide law enforcements authorities are concerned about Data breaches, because it increases widely and it threatens the society and results in the loss of confidentiality in public and private sector. Moreover, vital, sensitive, and private information are in danger such as financial information, personal data, and health care. A data breach is unintentional in some cases it happens un intentionally but criminals over the world committing electronic and digital crimes intentionally to obtain illegal benefits. In the digital era, data has become one of the most life-threatening mechanisms of an enterprise, and data breach is a serious threat to organizations, including substantial reputational damage and financial losses. It is important to prevent data loss because it affects directly on public sector and it affects individuals negatively. A data breach is becoming a main concern of people, banks, institutes and organizations, because it enables criminals to steal money in bank account or take personal information used by an individual unauthorized to do so. The most common form of a data breach is an attacker hacking into a corporate network to steal sensitive data. Data breach can be defined as a confirmed case of unauthorized and unlawful access to the governmental or private database to obtain illegal personal benefits by stealing sensitive data, personal health care information or identity information, or taking trade secrets, or intellectual property.

Safeguarding the protection of individual and governmental data has become a major concern for people, organizations, and governments. The sensitivity of personal data held by various entities has raised important questions about privacy and security. Legal security in data privacy has emerged as a framework to support the trust of individuals in the systems that securely process their data. It is a legal framework that defines the rights and responsibilities of individuals and organizations in handling personal information and seeks to strike a balance between technological innovation and the imperative of safeguarding individual privacy. This work aims to illustrate the main aspects of the criminal implications of data privacy. The international community has taken significant steps to protect privacy rights, such as the (European Convention on Human Rights) and the (International Agreement on Civil and Political Rights). Both agreements aim to protect rights of individual privacy, and “Article 12 of the Universal Declaration of Human Rights” emphasizes that the law must protect everyone from digital attacks. This research also provides suitable solutions and best practices that describe the future of legal security and data privacy.

Technology Growth and Skills Improvement (Police Forces)

Police skills are necessary in the digital age because the services of police are changing nowadays. Before the digital age types of crimes were different such as theft, murdering people, and many other traditional crimes. However, electronic crimes are recognized such as drug trafficking, security hacking, cyberbullying, fraud, Identity theft, and many others, that’s why police forces need to be trained well to identify these new technology crimes. On the other hand, new technology suggests new tools to prevent various crimes from happening. Meanwhile, digital crime is expanding. The ratio of crimes like hacking and drug trafficking by using internet-enables has expanded significantly in recent years. The harm of drug trafficking, child abuse, and pornography has increased with the wide use of the internet.

Moreover, police forces are facing new challenges entitled to unknowable threats, from anonymous sources, which will cause many illegal consequences and harm private and public interests (Hitchcock, 2017). It seems clear that police forces need more training, technology tools, and new laws to protect society from Cyberattacks.

Police workers are bound by legislation and instructions from legal bodies (parliament) and the Government, the use of existing laws related to digital and technology crimes is not sufficient in Iraq and Kurdistan because of the growing technology very fast and the lack of new digital rules. This is also true for some other Middle Eastern countries. While the law is slow to respond to the growth of online threats it has a bad impact on public and private interests. Cybercrime is the main concern for the police nowadays, they must use new tools and new technologies to discover digital criminals and to catch them. Law enforcement is necessary for the stability and economic growth of any country. Furthermore, any legal problems arising need different methods to deal with such as online threats, cyberterrorism attacks, and many other digital crimes. The criminal justice processes must be up to date with the digital age to defeat technology criminals (Wall and Williams, 2007).

Police investigations play an essential role in safeguarding sensitive information in different sectors. When an individual, private organization, or government entity falls victim to a data breach, the first step police must take is to investigate to discover the nature of the compromised data and the extent of the breach. Law enforcement agencies normally cooperate with cybersecurity experts to trace the criminals, evaluate the vulnerabilities exploited, and collect digital evidence. This includes analyzing server logs, digital footprints, and network traffic, to identify potential sources of the breach or suspects. Moreover, investigators work to secure the compromised systems, contain the breach, and mitigate further damage to stop additional data

loss. In cases involving governmental departments, specialized unit forces will participate in the investigation due to their difficulty and potential national security implications, cooperating with other law enforcement agencies and intelligence services to identify suspects and arrest them (Allahrakha, 2023).

As technology is always in progress, investigation procedures must use new tools and new technologies to fulfill the development. Law enforcement agencies in data privacy and technology breach cases often influence advanced scientific techniques to recover deleted or encrypted data and trace financial transactions linked to cyber criminals. The police forces should work with legal experts to obtain search warrants and orders to gather evidence from service providers and technology companies. In the private sector, assistance and collaboration between law enforcement and affected organizations is vital, as sharing information about the breach helps in tracking down criminals and avoiding future attacks. Furthermore, authorities may be involved in international cooperation when the breach involves cross-border cybercrime, as extradition and coordination with authorized law enforcement agencies in other jurisdictions become necessary to arrest suspects and bring them to justice. Eventually, the investigative process in data privacy and technology breaches requires different methods, combining digital forensics, legal techniques, and international collaboration to protect governmental sectors, individuals, and the private sector, from the increasing threat of cybercrime (Schwartz and Janger, 2007).

It seems obvious, that investigations into data privacy breaches and legal security need newly developed technology because of the massive growth of digital technology, to protect public and private interests some necessary steps are needed, intensive technology training is important for the police forces with cooperation with IT experts and intelligence agencies to

identify suspects and sources of the illegal technology actions, to arrest criminals and bring them to justice.

Data Protection Policies from a Legal Perspective:

It is vital to have strong legislation to protect individuals and Governmental sectors from breach or misuse of internet platforms. Europe has a great law for data and technology protection, and this work will shed light on them with other US and Middle Eastern technology laws.

Regulations and data Protection Laws

Data protection regulations and laws are important for preventing digital crimes, such as (GDPR) the “General Data Protection Regulation in Europe” and (CCPA) the “California Consumer Privacy Act” in the United States, which have led to a new era of data privacy. GDPR, for instance, lays out inclusive regulations governing the storage of personal data and data collections, managing. According to GDPR, individuals have the legal rights to know how their personal data is being used, the ability to request data erasure, then the power to grant or withhold confirmation for data processing. These laws serve as a strong legal framework for safeguarding personal information, ensuring that organizations handle data with extreme care (Kuner, 2012).

Data Breach Notification

One of the critical aside of legal security in data privacy is the requirement for organizations and online platforms to inform individuals and relevant police forces in case of a data breach. The GDPR obligates administrations to report data breaches within 72 hours of becoming

aware of them, for instance, “the Equifax breach in 2017”, has discovered the consequences of inadequate data breach notification. The legal obligation to notify affected individuals and authorities ensures transparency and empowers individuals and public sectors to take action to protect their data (Purtova, 2018).

Access Rights and duties

Data privacy laws grant individuals particular rights, containing the right to access their data, accurate and re-right their incorrect data, and request to delete some data. Notably, “the case of Google Spain v. AEPD and Mario Costeja González” in the European Court of Justice established the right to be disregarded as a fundamental aspect of data privacy. These vital rights authorize individuals to have fully control over their personal information and hold establishments responsible for its proper management (Lynskey, 2017).

Data Security Measures

It is significant to guarantee the security of individual and governmental data as a legal requirement in data privacy. Countries and Organizations are obligated to apply appropriate security plans to protect data from illegal access, expose, or criminals. The Yahoo data breach of 2013, which has affected billions of user accounts, was a great reminder of the consequences of inadequate and weak data security measures. Moreover, Legal provisions demand that organizations adopt strong security practices, safeguarding individuals, and official departments from data breaches and cyberattacks (Hoofnagle, Sloot and Borgesius, 2019).

Responsibility and Enforcement.

Legal security in data privacy makes clear that organizations are accountable for data protection violations. Furthermore, Data protection authorities have the power and authority to investigate

and impose penalties for non-compliance. In addition, the United Arab Emirates, as one of the important developing countries has been experiencing rights and duties for using technology in recent years. UAE has new legislation about technology law. However, in the case of technology developments must follow the advanced new protection laws worldwide. In the modern world, there are many options for a country to improve its cyber-security, by cooperating with many international agencies and organizations (The National, n.d).

Data Transfer

Data transfers are common particularly in cross borders, especially in an increasingly globalized world. Legal security in data privacy illustrates the complex issue of data transfer regulations, ensuring that personal data must be protected even when it moves across international borders. International agreements, such as the agreement of Europe with the US Privacy Shield (which was invalidated in 2020), have established frameworks for secure data transfers among countries. The plan of deciding to protect data privacy by the European Court of Justice further highlighted the significance of strong legal safeguards and protection for cross-border data transfers (Brown, 2010).

Cybercrime Legislation and Data Protection Regulation in Iraq

Iraq currently has an unregulated internet sector, which makes it one of the freest markets globally. However, this also leaves it vulnerable to cyber threats, making it obligatory to improve legal, technical, structural, and capacity-building essentials to provide inclusive cybersecurity for its citizens, businesses, private sector and the state, especially given the current political and security situation in the country.

There is a lack of electronic and internet regulations on the types of cybercrime in Iraq, and the government hardly publishes any information on it. However, previous reports announced by the Iraqi government reveal the most common types of cybercrime in Iraq, which have increased in the recent years. In 2013, the Iraqi Ministry of Planning described that most digital crimes are generally guided and shared through social media platforms, mainly Facebook, and is mostly directed towards individuals more than businesses or government agencies. The most shared types of cyberattacks include cyberspace fraud, fake identity, child abuse pornography, , cyber-blackmail, copyright violation, cyber-stalking , satellite piracy, and cyberterrorism (Jawad and Omer, 2017).

According to Data Guidance (2021), although Iraq currently does not have a inclusive data protection law applicable to private organizations, it has established a law that governs privacy within the public sector. The right to have a digital privacy is also recognized in the Iraqi Constitution, which acknowledges that it is necessary to balance it with other individuals' rights and public morals. Additionally, the country has enacted legislation that regulates privacy and confidentiality in certain sectors such as financial services, healthcare, telecommunications, and labor. The Iraqi Government is currently working on a cybercrime law, replacing an earlier draft that was abandoned in 2013 due to difficulties within the country and concerns about compliance with international standards.

In Iraq the protection of data is not governed by a single codified law. Instead, it is briefly covered by numerous laws, including the Constitution of Iraq, the Iraqi Penal Code No. 111 of 1969 , “the Iraqi Civil Code”, and other sector-specific related laws such as banking laws, securities, labor, and tax laws. Furthermore, while a particular data protection law has lately been approved, it only affects and applies to government bodies. There are currently no data

protection initiatives for the private sector in Iraq. However, the government has been studying the introduction of a law of cybercrime for the time being in order to understand more about the side effects of cybercrimes (AL Dabbagh, 2023).

Applicable Legislation

There is also a proposal presented in 2011 by Presidential Council of Iraq, a draft law called the “Iraqi Information Crimes Law”, the draft aimed to regulate the use of electronic devices, information networks, and computers. However, the proposed legislation faced significant criticism from local and international communities as it violated international standards that protect freedom of speech, association, and due process. As a result, the Iraqi parliament, rejected the draft law on 6 February 2013 after receiving a letter from the Culture department and Media Agency addressing the head of the Council and facing strong objections.

Currently, Iraq doesn't have any specific legislation governing cybercrime. In cases concerning cybercrime, the judiciary must apply provisions from sector-specific laws like the Banking Law of 2004 and Communications and Media Commission Law CPA Order 65 of 2004, as well as the Iraqi Civil Code No. 40 of 1951 and Iraqi Penal Code No. 111 of 1969.

Moreover, Iraq doesn't have any particular laws on data safety, and privacy protection under the Civil Code remains mainly not improved. While the Iraqi Constitution of 2005 recognizes the "right to personal privacy," there is no guidance or definition of this right in lawmaking.

Operating existing legislations In Iraq

As mentioned in previous paragraphs, cybercrimes are threatening the society, such as internet fraud, using other personal identity without a permission, child abuse and pornography, cyber-

stalking, cyber-blackmailing people, copyright violation, and cyberterrorism are widespread in Iraq. Although the Iraqi Penal Code states the criminal nature of these criminals, it can't be successful to incorporate their 'cyber' element effectively.

Any individual imprisoned of cybercrime relating violence, sexual abuse, threats, or guidance may face penalties according to Articles 393 and 394 of the Penal Code:

According to Article 393, a person can face imprisonment for not exceeding than 7 years (or 10 years if the victim is younger than eighteen years of age) if they assault another using force, threaten, manipulate, or violate the dignity of another male or female, or initiate such violation.

Every person found guilty of a cybercrime with involvement of copyright violation may be penalized according to Article 45 of the Copyright Law. The copyright owner can seek legal remedies under Article 45, including. The following are the actions that can be taken against infringers:

- Orders them to stop infringing actions.
- Taking and using the original, copies, and supplies used to create infringing copies.

Any individuals committed of cyberterrorism must face penalties according to the Anti-Terrorism Law No. 13 of 2005. Moreover, harmed persons have the right to report claims for compensations caused to them by virtue of said damages, according to the Civil Code.

Ensuring Legal Security in the Digital Age in Iraq

Iraq is one of the republic states in the Middle East that faces significant challenges in data protection policy. In 2011, the Committee of Media and Culture in the Iraqi Parliament presented a draft law on Data Technology Crimes (Cybercrimes' draft law, 2011) but it was removed in 2013 when it faced a lot of pressures from organizations, civil society and human rights departments. Their major disagreement was that certain regulations in the draft law disadvantaged and violated the rights of people from freedom of expression. It was not recognized by the Iraqi parliament, which is why the withdrawal decision was easy to make. It reintroduced the legislation draft with minor changes once again in 2019 with a different title, "Combating Cybercrimes Law, 2019. There were countrywide objections led by the UN organizations such as Human Rights Watch alongside the re-establishment of the Combating Cybercrimes law, focused by human rights activists and reporters, who were challenging the individual's right to practice their right to the expression and independence of opinion. Furthermore, in 2021 another efforts was made by Iraqi authorities to impose the draft law but it was rejected by UN and Iraqi protesters because it was against the rights of freedom of expression. It was never the law of data protection or privacy of people it was the draft for threatening people not to express their ideas freely (Abdulhamza, 2022).

With the increasing and widening numbers or criminals of hacking and cyber-attacks, people are becoming more vulnerable to extortion and theft. Unfortunately, in Iraq and Kurdistan region, there are no legal solutions in place to address these crimes. As a result, we are proposing a new law to combat this issue, which is attached to this research. Our proposed law would replace the outdated 1969 Penal Code number 111, which is no longer effective in dealing with the rapid digital changes of today's world. It is very important to encourage

Kurdistan parliament and Iraqi parliament to adopt and regulate cybercrime law. This work will provide a significant project to the authorities and legislators to work on creating cybercrime law, in order to addresses these digital crimes and punish criminals and protect the society. This work suggests a significant proposal which is prepared based on various digital crime laws for instance, United Arab Emirates, European countries, and the US. It provides different types of punishments and ensuring that the criminals of these crimes are must be brought to justice. It is necessary to create such an important legislation to prohibit criminals from doing illegal actions against public and private sector. Furthermore, necessary steps must be taken to protect people from hacking and other illegal actions. This proposal is the best solution for preventing cybercrimes, and we hope that the Kurdistan parliament and Iraqi parliament will create and adopt these kind of proposal quickly to protect the society from these crimes.

Conclusion

In conclusion, internet breach is a primary concern nowadays. EU counties and many other counties are focusing on creating new laws to protect their society and people. Kurdistan and Iraq are having lack in digital laws. It is vital to establish and regulate particular laws about data breach and illegal use of internet. Providing data privacy for individuals is one of important and essential works of Government through police forces and courts. To protect individual and public interests we need to have a modern and developed digital laws. Authorities must provide security and safety for people. The legislature brunch must create and provide necessary electronic laws. The Government as an executive brunch must implement these laws to protect private and public interests. The police forces and courts have to be trained to be able to defeat

criminals. Moreover, new technical enforcement mechanisms are needed to protect people from data breaches. It is significant to maintaining people's trust in the digital system, this trust can be achieved by providing new digital laws.

The Internet is an exclusive area that requires specific regulations. Laws that control different forms of media may not be effective in governing this medium. Attempting to apply them to the internet may create irregularity and uncertainty in their application. It is important to establish regulatory approaches that are designed exclusively for the internet and the illegalization of e-crimes. Although the regulations of Penal Code, provisions of Civil Code, and sector-specific laws that deal with electronic-transactions provide some level of cybersecurity, it is hoped that the Iraqi parliament will adopt new laws that precisely relate to cybercrime. Implementing and applying particular and wide-ranging cybercrime regulation will enable judicial reliability on the subject and enable the implementation of the law. Moreover, due to the increasing number of hacking and cyber-attacks, people are being hacked and extorted for money. Unfortunately, there are no legal solutions in Iraq and Kurdistan region to address these crimes. Therefore, we are proposing a new law to combat this issue and attach it to this research. The proposed law would replace the outdated 1969 Penal Code number 111, which is ill-equipped to handle the rapid digital changes of today's world. We urgently recommend presenting this project to the Iraqi parliament to criminalize cyber-attacks and create an official law to address these crimes. Our proposal is based on laws from Emirates, Europe, and the US and is attached to this research.

Reference list

- Abdulhamza, S.M. (2022). The Iraqi Legislative Policy to Protect National Cyber Security A study in the light of the principles of public international law. Lark Journal for philosophy, Linguistics and social Sciences, [online] 3(46 1ج). Available at: <https://www.iasj.net/iasj/article/236956> [Accessed 11 Mar. 2024].
- AL Dabbagh, A. (2023). *Iraq - Data Protection Overview*. [online] DataGuidance. Available at: <https://www.dataguidance.com/notes/iraq-data-protection-overview> [Accessed 4 Nov. 2023].
- Allahrakha, N., (2023). Balancing Cyber-security and Privacy: Legal and Ethical Considerations in the Digital Age, Tashkent State University of Law. 4. (2), p. 12.
- Brown, I., 2010. Communications Data Retention in an Evolving Internet. International Journal of Law and Information Technology. Vol. 19, No. 2, pp. 95-109. Available at: <https://ssrn.com/abstract=1683284>.
- DataGuidance. (2021). *Iraq*. [online] Available at: <https://www.dataguidance.com/jurisdiction/iraq> [Accessed 4 Nov. 2023].
- Hitchcock, A., 2017. Bobbies on the Net: a police workforce for the digital age, reform police (p. 16).
- Hoofnagle, C.J., Sloot, B.V., & Borgesius, F.Z. (2019). The European Union general data protection regulation: what it is and what it means, Information & Communications Technology Law. 28(1), pp. 65-98, DOI: 10.1080/13600834.2019.1573501. Available from: <https://doi.org/10.1080/13600834.2019.1573501> [Accessed 27 October 2023].

- IBM (2023). *What Is a Data Breach?* | IBM. [online] www.ibm.com. Available at: <https://www.ibm.com/topics/data-breach> [Accessed 8 March 2024].
- Jawad, H. and Omer, A. (2017). *Cybercrime Legislation in Iraq*. [online] Al Tamimi & Company. Available at: <https://www.tamimi.com/law-update-articles/cybercrime-legislation-iraq/> [Accessed 4 Nov. 2023].
- Kuner, C., 2012. The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law, Privacy and Security Law Report. p. 9.
- Lynskey, O. (2017) 'The "Europeanisation" of Data Protection Law', *Cambridge Yearbook of European Legal Studies*, 19, pp. 252–286. doi:10.1017/cel.2016.15.
- Purtova, N., 2018. The law of everything. Broad concept of personal data and future of EU data protection law, *Law, Innovation and Technology*. 10(1), p.13.
- Schwartz P.M., & Janger, E. J., (2007). Notification of Data Security Breaches, *Michigan law review*. p. 942.
- The National. (n.d.). *25,000 e-crime reports registered in Dubai as cyber attacks increase during pandemic*. [online] Available at: <https://www.thenationalnews.com/uae/government/25-000-e-crime-reports-registered-in-dubai-as-cyber-attacks-increase-during-pandemic-1.1232985>. [Accessed 27 October 2023].
- Wall, D.S. and Williams, M., 2007. Policing diversity in the digital age: Maintaining order in virtual communities, *Criminology & Criminal Justice*. 7 (4), p. 4.

Cybercrime law proposal

- **Article one**

Definitions: This provision aims to establish clear definitions for various cyber and electronic crimes, ensuring a shared understanding for the lack that exists in Iraqi cyber laws, this provision will address all cyber-crime issues.

- **Article two**

Penalties: This section outlines the penalties that will be imposed on individuals convicted of cyber-crimes, with punishments tailored to the severity and impact of the offense.

1. Identity Theft: criminals who engage in identity theft, such as stealing personal information to impersonate someone else online, could face imprisonment ranging from 1 to 3 years, depending on the severity of the offense, along with fines (compensations) equivalent to the financial damages caused to the victim.

2. Phishing: criminals involved in phishing scams, where they deceive others into sharing sensitive data like PINs or credit card numbers, may be subject to imprisonment for 1 to 5 years and fines proportional to the financial losses incurred by victims.

3. Hacking Public and private sector: Perpetrators who attacks public sector for illegal purposes which disrupt the normal functioning of a Governmental computer network, could face imprisonment for 2 till 10 years and fines reflecting the economic impact of the attack. However, hacking into the private sector led to imprisonment for 1 to 5 years and compensation reflecting the economic impact of the attack.

4. Cyberbullying: Criminals who involved in cyberbullying, including harassment, intimidation, or spreading malicious rumors online, may be subject to imprisonment for 1 to 5 years and fines from 3 to 5 million Iraqi dinar, those who aimed at compensating victims for emotional distress and other damages.

5. Cyber Extortion: Criminals involved in cyber extortion, where they threaten to release sensitive information or launch attacks unless they pay amount of money, could face imprisonment for 5 to 7 years and fines from 5 to 10 million or fines equivalent to the ransom demanded or the damage caused.

6. Data Breaches: Perpetrators who illegally access, steal, or disclose sensitive data through data breaches may be subject to imprisonment for 5 to 10 years and fines reflecting the value of the compromised data and the extent of harm caused to affected individuals or organizations.

7. Online Stalking: perpetrators who engage in online stalking, repeatedly harassing or threatening someone through various online platforms, may be subject to imprisonment for 1 to 5 years and fines from 1 to 3 million dinar aimed at compensating victims and deterring future harassment.

The above-mentioned penalties and legal remedies aim to prevent cybercriminal behavior, protect individuals and organizations from harm, and uphold the principles of justice in the digital realm. However, many other digital crimes can be added to this provision.

- **Article Three**

Jurisdiction: It explains the jurisdictional boundaries within which law enforcement agencies can investigate and prosecute cyber-crimes, penal code No 111 of year 1969 which does not contain these new cybercrimes. This law has jurisdiction over all digital and Cybercrimes.

- **Article Four**

Investigative Powers: This provision grants law enforcement agencies the necessary authority to conduct digital investigations, including surveillance and evidence collection, while also emphasizing the importance of judicial oversight and privacy protections.

- **Article Five**

Cybersecurity Measures: It encourages the adoption of robust cybersecurity practices by organizations to reduce cyber risks effectively, thereby enhancing overall cybersecurity strength.

- **Article Six**

Victim Support: This article establishes mechanisms to provide comprehensive support and assistance to victims of cyber-crimes, addressing their psychological, financial, and legal needs by supporting them according to laws and protecting them by the Government.

- **Article Seven**

International Cooperation: This article encourages and bound authorities to participate and implement international conventions and underscores the importance of international collaboration and information sharing in addressing transnational cyber threats, emphasizing the need for partnerships with foreign governments and organizations.

- **Article Eight**

Everyone must be subject to these provisions; this law has supervision over all other existing laws in terms of digital crime.

- **Article Nine**

Each of these provisions is crucial for the effective anticipation prohibition, investigation, and trial of cyber-crimes, as well as for the protection of individuals' digital rights.

- **Article ten**

This law must be published in the official Magazine of ministry of justice before its implementations, and it is considered applicable after one month from publishing this law in (waqa'e) magazine.

خلاصة:

مع تحول عالمنا إلى عالم أكثر رقمية، أصبح هناك مخاوف و قلق كبير من قبل القوانين والامن بالنسبة لجرائم المرتبطة بالتكنولوجيا . يستخدم المجرمون التكنولوجيا الرقمية لارتكاب الجرائم. تبحث هذه الرسالة في المشهد المتطور للأمن القانوني والجرائم الالكترونية وخصوصية البيانات. ويغطي تأثير تطوير التقنيات على خصوصية الأفراد والمجتمع، ومتطلبات الاستراتيجيات القانونية العملية، وتدابير حماية الخصوصية ومنع إجراءات الأنشطة الرقمية غير القانونية. كما يدرس الاستخدام الأخلاقي والإجرامي لخصوصية البيانات. علاوة على ذلك، تحدث خروقات البيانات وانتهاكات علي شبكة الانترنت يوميا. توفر هذه البحث أيضا الحلول المناسبة وأفضل الممارسات التي تصف مستقبل الأمن القانوني والجرائم الالكترونية. مع تغير طبيعة الجرائم، يجب أن يكون القانون واللوائح الرقمية جاهزة لهذا التحدي الجديد. يستخدم المجرمون

العصر الرقمي بشكل غير قانوني للحصول على مصالح خاصة، ولهذا السبب تتخذ الحكومات الأوروبية والشرطة والسلطات في المملكة المتحدة الخطوات اللازمة لحماية خصوصية بيانات الأفراد والقطاع العام. وسيقدم هذا البحث مقترحاً قانونياً لتجريم الخروقات الالكترونية.

یوخته:

له‌گه‌ل زياتر به ديجيتال‌بوونی جيهان زياتر نيگه‌رانيه‌كان دهر باره‌ی تاوانه ئه‌ليكترونيه‌كان و په‌يوه‌ندی نيوان ياسا و ئاسايش و نه‌ينی داتاكان بوومه نيگه‌رانيه‌کی بهرچاو. تاوانباران ته‌کنه‌لوژيای ديجيتالی به‌کارده‌هينن بۆ ئه‌نجامدانی تاوان. ئهم تويزينه‌ويه ليکوئينه‌وه له شيوازه گه‌شه‌سهندووه‌كاني ئاسايشی ياسایي و نه‌ينی داتاو‌زانیاری ده‌کات. کاريگه‌ری په‌رهي‌دانی ته‌کنه‌لوژياکان زور گرینگن له‌سه‌ر تايبه‌تمه‌ندی تاک و کومه‌لگا، بۆ ئهم مه‌يه‌سته ولاتانی پيشکه‌وتوی دونيا و هه‌ر ويا و به‌ري‌تانيا و په‌رسه‌ندنی ريساکانی ياسای ديجيتاليان گرینگی پيدا و ريککه‌وتنه نيوده‌وله‌تیه‌كاني په‌يوه‌ست به داها‌توی داتا و پاراستنی نه‌ينی، پيداويستیه‌كاني ستراتيژی ياسایي پراکتیکی، و ريشوئینه‌كاني پاراستنی نه‌ينی تاکه‌که‌سی و حکومه‌ت و ريگرکردن له ديجيتالی نایاسایي به‌کرده‌وه جيهه‌جی کردوه. هه‌روه‌ها ليکوئينه‌وه له به‌کاره‌ينانی ئه‌خلاقی و تاوانکاری نه‌ينی داتا ئه‌ليكترونيه‌كان ده‌کات. جگه له‌وه‌ش، پيشلکردنی داتا و پيشلکردنی تايبه‌تمه‌ندی رۆژانه رووده‌دات. هه‌روه‌ها ئهم تويزينه‌ويه چاره‌سه‌ری ياسایي گونجاو و باشتري‌ن پراکتیزه‌كان ده‌خاته‌روو که داها‌توی ئاسايشی ياسایي و نه‌ينی داتاكان باس ده‌کهن. له‌گه‌ل گو‌رانی سروشتی تاوانه‌كان، ياسا و ريسا ديجيتالييه‌كان ده‌بي‌ت ئاماده‌بن بۆ ئهم ته‌حه‌دايه نوويه، بۆيه پيوستمان به ياسای نوئ هه‌يه. تاوانباران به شيوه‌یه‌کی نایاسایي سه‌رده‌می ديجيتالی به‌کارده‌هينن بۆ به‌ده‌سته‌هينانی به‌رژه‌وه‌ندی تايبه‌ت، هه‌ر ئه‌مه‌شه وایکردووه حکومه‌ته‌كاني هه‌ر ويا و پوليس و ده‌سه‌لاتدارانی به‌ري‌تانيا هه‌نگاوی پيوست بنين بۆ پاراستنی نه‌ينی داتا‌کاني تاک و که‌رتی گشتی. ئهم تويزينه‌ويه پرۆژه ياسابه‌ک پيشنبار ده‌کات بۆ به‌تاوان ناساندنی تاوانه ئه‌ليكترونيه‌كان.