International Journal of Civil Law and Legal Research

E-ISSN: 2789-8830
P-ISSN: 2789-8822
Impact Factor (RJIF): 5.62
IJCLLR 2025; 5(2): 129-136
www.civillawjournal.com
Received: 10-06-2025
Accepted: 14-07-2025

Basira Abdullah Ahmed Mahmood
Assistant professor
Private law -civil law
Kirkuk University, Kirkuk, Iraq

Ahmed Mohammed Siddiq
Assistant professor
Private law -civil law
Kirkuk University, Kirkuk, Iraq

Correspondence
Basira Abdullah Ahmed Mahmood
Assistant professor
Private law -civil law
Kirkuk University, Kirkuk, Iraq

The legal protection of digital data privacy

Basira Abdullah Ahmed Mahmood and Ahmed Mohammed Siddiq

DOI: https://www.doi.org/10.22271/civillaw.2025.v5.i2b.152

Abstract
This study looks at the legal protection of personal information that is accessible online through electronic websites, especially in view of the quick advancement of contemporary information technologies and the rise in various violations that impact people because of how quickly and easily such information can be shared. The dignity of private life is seriously threatened by these infractions whenever any activity concerning digital privacy is carried out. Strengthening international efforts to offer legal protection for personal data when it is violated by outsiders has therefore become essential. In this sense, the Iraqi lawmaker needs to step in and pass legislation protecting the privacy of digital information.
In addition, we discussed the idea of information privacy, which deals with personal information. Since it pertains to the individual as a human being, such information is regarded as private. This includes details like name, address, phone number, and other records and information associated with each natural person. Additionally, the conversation looked at the hazards involved and the connection between digital privacy and information privacy protection. Particularly while using the global Internet network, people should be aware of the types of privacy intrusions that digital information privacy aims to prevent.
The study further analyzes the legislative approach of Iraq towards the protection of personal data, as embodied in the provisions of the Electronic Signature and Transactions Law No. 79 of 2012 and the Electronic Payment Services Regulations No. 3 of 2014. It also evaluates the Egyptian legislator's framework under the Personal Data Protection Law No. 151 of 2020, alongside the Qatari legislator's stance as outlined in the Personal Data Privacy Law No. 3 of 2016. Through this comparative perspective, the research highlights both the convergences and divergences in legislative strategies, revealing the extent to which each jurisdiction addresses emerging challenges in safeguarding digital information privacy.

Keywords: Digital information privacy, internet network, personal data

Introduction
The protection of digital information privacy has become a matter of paramount importance, particularly in light of technological advancements and the increasing number of internet users. Naturally, domestic legislation must evolve to address the emerging needs of society and keep pace with the legislative developments witnessed worldwide. This necessity arises from the extensive use of personal data in numerous daily activities, the sensitivity of such data, and its vulnerability to violations and breaches that harm individuals on a personal level and societies on a broader scale.
Building a secure digital platform requires the establishment of safe social relationships and interactions between electronic services and their users, enabling effective utilization of these services. Such an environment can only be achieved when users are assured of trust and security.
Interest in the right to privacy has intensified due to the growing risks and damages it faces as a result of advances in digital technology and information systems. These developments have the potential to penetrate and compromise this right, underscoring the need for the enactment of legal provisions that safeguard it in a manner commensurate with the nature and scale of these threats.

Research Importance
The importance of this research lies in shedding light on informational privacy in the digital environment, its significance, the risks posed by modern technologies to it, and methods of protection. Additionally, the novelty of the study topic, the scarcity of judicial rulings issued on this subject, and the fact that jurisprudence has not developed sufficiently in its research regarding this topic contribute to its importance.

Research Problem

The permanent Iraqi Constitution has addressed the right to privacy as one of the rights derived from the sanctity of private life. The Iraqi legislator has limited itself to protecting personal data on the internet in a number of legislations. Due to the freedom that the internet provides to users, this has led to a significant number of violations and unlawful practices that harm individuals and society. Therefore, establishing an independent legal framework that protects the right to digital informational privacy has become an urgent matter in Iraq. The legislator should adopt it due to its great importance for every individual in society.

Research Questions

- What specifically constitutes digital data?
- What information is required by law to be preserved?
- What are the legal texts that address the issue of protecting users' digital privacy?

Research Methodology

We relied on the inductive approach and the comparative approach between Iraqi, Egyptian, and Qatari law regarding the protection of informational privacy.

Research Scope

We limit the scope of our research to the individual's right to privacy of their data only, as this right is one of the most fundamental rights inherent to human beings.

Research Plan

First Section: The concept of digital informational privacy and its relationship to maintaining digital privacy.
First Requirement: The concept of informational privacy.

Second Requirement: The relationship between digital privacy and maintaining informational privacy.

Second Section: Risks related to digital privacy protection and the position of laws regarding digital privacy protection.
First Requirement: Risks related to digital privacy protection.

Second Requirement: The position of laws regarding digital privacy protection.

First Section

The Concept of Digital Informational Privacy and Its Connection to Maintaining Digital Privacy

Using the internet or social media sites requires individuals to share their data. Therefore, this section will be divided into two parts: the first will explore the concept of informational privacy, and the second will examine how digital privacy relates to maintaining informational privacy.

First Requirement

The Concept of Informational Privacy

Informational privacy means the fundamental rights that every individual enjoys in controlling the information that pertains to them. This data is called private data because it relates to the person as a human being, such as their name, address, phone number, and other information and data associated with each natural person [1]. Every individual has their private life, and the protection of their privacy is a guaranteed right under international and domestic laws as well as international constitutions. Any exposure to or violation of this privacy constitutes an infringement upon one of the fundamental human rights that both positive and divine laws have advocated for [2].

It is common knowledge that when registering on a website, individuals are required to provide personal information, such as their first name, last name, email address, password, gender, and date of birth. The website may also request some other information, such as their qualifications and professional experience that they provide in their profile during registration. All of this information can be described as personal data [3]. Social media sites collect three types of information that users enter: personal information, internet connection information (such as IP addresses), and data about the pages that users visit, taking into consideration that the social media site's access to the data that a person places on the site does not constitute unlawful practices unless this data is exploited after processing with the user's consent for other purposes that the user is unaware of [4]

Egyptian Law No. 151 of 2020 regarding combating information crimes defined personal data in Article (1) as any information related to a specific natural person or one who can be identified directly or indirectly through combining it with other information such as their name, voice, image, identification number, or internet identifier, or any data that determines the characteristics and attributes that distinguish them from others, including psychological, health, economic, cultural, or social identity. Article (1) of the Egyptian law also defined the private account as (a set of information belonging to a natural or legal person that grants them alone the right to access

The services available or their use from a website or information system. Article One of the Qatari Personal Data Protection Law No. 13 of 2016 defines personal data as (data about an individual whose identity is determined or can be reasonably determined either through this data or by combining it with any other data). The Qatari Personal Data Protection Law states in Article (16) that personal data of a special nature includes data related to ethnic origin, children, health or physical or psychological condition, religious beliefs, marital relationship, and criminal offenses, and the Minister may add other categories of personal data of a special nature if their misuse or disclosure would cause serious harm to the individual).

Here, a question arises: what specifically constitutes personal data?

---

[1]) Ben Qara Mustafa Aisha, The Right to Informational Privacy Between Technical Challenges and the Reality of Legal Protection, research published in the Arab Journal of Sciences and Research Publishing, Volume 2, Issue 5, 2016, p. 39.

[2]) Ghazwan Abdul Hameed Al-Shuwaysh, Muammar Khalid Abdul Hameed, "Balancing Media Freedom and the Right to Privacy," published research in the Journal of the College of Law for Legal and Political Sciences, Volume 9, Issue 33, 2020, University of Kirkuk, p. 259.

[3]) Dr. Jabbali Abu Hashima Kamel, Protection of Personal Data in the Digital Environment, research presented to the Conference on the Digital Age and its Legal Problems, Faculty of Law, Assiut University, April 2016, p. 4.

[4]) Ikram Sulaiman Qajam, Legal Protection of Personal Data in Qatari Law and Comparative Law, Master's thesis submitted to the Faculty of Law, Qatar University, 1442, p. 14.

To answer this question, we believe from our perspective that personal data includes his name, place of residence, personal identification number, banking information, email, electronic signature, online purchases that require personal data, postal and telegraphic correspondence, his personal photos and videos, his geographical place of residence, and his sharing on social media sites.

From our perspective, we propose to the Iraqi legislator regarding the definition of personal data the following text: (information related to a natural person that determines their identity, personal status, family situation, religious beliefs, and data that determines their geographical location).

Information privacy is data protection, as data is part of privacy and relates to confronting attacks on personal data. Meanwhile, privacy in its entirety encompasses data privacy, communications privacy, in addition to the privacy of exchanging electronic and regular messages, location privacy, and all these concepts are interconnected within one scope, which is the right to personal confidentiality or the right to privacy [5].

From our perspective, we define digital informational privacy as the right that internet users should have to decide on maintaining the data and information they wish to share and protecting it to safeguard their privacy.

Second Requirement

The Relationship between Digital Privacy and Maintaining Informational Privacy

The nature of the risks that personal information faces on the internet requires establishing a system to protect this privacy in the digital environment. Information spreads very quickly on the internet, and this information can be obtained online much more easily than it can be obtained in reality. A person's hobbies, photos, name, and tendencies have become available in the digital environment. Chats have become accessible, and data from online purchases is available since websites require personal information. Information about any person who may not wish

This person wishes to have disclosed [6]. Article (3) of the Qatari Personal Data Protection Law No. 13 of 2016 states that (every individual has the right to protect the privacy of their data, and such data may not be processed except within the framework of transparency, integrity, respect for human dignity, and acceptable practices per the provisions of this law). Article (4) of the Egyptian Personal Data Protection Law states that (the controller is obligated to obtain personal data or receive it from the holder or from the competent authorities to provide it as appropriate after the consent of the data subject or in legally authorized circumstances). In the digital environment, data and communications spread regardless of any consideration for geographical boundaries, and individuals place their personal information under the control of different or unknown entities, which raises the threat of misuse of this data, particularly in countries where legal protection standards for personal information do not exist. This may be the basis that drives toward concluding international agreements for the protection of personal data across borders, and it is the same basis that necessitates finding contractual tools that impose certain legal obligations on data-receiving entities, all of which revolve around the goal of protecting privacy and preventing the misuse of individuals' private data, in addition to their purpose in preventing fraudulent activities and harm to users in the digital environment [7].The internet, which is owned by everyone and owned by no one, has no central authority or sovereign entity that provides protection or offers opportunities and possibilities for legal protection when violations occur. Therefore, enacting domestic law to protect informational privacy in the digital environment has an effective role, and this is due to the element of sovereignty and control and the availability of an entity capable of monitoring and preventing violation or its continuation, which enables compensation and prosecution of violators. The internet is characterized by decentralization and the absence of controlling authority, although the struggle for internet control intensifies through seeking to control domain names and website addresses, competing to control the website hosting market through technical servers, and the tendency to control information and methods of exchanging it by controlling technical solutions and monopolizing them to become a means of controlling users' fate and an actual tool of control [8].

We propose from our side the following text: (Every natural person has the right to protect their data, and it may not be processed except after obtaining prior consent from the concerned person or in circumstances legally authorized).

Second Section

Risks Related to Digital Privacy Protection and the Position of Laws Regarding Digital Privacy Protection

In our current time, after the emergence of the internet and social media sites, the vessel that stores personal data has become different from traditional vessels, and traditional legal texts cannot address it due to the special nature of the virtual vessel. This requires the Iraqi legislator to follow the example of the Egyptian and Qatari legislators by intervening to enact a special law for the protection of personal data to be capable of confronting the phenomenon of violation of information or personal data on the internet or social media sites. Therefore, we will divide this section into two requirements, addressing them in

The first requirement is the risks related to digital privacy protection, and we address the position of laws regarding digital privacy protection.

First Requirement

Risks Related to Digital Privacy Protection

When individuals use internet sites, they expect a degree of privacy in their activity more than they expect in the real physical world, because in this world their presence can be observed and monitored by others. Unless a person reveals data about themselves, they believe that no one will know who they are or what they do. However, the internet, through server systems and network management systems, creates a large amount of information at every stop in the network space. This data may be captured and known about employees of an establishment, for example, when they use

[5]) Ben Qara Mustafa Aisha, previous source, p. 41.

[6]) Dr. Mona Turki Al-Mousawi, Jean Cyril Fadlallah, Informational Privacy, Its Importance, and the Risks of Modern Technologies to It, research published in Baghdad College Journal for Economic Sciences, University Special Issue of the College Conference, 2013, pp. 310-311.

[7]) Dr. Dina Abd Al-Aziz Fahmy, Criminal Liability Arising from the Misuse of Social Media Sites, research presented to the Fourth Scientific Conference entitled Law and Media, Faculty of Law, Tanta University, April 2017, pp. 15-16.

[8]) Dr. Mona Turki Al-Mousawi, Jean Cyril Fadlallah, previous source, pp. 312-313

the network or their subscriptions connected to it by the employer [9]. The internet consists of many computers linked to each other through wired and wireless communications and provides many services for obtaining information in various fields of life. It is the treasury of knowledge and a means for the flow of information [10]. The risks of modern technologies to privacy protection are increasing, such as camera surveillance technologies, electronic identity and identification cards, personal databases, mail and communications monitoring, and workplace surveillance[11]. Among the risks in the digital environment is hackers conducting unauthorized entry or penetration, or unlawful staying in a private communication system and collecting private information about others through intelligent software sent via email or through their appearance as fake links capable of spying on users [12].There may also be intrusion into others' private lives using viral programs or other technical means, such as cookies [13]. Article (One) of the Egyptian Personal Data Law states that technical operations that maintain the privacy, confidentiality, safety, unity, and integrity of personal data and prevent unauthorized access by any person to personal data or unlawful access to it, or any unlawful process of copying, sending, exchanging, distributing, transferring, or circulating aimed at disclosing personal data or modifying it during storage, transfer, or processing constitutes a breach and violation of personal data [14].Some social media users suffer from certain risks, including account hacking, the distribution of embarrassing photos, and difficulty removing or deleting accounts. Hence, internet users on these sites must take precaution and caution so that they are not exposed to harm on social networks and attempt to maintain control over their digital reputation because the user is the one who publishes their personal information and photos as well as shares links on social networks, as this collection represents their digital personal profile [15].

From our perspective, we propose the following text: (A breach of information or data security and safety is defined as any unlawful access process or unauthorized transfer or procedure on data or information).

Second Requirement

The Position of Laws Regarding Digital Privacy Protection

Legislation has given significant importance to protecting individuals' private lives by adopting the concept of private life and prohibiting violations of the right to personal data privacy and information protection. It aims to safeguard people's lives from the risks associated with information technology, while balancing this right with considerations of national interests and individual rights [16].

First: The Position of the Egyptian Legislator on Protecting Personal Data in the Digital World

Article (1) of the Egyptian Personal Data Protection Law No. 151 of 2020 defined the processing of personal data as (any electronic or technical operation for writing, collecting, recording, preserving, storing, merging, displaying, sending, receiving, circulating, publishing, erasing, changing, modifying, retrieving, or analyzing personal data using any medium or electronic or technical devices, whether done wholly or partially). Some define the processing of personal data as every operation or set of operations conducted on this data regardless of the means used, particularly collection, recording, organization, preservation, examination, use, modification, retrieval, or any other form of approximation, availability, connection, as well as deletion, closure, and destruction [17].

Article (2) of the Egyptian Personal Data Protection Law states that (personal data may not be collected, processed, disclosed, or revealed by any means except with explicit consent from the data subject or in legally authorized circumstances, and the data subject shall have the following rights: knowledge of their data held by any holder, controller, or processor, or access to it or obtaining it; withdrawal of prior consent to retain or process their data; correction, modification, erasure, addition, or update of personal data; knowledge and awareness of any breach or violation of their data; objection to the processing of personal data or its results when it conflicts with the fundamental rights and freedoms of the data subject). It is evident from this article that user personal data may not be collected except with their consent and in certain circumstances, and they can withdraw their prior consent to retain their data or erase it. Article (3) outlined the conditions for collecting, processing, and retaining personal data, requiring that personal data be collected for legitimate, specific, and declared purposes to the concerned person, that it be accurate, sound, and declared, that it be processed in a lawful manner appropriate to the purpose for which it was collected, that it not be retained for longer than necessary to fulfill its specified purpose, and determines the controls for processing, retention, and security according to the executive regulations of this law. Article (4) states the controller's obligation to obtain personal data from the holder or from the competent authorities to provide it after the consent of the data subject and ensure the accuracy of this data and its agreement and adequacy with the specified purpose of its collection, establish the method and style of processing under the specified purpose, perform or refrain from any act that would make personal data available except in legally authorized circumstances, take all technical measures to protect and secure personal data to preserve its confidentiality and prevent its breach, damage, or alteration,

[9]) Younes Arab, The Risks that Threaten Privacy and Information Privacy in the Digital Age, article available online on 14/4/2023 at the following website: https://kenanaonline.com/users/ahmedkordy/posts/323471#:~:

[10]) Nahla Abd Al-Qader Al-Momani, Information Crimes, Dar Al-Thaqafa, Jordan, 2008, pp. 38-39.

[11]) Dr. Mona Turki Al-Mousawi, Jean Cyril Fadlallah, previous source, p. 316.

[12]) Midhat Abd Al-Haleem Ramadan, Crimes Against Persons and the Internet, Dar Al-Nahda Al-Arabiya, 2000, p. 39.

[13]) Walid Al-Sayyid Saleem, Privacy Guarantees on the Internet, Dar Al-Jami'a Al-Jadida, Alexandria, 2012, p.

[14]) Yasser Mohammed Abd Al-Salam Rajab, Recent Legislative Developments in the Field of Information Security, Arab Journal of Informatics and Information Security, Arab Foundation for Education, Science and Arts, Volume 3, Issue 6, 2022, p. 121.

[15]) Mohammed Ahmed Al-Ma'adawi, Protecting User Informational Privacy Through Social Networks, p. 32, available on the following website, dated 13/4/2023: https://bu.edu.eg/portal/uploads/Law/Civil%20Law/1897/publications/Mohamed%20Ahmed%20Elmaadawy%20Abdrabo_desr.pdf

[16]) Mu'taz Ali Sabbar, "Legal Protection of Private Life in the Field of Taxation," published research in the Journal of the College of Law for Legal and Political Sciences, University of Kirkuk, Issue 5, Year 2, June 2013, p. 223.

[17]) Mohammed Sami Abd Al-Sadiq, Social Networks and the Risks of Violating the Right to Privacy, Dar Al-Nahda Al-Arabiya, 2016, p. 43.

erase this data immediately upon fulfillment of its specified purpose, and correct any error in the data immediately upon notification or knowledge of it.

Article (5) states the obligation of the personal data processor to conduct and implement processing according to the rules regulating this in this law, that the processing purposes be legitimate and their practice be lawful and not violate public order and public morals, for a specified period, and the controller and data subject must be notified of this period, and this data must be erased upon expiration of the processing period or delivered to the controller. Article (7) indicated the obligation of both the controller and processor, upon learning of the existence of a breach or violation of personal data in their possession, to notify the Center within seventy-two hours, and in case this breach or violation relates to national security considerations, the notification shall be immediate, describing the nature of the breach or violation, its form, causes, and the approximate number of personal data and its records. Article (8) explains the appointment of personal data protection officers, establishing a register at the Center for registering personal data protection officers, and Article (9) states the officer's obligations to conduct periodic assessment and examination of personal data protection systems and prevent their breach, enable the data subject to exercise their rights stipulated in this law, and notify the Center in case of any breach or violation of personal data in their possession. Article (12) states that it is prohibited for the controller or processor, whether a natural or legal person, to collect, transfer, store, preserve, process, or make available sensitive personal data except with a license from the Center, and Article (14) explained that operations for transferring personal data collected for processing to a foreign country or storing or sharing it are prohibited except with the availability of a level of protection no less than the level stipulated in this law and with a license from the Center.

In addition to the Egyptian Personal Data Protection Law, the Egyptian Information Crimes Law No. 175 of 2018 addressed the protection of data and information of electronic website users. Article (2) states the obligations and duties of service providers to preserve and store data, stating: (Service providers are obligated to the following / First: 2- Maintain the confidentiality of data that has been preserved and stored and not disclose or reveal it without a reasoned order from one of the competent judicial authorities, and this includes personal data of any of their service users or any data or information of the private websites and accounts that these users or persons access and the entities they communicate with. 3- Secure data and information in a way that preserves their confidentiality and prevents their breach or damage). Article (2/Third) of the Egyptian Information Crimes Law also indicated the necessity of protecting users' private lives, stating: (While respecting the sanctity of private life guaranteed by the Constitution, service providers and their affiliates are obligated to provide, upon request of national security agencies and according to their needs, all technical capabilities that allow those agencies to exercise their competencies according to the law). Article (2/Fourth paragraph) of the Egyptian Information Crimes Law also states the right of service providers and their agents only to obtain user data and no others, stating: (Information technology service providers, their agents, and distributors affiliated with them who are entrusted with marketing those services are obligated to obtain user data, and others are prohibited from doing so). It is clear to us that this article emphasizes the protection of users' personal data and obliges the service provider not to disclose any data or information concerning the user. It also obliges the service provider to necessarily provide adequate security and guarantee to maintain the confidentiality of user data and protect it from breach and disclosure. It also confirmed that user data may not be disclosed except in very narrow cases specified by this article in a reasoned request from one of the national security agencies, provided that it does not violate the user's sanctity. The article also limited-service providers and their agents to obtaining user data and no others.

Article (6/paragraph 3) of the Egyptian Information Crimes Law also states: (The investigation authority may order the service provider to deliver any data or information they possess related to an information system or technical device under their control or stored with them, as well as data of their service users and communication traffic that occurred on that system or technical system, and in all cases the order of the competent investigation authority must be reasoned). It is clear to us that this article emphasizes that the investigation authority's request must be reasoned when requesting information or data concerning users.

Article (20) of the Egyptian Information Crimes Law confirms that obtaining information or data or even viewing them without legal justification is not permitted, nor is hacking email or users' private accounts due to what this behavior carries in terms of violating users' privacy and breaching their private lives. Article (23) also obligated not to use the information network to access without legal justification bank numbers or cards and services and other electronic payment tools, and punishes those who commit this with imprisonment and fines. Article (24) of the Egyptian Information Crimes Law considers attributing someone else's account (a natural person) in a manner that contradicts the truth as something that involves an assault on user privacy. Article (25) of the Egyptian Information Crimes Law came to emphasize that violating individuals' private life sanctity is not permitted, whether by bothering them by sending electronic messages without their consent, using user data for marketing purposes without their consent, providing personal data to a system or electronic website to promote goods or services without their consent, or publishing through the information network or by one of the information technology means news, images, and similar content that violates any person's privacy without their consent, whether the published information is accurate or inaccurate. Article (26) of the Egyptian Information Crimes Law emphasizes that using user data in undisciplined content contrary to morals that may lead to harming the user's reputation is not permitted.

Second: The Position of the Qatari Legislator on the Protection of Personal Data in the Digital World.

The Qatari legislator defined in Article (1) of the Personal Data Protection Law No. 13 of 2016 the processing of personal data as (performing an operation or a set of operations on personal data such as collection, receipt, organization, recording, storage, preparation, modification, retrieval, use, disclosure, publication, transfer, blocking, disposal, erasure, and deletion).

Article (4) of the Qatari law states that the controller cannot process personal data except after obtaining the individual's consent, unless it is necessary to achieve a legitimate purpose for the controller or the third party to whom the data is sent.
Article (5) of the Qatari law also stated that an individual may at any time object to the processing of their data if it is not necessary to achieve the purposes for which it was collected, or if it is excessive to their requirements, or discriminatory, unfair, or contrary to the law.
Similarly, Article (8) obligated the service provider to process personal data with integrity and lawfulness, taking into account the special controls for designing, changing, or developing products, systems, and services related to personal data processing, and to take administrative, technical, and physical precautions to protect this data under what is determined by the competent administration and issued by a ministerial decision.
The Qatari legislator recognized the necessity of processing personal data under normal circumstances with the user's consent and notification about the processing operation, as Article (9) states that: (The controller, before beginning to process any personal data, must inform the individual of the following:

1. The controller's data, or any other party that undertakes data processing on behalf of the controller or for its exploitation.
2. The legitimate purposes for which the controller or any other party wishes to process the personal data.
3. A comprehensive and accurate description of processing activities and degrees of disclosure of personal data for legitimate purposes, and if the controller cannot do so, they must enable the individual to have a general description of them.
4. Any other necessary information and required to fulfill the conditions for processing personal data.

Based on the provisions of Article (14), the service provider or website owner (controller) is obligated to notify the user of any breach of personal data and notify the competent authority in the state of such breach so that it may impose appropriate penalties on whoever committed it.
However, Article (19) contained exceptional cases from the general rule, which is the necessity for service providers to obtain client consent. It states that the competent authority may decide to process personal data without being bound by the provisions of Articles (4, 5, 15, 19) of this law to achieve any of the following purposes: protecting national security, public security, international relations, and the economic or financial interests of the state; preventing any criminal offense or collecting information about it or investigating it.

Third: The Position of the Iraqi Legislator on the Protection of Personal Data in the Digital World.
The Iraqi Constitution of 2005 stipulates in Article (17) the right to privacy, which states: (Every individual has the right to personal privacy in a manner that does not conflict with the rights of others and public morals). Article (40) also states that (freedom of communications and postal, telegraph, telephone, electronic, and other correspondence is guaranteed, and they may not be wiretapped or disclosed except for legal and actual necessity and by a judicial decision).

The Iraqi Electronic Payment Service Systems No. 3 of 2014 clarifies in Article (13) the maintenance of confidentiality of data and information by supervisors of electronic payment systems and providing necessary protection to prevent unauthorized persons from accessing the computer environment. Article (13) states in the following paragraphs that:-

Fourth: Electronic payment service providers, participants, and any third party must provide information and data and refrain from any actions that affect or prevent the supervision and oversight mission, and cooperate as necessary to accomplish the supervision and oversight mission by the Bank.

Fifth: The Bank has access to the electronic payment service providers' system whenever the need arises. Persons authorized to access must respect and protect data and adhere to the principle of professional confidentiality.

Sixth: The Bank may provide regulatory authorities in another country with information obtained during its oversight and supervision operations in accordance with principles that stipulate information protection and respect for the confidentiality principle, and that it shall not be used except for the purposes based on which this information was granted.

Article (12) of the Iraqi Electronic Signature Law No. 79 of 2012 states that:
First: Licensed entities must provide the company or competent court with the reports, information, and data they request relating to the activities they conduct.

Second: With due regard to the provisions of item first of this article, electronic signature data, electronic means, and information provided to electronic certification authorities are confidential, and whoever receives or accesses them by their work may not disclose them to others or use them for purposes other than those for which they were provided.
It is evident from this article that electronic certification authorities are obligated to maintain the confidentiality of data and electronic signature information provided to them, and whoever accesses them by virtue of their work may not disclose them to others or use them for purposes other than those for which they were provided.
The Iraqi legislator addressed the protection of personal data in the digital world in a scattered manner across various laws and did not regulate a specific law for the protection of personal data on the internet.
Therefore, we suggest on our part to the Iraqi legislator, when legislating a personal data protection law, the following: -
Processing of personal data as: one or more operations carried out by any means to collect data, storing it, copying it, sending it, distributing it, linking it to other data, displaying it, concealing it, modifying it, describing it, or disclosing it in any manner whatsoever.

The following conditions are required for collecting, processing, and retaining personal data:

1. The data must be accurate and secure.
2. Explicit consent from the concerned person for collecting, processing, or disclosing this data.

3. Personal data must be collected for legitimate and specific purposes that are declared to the concerned person, and this data must be processed in legitimate and appropriate ways for the purpose for which it was collected.
4. It must be retained according to the duration necessary to fulfill the specified purpose.

The controller is obligated to the following

1. Take necessary procedures to protect the data in their custody.
2. Take security, technical, and organizational measures that ensure data protection from any breach of its security and integrity, or any alteration, addition, or destruction.
3. Establish mechanisms and procedures to which processing is subject, receive complaints regarding it, and respond to them following the provisions of this law.
4. Provide means that enable the concerned person to exercise their rights in accordance with the provisions of this law.
5. Correct incomplete or inaccurate data if it becomes apparent to them that it is incorrect or does not conform to reality before beginning processing.
6. Enable the concerned person to object to processing, withdraw prior consent, access their data, update it, and provide appropriate means to enable them to do so.
7. The controller is obligated, before beginning processing, to inform the concerned person of the data being processed and the date of its commencement, the purpose or objective for which data processing is conducted, the period during which data processing takes place (this period may be extended with the consent of the concerned person), and the protection of data security and integrity.
8. 8-Appointing a supervisor for processing sensitive personal data and transferring databases outside the country.

Data shall be erased or concealed, and necessary measures shall be taken by the controller upon request of the concerned person if they withdraw their prior consent upon which the processing was based, and if processing was carried out for a purpose other than that for which it was collected.

The supervisor shall undertake the following tasks

1. Monitor the controller's procedures related to data protection.
2. Ensure that assessment and periodic examination of database systems, data processing systems, and systems for maintaining data security, integrity, and protection are conducted periodically, provided that the assessment results are documented.
3. Establish internal instructions for receiving and studying complaints, data access requests, and requests for correction, erasure, concealment, or transfer of data, and make this available to the concerned person.
4. Organize training programs for the controller and processor to qualify them to handle data following the requirements of this law.

The processor is obligated to the following:

1. Conduct and implement processing.
2. Not exceed the specified purpose and specified duration for processing.
3. Erase data upon expiration of the processing period or deliver it to the controller.

Data undergoing processing is considered confidential data, and it is the responsibility of the controller, processor, and supervisor to maintain its confidentiality.

Conclusion

Findings

1. The rapid spread of information on websites has brought many concerns to people due to the sensitivity of private information, which prompted many countries to enact laws that control the misuse and storage of data.
2. There is no law or legislation in Iraq specifically for protecting personal data from violation by others.
3. Data and information security is an integral part of society's stability and have a close connection to the economic and social dimensions of the state.

Recommendations

The absence of Iraqi legislative regulation and the inadequacy of legal texts contained in traditional electronic laws, therefore, the Iraqi legislator must intervene to enact a specific law for the protection of personal data, and we suggest on our part the following provisions:-

Article One

1. Personal data means (information relating to a natural person that identifies their identity, personal status, family situation, religious beliefs, and data that determines their geographical location).
2. Digital informational privacy is the right that internet users must have to decide on maintaining the data and information they wish to share and protecting it to safeguard their privacy.
3. Breach of information or data security and integrity means any unauthorized access, transfer, or unauthorized action on data or information.
4. Processing of personal data means: one or more operations carried out by any means to collect data, store it, copy it, send it, distribute it, link it to other data, display it, conceal it, modify it, describe it, or disclose it in any manner whatsoever.

Article Two: Every natural person has the right to the protection of their personal data, and it may not be processed except after obtaining prior consent from the concerned person or in circumstances legally authorized.

Article Three: The following conditions are required for collecting, processing, and retaining personal data:-

1. The data must be accurate and secure.
2. Explicit consent from the concerned person for collecting, processing, or disclosing this data.
3. Personal data must be collected for legitimate and specific purposes that are declared to the concerned person, and this data must be processed in legitimate and appropriate ways for the purpose for which it was collected.

4. It must be retained according to the duration necessary to fulfill the specified purpose.

Article Four: The controller is obligated to the following:

1. Take necessary procedures to protect the data in their custody.
2. Take security, technical, and organizational measures that ensure data protection from any breach of its security and integrity, or any alteration, addition, or destruction.
3. Establish mechanisms and procedures to which processing is subject, receive complaints regarding it, and respond to them following the provisions of this law.
4. Provide means that enable the concerned person to exercise their rights in accordance with the provisions of this law.
5. Correct incomplete or inaccurate data if it becomes apparent that it is incorrect or does not conform to reality before beginning processing.
6. Enable the concerned person to object to processing, withdraw prior consent, access their data, update it, and provide appropriate means to enable them to do so.
7. The controller is obligated, before beginning processing, to inform the concerned person of the data being processed and the date of its commencement, the purpose or objective for which data processing is conducted, the period during which data processing takes place (this period may be extended with the consent of the concerned person), and the protection of data security and integrity.
8. Appoint a supervisor for processing sensitive personal data and transferring databases outside the country.

Article Five: The data shall be erased or concealed, and necessary measures shall be taken by the controller at the request of the data subject if he withdraws his prior consent on which the processing was based, or if the processing has been carried out for a purpose other than that for which the data was originally collected.

Article Six: The supervisor shall undertake the following tasks:

1. Monitor the controller's procedures related to data protection.
2. Ensure that assessment and periodic examination of database systems, data processing systems, and systems for maintaining data security, integrity, and protection are conducted periodically, provided that the assessment results are documented.
3. Establish internal instructions for receiving and studying complaints, data access requests, and requests for correction, erasure, concealment, or transfer of data, and make this available to the concerned person.
4. Organize training programs for the controller and processor to qualify them to handle data per the requirements of this law.

Article Seven: The processor is obligated to the following:

1. Conduct and implement processing.
2. Not exceed the specified purpose and specified duration for processing.
3. Erase data upon expiration of the processing period or deliver it to the controller.

Data undergoing processing is considered confidential data, and it is the responsibility of the controller, processor, and supervisor to maintain its confidentiality.

References

1. Qajam IS. Legal protection of personal data in Qatari law and comparative law [master's thesis]. Doha: Faculty of Law, University of Qatar; 2021.
2. Aisha BQM. The right to informational privacy between technical challenges and the reality of legal protection. Arab J Sci Res Publ. 2016;2(5):45-62.
3. Kamel JAH. Protection of personal data in the digital environment. In: Digital Age and Its Legal Issues Conference; 2016 Apr; Assiut, Egypt. Assiut University, Faculty of Law.
4. Fahmy DA. Criminal liability arising from misuse of social media sites. In: Fourth Scientific Conference: Law and Media; 2017 Apr; Tanta, Egypt. Tanta University, Faculty of Law.
5. Al-Shuwaysh GA, Abdul Hameed MK. Balancing media freedom and the right to privacy. J Coll Law Legal Polit Sci. 2020;9(33):155-176.
6. Abdul Sadiq MS. Social networks and the risks of privacy right violations. Beirut: Arab Renaissance House; 2016.
7. Al-Mousawi MT, Fadlallah JC. Informational privacy and its importance and the risks of modern technologies on it. Baghdad Coll J Econ Sci. 2013;(Conf Suppl):210-229.
8. Ramadan MA. Crimes of assault on persons and the Internet. Cairo: Arab Renaissance House; 2000.
9. Sabbar MA. Legal protection of private life in the field of taxation. J Coll Law Legal Polit Sci. 2013;2(5):88-103.
10. Al-Momani NA. Cybercrime. Amman: House of Culture; 2008.
11. Salim WS. Privacy guarantees on the Internet. Alexandria: New University House; 2012.
12. Rajab YMA. Recent legislative developments in information security. Arab J Inform Inf Secur. 2022;3(6):233-250.
13. Arab Y. Risks threatening privacy and information privacy in the digital age [Internet]. 2023 Apr 14 [cited 2025 Aug 25]. Available from: https://kenanaonline.com/users/ahmedkordy/posts/323471
14. Al-Ma'dawi MA. Protection of user's informational privacy through social networks [Internet]. 2023 Apr 13 [cited 2025 Aug 25]. p.32. Available from: https://bu.edu.eg/portal/uploads/Law/Civil%20Law/1897/publications/Mohamed%20Ahmed%20Elmaadawy%20Abdrabo_desr.pdf
15. Republic of Iraq. Constitution of Iraq. Baghdad; 2005.
16. Republic of Iraq. Electronic Signature Law No. 79 of 2012.
17. Republic of Iraq. Electronic Payment Service Systems Law No. 3 of 2014.
18. State of Qatar. Personal Data Protection Law No. 13 of 2016.
19. Arab Republic of Egypt. Personal Data Protection Law No. 151 of 2020.