

Data Protection in Iraq: Limitations of Existing Laws Amid the Tech Wave

Sanar Shareef Ali

¹A PhD student at Karoli Gaspar University of the Reformed Church in Hungary, Doctoral School of Law and Political Science

² Assistant lecturer, Soran University

DOI: <https://doi.org/10.31918/twejer.2584ELI.21>

Published:2/11/2025

Abstract

As technology advances, data protection has become a critical concern, extending beyond privacy to encompass state sovereignty, security, and economic interests. By July 2024, over 120 countries had enacted data protection laws, highlighting the inadequacy of traditional provisions in the digital age. However, Iraq lacks comprehensive legislation in this area, relying instead on scattered provisions within the 2005 Constitution, the 1969 Penal Code, and other laws. The absence of binding universal rules has significantly exacerbated this issue. This article examines Iraq's current privacy-related laws, identifies their shortcomings, and proposes legal reforms to address the evolving challenges posed by technology and data protection.

Keyword: Data protection, international law, privacy

Data Protection in Iraq: Limitations of Existing Laws Amid the Tech Wave

Sanar Shareef Ali

¹A PhD student at Karoli Gaspar University of the Reformed Church in Hungary, Doctoral School of Law
and Political Science

² Assistant lecturer, Soran University

sanarshareef@gmail.com

sanar.ali@soran.edu.iq

1– Introduction

Data protection has been a growing concern for the international community since the late 1960s (UN International Law Commission, 2006: 219). Following significant technological developments, legal concerns have emerged, particularly regarding the collection of personal data, which has become more vulnerable than ever before. As technology advances, so have data protection concerns.

According to the United Nations Conference on Trade and Development (UNCTAD), 137 out of 194 countries have enacted legislation to ensure data protection and privacy (Data Protection and Privacy Legislation Worldwide, no date). In fact, many countries have passed, or are in the process of passing, new laws that impose obligations on data controllers and processors to protect consumers' privacy (Securiti Research Team, 2024). However, other countries

are still struggling to enact comprehensive data protection laws, raising concerns about the adequacy of traditional privacy laws to address modern challenges.

Iraq, the focus of this study, is one such country. It has yet to develop a comprehensive data protection law. Instead, it relies on existing provisions and principles in its constitutional, criminal, and civil laws, among others, to regulate privacy and protect certain aspects of data.

The problem of the study is the absence of comprehensive domestic data protection laws in Iraq, coupled with the lack of binding global rules, have resulted in many challenges facing the government, citizens, and organizations. The lack of international standards makes it difficult to create and enforce consistent regulations, leaving gaps in national policies that can prevent effective data protection. Citizens face increased vulnerability because they lack legal protection against data exploitation and cybercrime, with no global framework to protect their rights in cross-border situations. Additionally, the lack of global rules prevents global cooperation, making it difficult for Iraq to effectively address cross-border cybercrime and data breaches. In cases of legal conflict, judges must rely on existing privacy laws, which are often inadequate to address modern data protection concerns. To explore this issue, the study poses the following questions:

- 1- What are the concepts of privacy and data protection, and are traditional privacy frameworks sufficient to address data protection concerns?

- 2- What is the position of international law regarding data protection?
- 3- What Iraqi laws govern privacy and data protection?
- 4- Are these laws sufficient to address data protection concerns?

The study aims to identify the provisions of Iraqi law that apply to data protection, and to demonstrate their inadequacy in dealing with modern data protection challenges, especially in the absence of binding global laws.

As the life becomes increasingly digitalized, and the number of users on online platform grows, so do the legal concerns. this study is of great importance as it analyzes the status of existing Iraqi laws and assesses their adequacy in addressing these developments. It also provides recommendations to close legal gaps and improve the data protection framework in Iraq.

The study took a descriptive and analytical approach, which is a document-based study, rely on official sources such as laws, regulations, international and regional frameworks, and unofficial sources such as books, articles, and websites.

For this purpose, we divided the study into four chapters, in addition to an introduction and a conclusion. The first chapter is introduction. The second chapter explains the concepts of data protection and privacy highlighting their difference. The third chapter examines the status of data protection in international law and demonstrates its inadequacies. The fourth chapter presents the provisions of Iraqi laws related to privacy and data protection. The fifth

chapter assesses these laws and their suitability in addressing contemporary data protection concerns.

2. Privacy and data protection

Historically, data protection was often considered part of privacy rather than a separate concept. Although data protection is related to information privacy, its development has taken a different path, emerging as a separate field with dedicated laws and institutions; and now focuses on the legal frameworks that regulate the use of personal information, and set out the conditions and restrictions on its use (Peter Blume, 2010: 153).

Privacy and data protection are closely related, the historical relationship between them highlights the latter as a newer concept, often viewed as a facet of privacy. Privacy is broader, and data protection is seen as part of it.

Data protection is a legal mechanism that ensures privacy, (Peter Blume, 2010: 153), and a law designed to protect personal data (Privacy International: 9), it refers to a collection of information that is transformed into a format optimized for transmission or processing. It can take various forms such as text, numbers, images, charts, or symbols. For example, data may consist of personal details such as people's names, ages, and other identifying information (Jigyasa Singh, 2022: 495).

In Europe, data protection evolving into a distinct concept with its own laws and institutions (Peter Blume, 2010: 153). The inception of initial data protection laws in the early 1970s, in addition to the subsequent advancements, have focused on addressing challenges arising from the advent of new technologies (Norberto Nuno Gomes de Andrade, 2011: 91). This inception was further defined by a landmark 1983 judgment by the German Federal Constitutional Court, later adopted by the EU through the Data Protection Directive 95/46 (Christopher Kuner, 2009: 309). The more technology evolves, the more data protection gains independence from privacy.

Privacy defined as a citizen's right to control personal information and make decisions about its disclosure (Peter Blume, 2010: 153). Privacy is widely believed to relate to aspects of a person's physical surroundings or psychological environment (Peter Blume, 2010: 153), in other words, it rooted in autonomy and control over these two aspects, extends to safeguarding ideas and information (Peter Blume, 2010: 153). Additionally, discussions on data protection's laws and policies often favor defining privacy in terms of information control (Lee A. Bygrave, 2010: 170).

Daniel Solove, a prominent American privacy scholar, has explained the privacy through several overlapping categories, including the right to be left alone, control over one's personal information, and protection of identity and dignity.

Together, these elements encompass much of what we mean by privacy (Mireille Hildebrandt, 2020: 104).

While it was noted in the report of the Special Rapporteur to the Human Rights Council (A/HRC/31/64), that there is currently no internationally unified definition of privacy (Data Privacy:9), another report, (A/HRC/23/40) defines privacy as “the presumption that individuals should have an area of autonomous development, interaction and liberty, a “private sphere” with or without interaction with others, free from State intervention and from excessive unsolicited intervention by other uninvited individuals. The right to privacy is also the ability of individuals to determine who holds information about them and how is that information used” (Frank La Rue, 2013: 6).

Calls for international frameworks often blend the terms 'data protection' and 'privacy.' International efforts, like the resolution from the 30th International Conference in Strasbourg, recognize the interconnection between the two by addressing them in the same legal or policy framework (Christopher Kuner, 2009: 309). The 'Global Privacy Standard,' published in November 2006, frequently mentions 'privacy' but focuses on principles like consent, purpose limitation, and access rights, which traditionally considered key concepts of data protection law (Christopher Kuner, 2009: 308). Efforts to bridge the gap between data protection and privacy emphasize their intertwined nature in legal and policy frameworks.

Privacy and the data protection share similar concerns. In the digital age, both are threatened by the widespread use of internet-based communications, which are notoriously difficult to regulate; the emergence of data-hungry apps like social media, search engines, and targeted advertising platforms; and the use of various online surveillance techniques by both public and private organizations (Kai Feng and Sylvia Papadopoulos 2018: 262).

In conclusion, though data protection forms part of privacy, data protection in its modern legal form, is a relatively new concept, as technology advances it is leaning towards appearing as an independent legal framework regulating the collection, processing and storage of personal data online. It extends beyond traditional privacy concerns to address national security and economic interests. This leads us to question the necessity and significance of data protection laws regulating areas beyond what privacy laws traditionally cover?

3- Why data protection laws needed?

Over the past two decades, internet usage has skyrocketed, leading websites, social media platforms and many online services to collect and store personal information from users, including names, contact details and behavioral data. Just as individuals value their privacy, many also seek control over how their information is collected and used online (Veritas, no date). This situation

gives rise to various challenges– legal, security, and economic– and poses difficulties for legislators to keep pace with this rapid trend. Alongside these developments government interventions have increased, and the motive behind these actions is not solely the protection of privacy only, as often portrayed, instead, many other interests are at play, such as national security, sovereignty, and various economic pursuits.

A report shows that deliberate intrusions of government and private computer systems, coupled with inadequate corporate privacy and cybersecurity measures, have put the personal data of millions of Americans at risk (Congressional Research Service, 2019: 1). Data reveals that while 90% of Americans consider online privacy to be extremely important, less than 25% of smartphone users feel they have control over their personal information online (Veritas, no date). The U.S. has implemented several federal laws to protect specific types of data, and more than a dozen states have passed comprehensive consumer data protection laws (Bloomberg Law, no date). However, if the United States, despite these legislative efforts, still faces significant challenges, one can only imagine the difficulties faced by countries that lack any data protection laws at all.

According to DataReportal, which provides global data, insights and trends to inform decision-makers, Iraq had 33.72 million internet users (74.9% of penetration), 25.53 million social media users (56.7% of population), and 45.76

million active mobile connections (101.7% of population) at the start of 2023 (Simon Kemp, 2023).

While the internet user's percentage in 2013 was only 9.20% according to ITU report (International Telecommunication Union, 2013). The Iraqi Ministry of Planning reported significant cybercrime activity, with Facebook linked to 78 kidnappings, 55 threats, 47 data breaches, 39 rapes, 17 drug cases, and 15 suicides, with child abductions being the most common. Overall, satellite hacking (41%) and social security fraud (22%) were the most common types of cybercrime. Charges included 67 cases of internet fraud, 40 cases of satellite hacking, 31 cases of data breaches, and 29 cases of child pornography, with internet fraud and satellite hacking dominating (Sattar Aboud, 2014: 423).

Personal information, including names and Social Security numbers, is highly sensitive and can be misused for identity theft, fraud, or even physical harm. Protecting this data is vital to preserving individual rights and freedoms, as data collection by companies and governments can shape behavior, influence decisions, and impact opportunities. Ultimately, data protection is a fundamental human right that protects autonomy and privacy, making it essential to have strong laws and hold violators accountable for violating privacy rights (Veritas, no date).

With the exponential growth of data storage and creation, enhancing data protection has become essential and crucial. This surge has led to the development of international data protection laws, which provide several key benefits (Thales Group, 2024). Including:

- The right to data protection can impact the effectiveness of other fundamental rights, including freedom of expression, freedom of thought, and freedom of assembly (European Data Protection Board, no date).
 - Important data is protected against leakage and loss.
 - Organizations are able to enhance the trust of the public, investors, and customers (Thales Group, 2024).
 - Data protection laws ensure that personal data is used fairly and securely, helping to prevent issues such as discrimination. Complying with these laws not only saves time and money, but it builds trust and enhances reputation by demonstrating a commitment to protecting customer information. This is vital for businesses of all sizes (Information Commissioner's Office, no date).
 - Managing the consequences of a personal data breach, such as a hacking incident, can be costly and time-consuming. This requires notifying affected individuals and potentially facing fines and compensation claims from those affected (European Data Protection Board, no date).
- Improvements in automation, digitization, and innovation resulting from

business process transformation have enhanced trust and credibility across markets and customers. These developments also provide a deeper understanding of data, its value, and the benefits it provides. As a result, better data management and control have emerged, fostering further innovation and transformation (Thales Group, 2024).

Modern data protection laws, such as General Data Protection Regulation (GDPR, 2018), in Europe, the Personal Information Protection Law (PRC, 2021) in China, California Consumer Privacy Act (CCPA, 2018) address critical aspects of privacy, national security, sovereignty and jurisdiction, and economic interests, where traditional laws fall short. In the lack of such regulations, all these concerns remain at risk, raising questions about the consequences of their absence, particularly countries like Iraq which lack even a single comprehensive law in this field.

Furthermore, in light of the transnational nature of digital data, one might question the extent to which domestically oriented regulations can function effectively within the international domain without engendering conflicts. Additionally, what is the stand point of international law regarding data protection?

2– International Law Framework

The absence of globally agreed-upon rules governing data protection has facilitated the proliferation of national laws. As countries become preoccupied with their own legislation, they appear to exhibit little concern for the lack of a

cohesive global agreement on these matters. Furthermore, the sensitivity of the issue contributes to the absence of universal standards, as nations remain wary of the opaque nature of emerging high-tech developments. This overreliance on national legislation fosters a fragmented regulatory landscape, thereby complicating efforts to tackle data protection challenges on a global scale.

Existing rules of international law applicable to this field can be divided into three categories. First, privacy rules enshrined in key human rights instruments, such as Article 12 of the Universal Declaration of Human Rights (1948), and Article 17 of the International Covenant on Civil and Political Rights (1966). Regionally, there are legally enforceable international agreements, including Article 11 of the American Convention on Human Rights (1969), and Article 8 the European Convention on Human Rights (1950), the latter has been interpreted by the European Court of Human Rights to include privacy and data protection matters as demonstrated in *Kruslin v. France* (ECHR, 1990, Case 11801/85), *Rotaru v. Romania* (ECHR, 2000–V, Case 28341/95).

However, these rules are quite fundamental and can't accommodate the complexities of modern technology. They were originally designed to safeguard privacy, and their application in the digital realm remains unclear.

The second category consists of regional rules with limited geographical application, such as GDPR, and the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

(convention108) (1981), this convention is one of the first data protection frameworks with international aspirations and global influence (Mark Phillips, 2018: 575). Additionally, the Economic Community of West African States (2010) has developed its Personal Data Protection framework. Another important regional framework is the Asia-Pacific Economic Cooperation (APEC) Privacy Framework (2005). It plays an important role in shaping the regional landscape of modern Asia (Nick Bisley, 2012), by implementing a set of guidelines and principles aimed at creating efficient privacy protection without impeding information flows within the 21-nation APEC region. To support this framework, the Cross-Border Privacy Rules (CBPR) system was created by APEC (Mira Burri, 2021: 750). This system allows Companies participate in a government-backed data privacy certification, to show that they comply with globally recognized data privacy protections (Asia-Pacific Economic Cooperation, no date).

Despite the valuable details these frameworks provide and their global influence globally, their application scope remains limited to specific regional zones.

The third category includes universal non-binding rules, such as the Organization for Economic Co-operation and Development (OECD) Privacy Guidelines (1980). The primary goals of these Guidelines are to establish privacy standards and facilitate the free flow of information for law enforcement purposes.

Key principles from the Guidelines – such as collection limitation, data quality, purpose specification, use limitation, security safeguards, transparency, individual participation, and accountability – can be incorporated into national privacy laws (Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 1980). The Guidelines were redesigned in (2013) and continue to serve as an essential source of information for OECD internal policies and processes. The OECD has played a pivotal role in formulating laws safeguarding personal data for a considerable duration (Personal Data Protection, 2023).

In (1990), the United Nations General Assembly adopted the Guidelines for the Regulation of Computerized Personal Data Files, which set out several important principles (GAG). These principles include legality, integrity, accuracy, purpose specificity, accessibility to interested individuals, non-discrimination, authority to grant exceptions, security, oversight, sanctions, considerations of cross-border data flows, and requirements that only relevant and adequate data be collected.

Despite significant advances in cyberspace and the increasing complexity of data protection, the Human Rights Committee has not yet developed a comprehensive set of obligations relating to privacy law. Rather, it has recognized only a few basic principles, including that Legal frameworks must regulate the collection and storage of personal data, whether by government bodies,

individuals or private organizations. States must take measures to ensure that personal information is not accessed, processed or used by unauthorized parties, and is not used in ways that violate the Covenant (ICCPR, 1988: general comment no 16).

In recent years, there have been growing calls from prominent figures in the public and private sectors for an international legal framework for data protection and privacy (Christopher Kuner, 2009: 309). An important example is the Montreux Declaration, issued in (2005) at the 27th International Conference of Data Protection and Privacy Commissioners. The Declaration urged the United Nations to develop a legally binding instrument to enforce human rights related to data protection and privacy. (Montreux Declaration, 2005). This call has been reinforced at subsequent gatherings, including the UN-sponsored World Summit on the Information Society in Tunis in 2005 and the 30th International Conference in Strasbourg in 2008. (30th International Conference of Data Protection and Privacy Commissioners, 2008).

Although the third category is not restricted to a specific region and is more universal in nature, these rules are not binding and have limited impact.

This indicates that international law falls short of providing sufficient binding rules applicable to all countries. Due to the sensitivity of the issue, there are no signs of hope for such rules in the near future, as each country is developing its own laws and is often reluctant to adopt universal rules.

It's worth mentioning that there are many data protection principles have gained broad acceptance among countries and international instrument, at the international and regional levels. Widely accepted principles of data protection include lawfulness, integrity, transparency, purpose limitation, data minimization, retention period, accuracy, notification, data subject rights, processing of sensitive personal information, accountability, confidentiality, and security – those principles are represented in instruments such as those issued by the OECD, APEC, GAG, convention108, GDPR, and the Personal Data Protection Within Economic Community of West African States (2010). However, most data protections issues are left to domestic laws, allowing for diverse approaches.

This raises the question of how, in the absence of universal binding rules, states without specific data protection laws, protect their citizens' privacy, national security and economic interests. Iraq is a vital example that still doesn't have specific data protection laws, and it relies on scattered privacy provisions or criminal provisions in various laws to address data protection issues.

4- Data protection bases in Iraqi laws

There is no comprehensive law governing data protection in Iraq, including for the private sector (Ali AL Dabbagh, Iraq 2024). However, there are some provisions regulating privacy in general, provide protection for personal data in telephone communications, telegraphs, and government documents. These provisions can be found in the 2005 Constitution, the Penal code 1969, the civil

law 1951 and others. It is worth mentioning that all these laws, with the exception of the informatic crimes draft law introduced in 2011, were enacted prior to the 2005 constitution. In this chapter we will review these laws, examine their relevant provisions, assess the possibility of applying these rules to online data privacy, and highlight their inadequacies in this regard.

4.1. The Iraqi constitution (2005)

Article 17 grants individuals the right to personal privacy, as long as it does not conflict with the rights of others or public morals. Article 40 guarantees “freedom of communications and correspondence—whether postal, telegraphic, electronic, or telephone—and prohibits monitoring, wiretapping, or disclosure thereof, except in cases of legal and security necessity, and pursuant to a judicial decision.

4.2. The Iraqi Civil Code No. 40 (1951)

Since the law does not explicitly address privacy, reference must be made to the civil liability provisions set out in the law itself (Hamoudi Bakr Hamoudi, 2019: 322). Articles 168 and 169 concern contractual liability, and set out guidelines for compensation in cases of non-fulfillment of contractual obligations. These provisions can be applied to various contracts, including contracts between data processors and data subjects. In addition, Article 202 addresses unlawful acts against individuals, requiring compensation for any damage caused, such as death, injury, assault or other personal harm. Furthermore,

Article 204 expands its scope by imposing compensation for damages beyond those specified in the previous articles. Importantly, Article 205 introduces the right to compensation for moral damage, and states that any violation of a person's freedom, dignity, reputation, social standing or financial situation renders the offender liable for compensation.

4.3. Civil Status Law No. 65 (1972)

Article 7 of the Law states that Registrations in the civil registry and clarifications in the facts register shall remain confidential. Individuals may view information relating to them, as may competent and authorized employees, judicial and investigative authorities, and recruitment officers, but only to the extent necessary to perform their duties.

4.4. Penal code No. 111 (1969)

Article 437 of the law states that anyone who obtains, discloses or uses confidential information for personal gain or the benefit of others may face imprisonment for up to two years or a fine not exceeding two hundred dinars or both. However, this does not apply in cases where the disclosure is made with prior consent or for the purpose of reporting or preventing a felony or misdemeanor.

Article 438 of the Penal Code provides for a penalty of imprisonment for a period not exceeding one year or a fine not exceeding one hundred dinars, or one of these two penalties, for the following crimes:

Publishing a picture, comment or information about a person's private or family life, even if it is true, if it is likely to cause offence.

Disclosing information from a letter, telex or phone call to someone other than the person to whom it was sent, which results in harm to others.

Article 327 stipulates that any public official or agent charged with a public service who knowingly discloses information obtained in the course of his duties to a person who was not entitled to receive it shall be punished by imprisonment for a period not exceeding three years and a fine not exceeding three hundred dinars, or by one of these two penalties. This article specifically addresses government employees in the public sector who disclose confidential information obtained in the course of their duties.

Article 328 stipulates that any employee or worker in a postal or communications service, as well as any public official or person charged with a public service, who opens, destroys, conceals or assists in opening or concealing a letter or telex entrusted to that service, or discloses the secrets contained therein, shall be punished with imprisonment for a period not exceeding seven years or with detention. The same penalty shall apply to anyone who discloses the contents of a telephone conversation or assists another in doing so.

4.5. Code of Criminal Procedure No. 23 of (1971)

Articles 72–84 of the Code of Criminal Procedure stipulate that no person may be searched, nor may his residence or any place in his possession be

entered or searched except in the cases specified by law, and by persons legally authorized to do so. This must also be based on a decision by a legally competent authority.

If the investigating judge believes that a person has items or papers that may assist in the investigation, the judge may order in writing that they be produced within a specified period. If the judge believes that the person may not comply, or fears that the items may be hidden or that the accused may flee, a search may be ordered. If letters, papers or other personal items are found during the search, they may only be viewed by the person conducting the search, the judge, the investigator and the representative of the Public Prosecution. If the items are sealed or otherwise secured, they may only be opened and searched by the investigating judge or investigator, and this must be done in the presence of the accused and the parties concerned whenever possible.

4.6. Informatics Crimes draft Law (2011)

The draft Cybercrime Law in Article 2 sets out the law's purpose as providing "legal protection for the legitimate use of computers and information networks," punishing offenders who violate the rights of users (individuals and legal entities), and preventing the misuse of computers to commit crimes.

For example, Article 19 imposes prison sentences and fines for the following acts:

(a) illegally obtaining information or data and leaking or disseminating it via computers with the intent to cause harm.

(b) disclosing subscriber information, secrets, or login data to third parties without legal consent.

(c) selling, copying, or exchanging personal information without consent for financial gain.

The law covers a wide range of crimes, including those related to national security, public order, terrorism, human trafficking, and drug abuse. Article 7 imposes severe penalties on anyone who uses computers or networks to steal money, financial rights or property, obtain financial benefits or deprive others of their financial rights. It also addresses fraudulent activities such as the seizure of software, data or electronic transactions using false identities or deceptive methods.

The law defines “information” in Article 1(12) as data, text, images, shapes, sounds, icons, databases, computer programs and similar materials that are generated, stored, processed or transmitted by electronic media; and defines email in Article 1(13) as a message containing information generated, sent or received by electronic or digital means; it lacks a definition of personal data.

There are specific data protection requirements for sectors, such as the Document Retention Law No. 37 of (2016), which sets out data retention rules that apply only to the public sector. Under Iraqi labor law, employers with more

than 15 employees are required to keep a personal file for each employee for two years after the end of the employment relationship (Ali AL Dabbagh, 2024).

To conclude, Despite the provisions mentioned above, many key aspects of modern data protection, such as data controller, data processor, personal data, sensitive data, biometric data, pseudonyms, special categories of personal data, and many others, are not recognized yet under Iraqi law.

5. Do existing laws suffice to protect personal data on internet

The Iraqi constitution prohibits monitoring, wiretapping, or the disclosure of communication and correspondence in all forms. However, as is often the case with constitutions, they only provide general, broad statements, leaving details to specific legislations.

Civil law has generally not addressed violations of the right to privacy as a separate legal issue, but has instead relied on provisions within the broader framework of general legal principles of Civil liability namely contractual liability and tort liability. Contractual liability arises from a breach of an obligation stipulated in a contract, while tort liability arises from a breach of a duty imposed by law (Sudad Hassan Muhssn, 2023: 631). Although the law contains general principles of tort and contractual liability that may be partially applicable to privacy issues, these provisions are not sufficient to address the complexities of personal data protection. At best, these provisions provide only a basic level of protection,

and lack the comprehensive safeguards needed to effectively regulate the handling of personal data in today's digital landscape.

The Civil Status Law of (1972) provides protection for the civil registry maintained by the government. However, it is very specific and not intended for the private sector, therefore fall short of protecting data online. Additionally, the law states exceptions for public officials performing their duties, and allows individuals to access their personal data.

While article 437 of the penal code applies to anyone, including individuals in the private sector who use or disclose confidential information, its application in the digital sphere, particularly with regard to data protection, remains unclear. Furthermore, it provides two legitimate grounds for data processing: consent and reporting or preventing a felony or misdemeanor. It is important to note that the term "confidential information" might be interpreted more narrowly than "data," resulting in more restrictions on the scope of the article.

The article 438 punishes publishing a picture or comment or information about private or family life, and the second paragraph could serve as a basis for punishing unauthorized disclosure of data. However, the article does not distinguish between private and public places, as most researchers and specialists do, who usually provide protection only for private places. In addition, the law only penalizes the publication of such data, not its retention (Sudad Hassan Muhssn, 2023: 629–630), use, or sell, which is an incomplete approach.

Moreover, the law makes the punishment conditional on the condition of causing harm which is not a common requirement in contemporary data protection laws.

The law provides two possible grounds for legitimate data processing: consent from the individual, and processing for the purpose of reporting a felony or misdemeanor or preventing the commission of such a crime.

The general meaning of provisions 72–84 of criminal procedure code may be applied to data protection by extending the same principles of authorization, judicial oversight, and protection against unauthorized access to digital data. Just as personal items are protected, data may only be accessed or searched under legal authority and under strict conditions, ensuring privacy and limiting access to sensitive information. These rules provide a basis to challenge unauthorized data use or disclosure.

Finally, the draft informatics crimes law punishes those who violate the rights of computer users by illegally obtaining, leaking or disseminating data with the intent to cause harm. Again, the condition of “intent to cause harm” limits the scope of the article, as the data subject is harmed regardless of the perpetrator’s intent. Additionally, the law penalizes the disclosure of subscriber data without legal consent, as well as selling, copying or exchanging of personal information for financial gain. But what if these actions are done without financial gain? Would they then legal?

As for the definition of information, Article 1 (12) provides a long list, including images, text, icons and concludes with “similar materials.” We can argue that the definition is not as clear as those provided by frameworks like GDPR, for example, it could still be interpreted broadly enough to include people’s behavior on online platforms.

The draft Cybercrime Law focuses primarily on computer-related crimes and penalties, with little emphasis on data protection. In general, the law addresses crimes arising from intentional and unlawful acts.

In 2013, the Parliamentary Committee on Media and Culture called for the withdrawal of the draft after pressure from individuals and civil society organizations. These groups raised concerns about the law’s many restrictive provisions (Iraq’s New Draft Law on Combating Cybercrimes Still Contains Problematic Provisions Restricting Fundamental Freedoms, 2020). This provision is likely to be used to suppress freedom of opinion, expression and publication, allowing Iraqi authorities to prosecute activists. The vague criteria in the law raise concerns because they create opportunities for abuse (Omar Alajlouni, 2023).

While these laws provide some basic protection for personal data, they were not intended to target online data, in other words, they were not conceived with the complexities of online data processing and control in mind. As such, they fail to directly address the emerging concerns associated with digital privacy. Consequently, the legal landscape for safeguarding personal data remains

inadequately defined, with no unequivocal statutory safeguards in place. The extension of these laws to encompass contemporary issues in digital privacy depends heavily on individual judges' interpretations, the political atmosphere and degree of respect for human rights. This introduces a significant degree of variability in the judicial handling of similar cases, where subjective judgment often eclipses objective legal standards, leading to inconsistent and sometimes unpredictable outcomes.

Additionally, these provisions fall short of international data protection standards, such as those set by the GDPR, OECD, APEC, PIPL, making them ill-suited to address data protection concerns in a rapidly evolving technology landscape. Moreover, as previously mentioned, data protection is no longer a sole privacy issue, and its implications extend to security, sovereignty, and economy. Countries are developing laws to control different aspects of this area, such as jurisdiction, and data localization. Therefore, the definitions and principles of the GDPR and other frameworks should be taken into account when defining online privacy and data protection in Iraq (Wahhab, Hussein and Ramalinggam, 2022: 6871).

6. Conclusion

Privacy is the right of an individual to control personal information, while data protection refers to the legal framework that protects this right. With the evolve of hi-tech data protection has gotten more independence and nowadays

is no longer a sole privacy issue. Consequently, countries have enacted new data protection laws to address the gaps created by technological developments, as existing privacy provisions are no longer sufficient to prevent data misuse, breaches, cybercrimes, or address concerns related to national security and sovereignty.

The absence of comprehensive domestic data protection laws in Iraq, coupled with the lack of binding global rules, creates significant challenges. The absence of global rules hinders the creation of consistent regulations, leaving citizens vulnerable to data exploitation and cybercrime. It has also made global cooperation to address cross-border cybercrime and data breaches more difficult.

The legal framework in Iraq consists of scattered provisions found in the Constitution of 2005, the Civil Code of 1951, and others. However, these provisions contain only limited privacy protections, with broad general statements that fail to adequately address data privacy concerns. They primarily drew upon general principles of civil liability, and include very specific provisions that are ill-suited for the private sector, falling short of standards required by the contemporary data protection legislations. Some provisions penalize the publication of personal data but do not address its retention, use, or sale, resulting in an incomplete approach. Furthermore, the requirement in some laws for harm

to occur as a bases for punishment is not a common feature of contemporary data protection laws.

The Draft Cybercrime Law mostly deals with computer crimes and contain very little regarding data protection. It penalizes the disclosure of subscriber data without legal consent, as well as the sale, copying, or exchange of personal information for financial gain. However, it raises the question: if these actions are carried out without financial gain, are they still considered legal? Most importantly the law is still draft and faces a lot of criticism for the restrictive provisions it contains, and its likeliness to be abused against freedom of opinion and expression.

To sum up, these laws were not intended to regulate data protection in the digital realm, and they lack key provisions found in modern data protection laws, such as data protection principles, clear definitions of personal data, data processing, and many other aspects, which are essential components of new data protection laws. Traditional physical laws cannot address or accommodate the new challenges posed by the digital age. As a result, citizens, the government and the entire Iraqi nation face significant risks that threaten national security and economic interests.

Recommendations

- 1- Iraq must urgently begin efforts to regulate and protect online data to address the – growing risks in the digital realm.

- 2- Building a robust technological infrastructure is essential to support the effective implementation of data protection laws and the protection of citizens' data.
- 3- Iraq should bring together experts from various fields to study the country's legal and technical landscape as a basis for drafting new, comprehensive data protection laws.
- 4- As an immediate step, Iraq should adopt privacy guidelines provided by international and regional frameworks, such as the OECD, the Asia-Pacific Economic Cooperation, and the UN General Assembly Guidelines on Computerized Files.
- 5- It is essential to amend existing laws to address critical contemporary issues related to data protection, and to ensure that they are compatible with current technological and societal challenges.
- 6- Iraq should conclude multilateral and bilateral agreements, to enhance cross-border data protection and ensure safety.
- 7- The draft cybercrime law should be revised to include contemporary data protection principles. It should also be drafted in a way that respects human rights and public freedoms.
- 8- There are certain shortcomings in existing laws that need to be addressed.
For example:

- The condition of "intent to cause harm" significantly limits the scope of protection under the law, as data subjects can suffer harm regardless of the perpetrator's intent.
- The law should be amended to ensure all unauthorized handling of personal data is penalized, regardless of financial motivation.

References

Aboud, Sattar J. (2014). Cybercrime in Iraq. {Online}. *International Journal of Scientific & Engineering Research*, 5 (3), 422–425. Last Accessed 29 November 2024 at: <https://www.ijser.org/researchpaper/Cybercrime-in-Iraq.pdf>.

Alajlouni, Omar (2023) "Why Iraq's Cybercrimes Draft Law Must Be Amended." *Euro-Mediterranean Human Rights Monitor*. {Online}. Last Accessed 27 September 2024 at: <https://euromedmonitor.org/en/article/5506/Why-Iraq%E2%80%99s-cybercrimes-draft-law-must-be-amended>.

Asia-Pacific Economic Cooperation (2015) APEC Privacy Framework. {online}. Last accessed 6 October 2024 at: https://www.apec.org/docs/default-source/Publications/2017/8/APEC-Privacy-Framework-%282015%29/217_ECSG_2015-APEC-Privacy-Framework.pdf.

Asia-Pacific Economic Cooperation (2023) What is the Cross-Border Privacy Rules System. {online}. Last accessed 7 November 2023 at:

<https://www.apec.org/about-us/about-apec/fact-sheets/what-is-the-cross-border-privacy-rules-system>.

Ali AL Dabbagh (2024) *Iraq – Data Protection Overview*. {Online}. Last Accessed 7 September 2024 at: <https://www.dataguidance.com/notes/iraq-data-protection-overview>.

Asia-Pacific Economic Cooperation (2015) APEC Privacy Framework. {online}. Last accessed 6 October 2024 at: https://www.apec.org/docs/default-source/Publications/2017/8/APEC-Privacy-Framework-%282015%29/217_ECSG_2015-APEC-Privacy-Framework.pdf.

Burri, Mira (2021) *Privacy and Data Protection*. {online}. 2 ED, the Oxford Handbook on International Trade Law. Last Accessed 8 December 2024 at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3947048

Bygrave, Lee A (2010) Privacy and data protection in an international perspective. {online} *Scandinavian studies in law*, 166–200. Last Accessed 7 December 2024 at: <https://scandinavianlaw.se/pdf/56-8.pdf>

Bloomberg Law (no date) *Everything You Need to Know About Consumer Data Privacy Laws so You Can Mitigate Risk and Stay Compliant*. {Online}. Last Accessed 9 October 2024 at: <https://pro.bloomberglaw.com/insights/privacy/consumer-data-privacy-laws/#:~:text=The%20U.S.%20does%20not%20yet,Gramm%2DLeach%2DBliley%20Act>

Blume, Peter (2010) Data Protection and Privacy: Basic Concepts in a Changing World. {Online}. *Scandinavian Studies in Law ICT Legal Issues*, 56/32, 152–164. Last accessed 8 December 2024 at: <https://www.scandinavianlaw.se/pdf/56-7.pdf>

Bisley, Nick (2012) *Asia-Pacific Economic Cooperation*. {online}. London, Routledge. Last Accessed 8 December 2024 at: https://d1wqtxts1xzle7.cloudfront.net/38783459/Routledge_handbook-libre.pdf?1442376701=&response-content-disposition=inline%3B+filename%3DRoutledge_Handbook_of_Asian_Regionalism.pdf&Expires=1734430415&Signature=YN-XvBUaYRyRA12jTA1DY1Q-vwNnSGEnza~HTcZku-P98ipswERIG7WqqCb4Ac4i21EH02CoJnHb0OBF5uye6VTEA2DJXZXK0g0OOd2Vv3pL1fyf66oKsylaO6T7bmVffK7iKLNCpa8tVd6D-lxn0qHqNPtn061090EyCmRW2KIGxpB9a5otbmyW-t0WWinGVN~sCmdsv-Vp8eQQlcXdhvkxaOJ-UrSgasPWYLSAqIWAD-xcnd8xHFfc89y3HOE62TLfJ73-XUG68N2kRWbCNfyf8ddtk6NYQneWNK5toSw-ZWrBSs14aN3Gm2VRAUCuUo0qY8xH5uvWHN5aG8-tg__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA#page=364

China Briefing Team (2021) *The PRC Personal Information Protection Law (Final)*. {Online}. Last Accessed 9 December 2024 at: <https://www.china->

[briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation/](https://www.briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation/).

CCDCOE (2023) The OECD Issues Revised Privacy Guidelines. {online}. Last accessed 7 November 2023 at: <https://ccdcOE.org/incyder-articles/the-oecd-issues-revised-privacy-guidelines/>.

Council of Europe (1981) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS). {online}. Last accessed 6 October 2024 at: <https://rm.coe.int/1680078b37>.

Civil Status Law No. (65), 1972. {online}. Last accessed 8 September 2024 at: <https://wiki.dorar-aliraq.net/iraqilaws/law/5595.html>

Criminal Procedure Code No. (23), 1971. {online}. Last accessed 18 December 2024 at: https://wiki.dorar-aliraq.net/iraqilaws/law/4895.html#google_vignette

Council of Europe (1950) European Convention on Human Rights, ETS No. 5. {online}. Last accessed 6 October 2024 at: https://www.echr.coe.int/documents/convention_eng.pdf.

California (2018) California Consumer Privacy Act of 2018 as amended by California Privacy Rights Act 2020. {online}. Last accessed 6 October 2024 at: <https://cdp.cooley.com/ccpa-2018/>.

Congressional Research Service (2019) *Data Protection Law: An Overview*. Washington D.C.: Congressional Research Service. {online}. Last accessed 6 October 2024 at: <https://sgp.fas.org/crs/misc/R45631.pdf>.

Christopher, Kuner., (2009). An International Legal Framework for Data Protection: Issues and Prospects. *Computer Law & Security Review*, 25 (4), 307–317. {Online}. Last Accessed 8 December 2024 at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1443802

DigWatch (2023) *Privacy and Data Protection*. {Online}. Last Accessed 10 November 2023 at: <https://dig.watch/topics/privacy-and-data-protection>.

De Andrade, Norberto Nuno Gomes (2011) Data protection, privacy and identity: distinguishing concepts and articulating rights. {online}. *Springer Berlin Heidelberg*, 90–107. Last Accessed 8 December 2024 at: https://link.springer.com/chapter/10.1007/978-3-642-20769-3_8

European Data Protection Board (2024) *Data Protection Benefits for You*. {Online}. Last Accessed 6 October 2024 at: https://www.edpb.europa.eu/sme-data-protection-guide/data-protection-benefits-for-you_en.

European Parliament and European Council (2016) General Data Protection Regulation 2016/679. {online}. Last accessed 6 October 2024 at: <https://gdpr-info.eu/>.

European Court of Human Rights (1990) Case 11801/85 *Kruslin v. France*, EU. {online}. Last accessed 6 October 2024 at: <https://hudoc.echr.coe.int/eng?i=001-57776>.

Economic Community of West African States (ECOWAS) (2010) Personal Data Protection Within ECOWAS. {online}. Last accessed 6 October 2024 at: <https://www.statewatch.org/media/documents/news/2013/mar/ecowas-dp-act.pdf>.

Feng, Kai. and Papadopoulos, Sylvia., (2018). Data Protection in the Digital Age: A Comparative Study. *Comparative and International Law Journal of Southern Africa*, 51, 261–287. {Online}. Last Accessed 8 December 2024 at: <https://unisapressjournals.co.za/index.php/CILSA/article/view/8257/4493>

Hamoudi Bakir, Hamoudi., (2014). Tort Liability Resulting from Violation of the Right to Privacy via the Internet. *International Journal of Scientific & Engineering Research*, 423, 315–352. {Online}. Last Accessed 8 December 2024 at: <https://www.iasj.net/iasj/download/48021f1007072d40>

Hildebrandt, Mireille (2020) *Privacy and Data Protection', Law for Computer Scientists and Other Folk*. {online} Oxford. Last accessed 11 September 2024 at: <https://doi.org/10.1093/oso/9780198860877.003.0005>

Informatics Crimes Law, 2011. {online}. Last accessed 4 September 2024 at:

https://iq.parliament.iq/law/frm_file/aWQ6Mzg2fGZpbGVuYW1lOtmC2KfZhtml2YYt2KzYsdin2KbZhS3Yp9mE2YXYudmE2YjZh din2KrZitipLnBkZg

Iraqi Constitution, 2005. {online}. Last accessed 8 September 2024 at: https://www.constituteproject.org/constitution/Iraq_2005

International Telecommunication Union (2013) Cyberwellness Profile: Republic of Iraq. Geneva: International Telecommunication Union. {online}. Last accessed 29 November 2024 at: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Iraq.pdf.

International Conference of Data Protection and Privacy Commissioners (2008) 30th International Conference of Data Protection and Privacy Commissioners, Strasbourg. {online}. Last accessed 6 October 2024 at: <https://icdppc.org/>.

Information Commissioner's Office (2024) The Benefits of Data Protection Laws. {online}. Last accessed 6 October 2024 at: <https://ico.org.uk/for-organisations/advice-for-small-organisations/the-benefits-of-data-protection-laws/>.

Kemp, Simon. (2023) *Digital 2023*: Iraq. {online}. Last accessed 29 November 2024 at: <https://datareportal.com/about>.

Law of Preservation of Documents No. (37), 2016. {online}. Last accessed 29 November 2024 at: <https://www.dataguidance.com/legal-research/document-retention-law-no-37-2016>

La Rue, F. (2013) Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression. Geneva: United Nations Human Rights Council. {online}. Last accessed 18 December 2024 at: https://www.ohchr.org/sites/default/files/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

Montreux Declaration (2005) The Protection of Personal Data and Privacy in a Globalized World: A Universal Right Respecting Diversities. {online}. Last accessed 6 October 2024 at: <https://www.montreuxdeclaration.org/>.

Muhssn, Sudad Hassan., (2023). Legal Protection of Women's Right to Privacy). *Journal of Duhok University*, 26 (1), 622–637. {Online}. Last Accessed 8 December 2024 at: <https://doi.org/10.26682/chjuod.2023.26.1.45>

MENA Rights Group (2020) *Iraq's New Draft Law on Combating Cybercrimes Still Contains Problematic Provisions Restricting Fundamental Freedoms*. {Online}. Last Accessed 27 September 2024 at: <https://menarights.org/en/articles/iraqs-new-draft-law-combating-cybercrimes-still-contains-problematic-provisions>.

Organization of American States (1969) American Convention on Human Rights. {online}. Last accessed 6 October 2024 at: <https://oas.org/en/iachr/mandate/Basics.asp>.

Organisation for Economic Co-operation and Development (OECD) (1980) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

{online}. Last accessed 7 November 2023 at:

<https://doi.org/10.1787/9789264196391-en>.

Organisation for Economic Co-operation and Development (OECD) (1980) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

{online}. Last accessed 6 October 2024 at:

<https://doi.org/10.1787/9789264196391-en>.

OECD (2013) Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.

{online}. Last accessed 18 December 2024 at:

<https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188>.

Organisation for Economic Co-operation and Development (OECD) (2023) Personal Data Protection. {online}. Last accessed 6 November 2023 at:

www.oecd.org/general/data-protection.htm

Phillips, Mark., (2018) International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR). *Human genetics*, 137, 575–582.

{online}. Last accessed 18 december 2024 at:

https://media.proquest.com/media/hms/PFT/1/oEL07?_s=FYt2p53cAWUAfYVm%2B1IXiOrAN6Q%3D

Privacy International (2018) A Guide for Policy Engagement on Data Protection. Part 1: Data Protection, Explained. London: Privacy International.

{online}. Last accessed 18 September 2024 at:

<https://privacyinternational.org/sites/default/files/2018-09/Part%201%20-%20Data%20Protection%2C%20Explained.pdf>.

Singh, Jigyasa., (2022). Data Localization. *Jus Corpus Law Journal*, 3 (2), 495–503. {Online}. Last Accessed 8 Decemebr 2024 at: https://heinonline.org/HOL/Page?public=true&handle=hein.journals/juscrp3&div=317&start_page=495&collection=journals&set_as_cursor=0&men_tab=srchresults

Securiti Research Team (2024) *Data Privacy Laws and Regulations Around the World*. {Online}. Last Accessed 6 October 2024 at: <https://securiti.ai/privacy-laws/>.

Thales Group (2024) *Beyond GDPR: Data Protection Around the World*. {Online}. Last Accessed 8 October 2024 at: <https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/magazine/beyond-gdpr-data-protection-around-world>.

United Nations Conference on Trade and Development (2024) Data Protection and Privacy Legislation Worldwide. {Online}. Last Accessed 19 July 2024 at: <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>.

United Nations (1948) Universal Declaration of Human Rights, A/RES/217(III). {online}. Last accessed 6 October 2024 at: <https://www.un.org/en/universal-declaration-human-rights/>.

United Nations (1990) Guidelines for the Regulation of Computerized Personal Data Files, General Assembly resolution 45/95. {online}. Last accessed 6 October 2024 at: <https://digitallibrary.un.org/record/105299?v=pdf>.

United Nations Human Rights Committee (UNHRC) (1988) General Comment No. 16: Article 17 (Right to Privacy). {online}. Last accessed 6 October 2024 at: <https://www.refworld.org/docid/453883f922.html>.

United Nations (1990) Guidelines for the Regulation of Computerized Personal Data Files, General Assembly resolution 45/95. {online}. Last accessed 6 October 2024 at: <https://digitallibrary.un.org/record/105299?v=pdf>.

UN International Law Commission (2006) Yearbook of the International Law Commission 2006. Geneva: UN International Law Commission. {online}. Last accessed 18 December 2024 at: https://legal.un.org/ilc/publications/yearbooks/english/ilc_2006_v2_p2.pdf.

United Nations Development Group (2014) Data Privacy, Ethics and Protection: Guidance Note on Big Data for Achievement of the 2030 Agenda. New York: United Nations Development Group. {online}. Last accessed 18 December 2024 at: https://unsdg.un.org/sites/default/files/UNDG_BigData_final_web.pdf.

United Nations (1966) International Covenant on Civil and Political Rights, A/RES/2200(XXI). {online}. Last accessed 6 October 2024 at: <https://www.ohchr.org/en/professional-interest/ccpr>.

Veritas (2024) *Data Privacy: Understanding Its Importance and Ensuring Compliance*. {Online}. Last Accessed 6 October 2024 at: <https://www.veritas.com/information-center/data-privacy>.

Wahhab, Bareq Muntadher Abdul., Hussein, Safinaz Mohd., Ramalingam, Rajamanickam., (2022). The Concept of Online Privacy and Personal Data Protection in Iraq: A Way Forward. *Journal of Positive School Psychology*, 6 (3), 6870–6881. {Online}. Last Accessed 8 December 2024 at: <https://www.journalppw.com/index.php/jpsp/article/download/4223/2781/4803>