Challenges in Regulating Online Privacy of Personal Data: Policy Guidelines for States: Iraq as a Case Study

Bareq Muntadher Abdul Wahhab[1*], Safinaz Mohd Hussein[2], Ramalinggam Rajamanickam[3], Omar Abdulsalam Hussein[4]

Abstract

The failure of nations to keep pace with technological advancement has resulted in a deficiency in regulating online privacy to safeguard people's personal data since their conventional legal texts and policies are difficult to adapt to the virtual world in order to secure it. Due to the increase in the amount of data collected, processed, and used on the internet; the difficulties in controlling data streaming over, and the decreased ability to control that flow as a result of decentralisation, individuals in countries without a policy, laws, or guidelines are unable to control their personal data. In another word, the violation of an IP address is not the same as the violation of residential or body privacy, nor is it the same as the violation of an e-mail address or password. The researcher will construct a set of principles that may be used to create a cohesive privacy policy with an adequate legal framework for each nation. To guarantee that personal information is safeguarded.

Key Words: Regulation, Policy, Privacy, Data Protection, Personal Data, Internet.

DOI Number: 10.14704/nq.2022.20.6.NQ22015 **NeuroQuantology 2022; 20(6):133-144**

Introduction into the Challenges

It is customary that violation of privacy is a crime that affects individuals by disclosing or processing their personal data, without having the ability in controlling their own data. Iraqi individuals are facing several challenges that preventing it from being protected from information technology crime precisely online privacy violations. Iraq needs a new and clear privacy policy that keeps pace with technological development and meets the need for legal protection and commercial practices to create a healthy environment protected from any form of attacks that occur via the Internet.

When the current Iraqi penal code was established in 1969, the only traditional types of privacy, such as privacy of houses or bodily privacy, were subject to violation. The Iraqi legislature did not predict privacy and personal data would transform into technological shapes, such as financial information, fingerprints, and eye scanners, which would be subject to violation. Therefore, these laws have been enacted to deal with crimes of privacy violations committed against tangible things and provide adequate rules to protect them. Since the Iraqi legislature did not take into account that intangible property, especially personal data, may be subject to such illegal behaviors, there are no provisions in the Iraqi legal framework that regulate the violation of personal data's online privacy. As a result, courts often encounter some difficulties in enforcing penal codes or finding an appropriate legal framework to regulate online privacy and personal data.

The first section will discuss international standards that can be used as a foundation for enacting personal data protection legislation, such as Convention 108, the OECD Guidelines, and the General Data Protection Regulation (GDPR).

Corresponding author: Bareq Muntadher Abdul Wahhab

Address: [1*]Faculty of law, University Kebangsaan Malaysia; [2]Faculty of Law, University Kebangsaan Malaysia; [3]Faculty of Law, University Kebangsaan Malaysia; [4]Faculty of Law, University Kebangsaan Malaysia

E-mail: [1*]bariq_montder@yahoo.com; [2]finaz@ukm.edu.my; [3]rama@ukm.edu.my; [4]omaralmulla91@yahoo.com

To ensure transparent and inclusive negotiations for all parties, Establish a set of legally enforceable data protection standards and incorporate them into the legal framework and determine the legal basis for data processing; in addition, include a list of data subject rights that are binding in law; define a clear scope of application; establish binding and transparent means for securely transferring data to third countries; furthermore, provide protection of information security and integrity of the processing process; prevent and report data breaches; with the existence of an independent authority; and establish strong law enforcement mechanisms.

The second section will be on the difficulties of compliance with data privacy laws in Iraq, with a comprehensive analysis of the challenges that face the Iraqi legislator in getting a legal framework regulating the online privacy of personal data protection. The final section will be the findings and conclusion.

International Standards as a Guide to Enacting Personal Data Protection Legislation

The right to protect personal data and online privacy is linked to recognising individuals' right to a space for self-development based on the principles of interaction and freedom, or their right to a private life free from state interference or excessive interference by others," according to the annual report of the United Nations High Commissioner for Human Rights.[1]

Additionally, the report discussed the interventions of governments and companies that collect billions of personal data from users of electronic transactions, as well as information brokers who trade in personal data from users who find themselves in a situation where it is impossible to trace the path of their personal data and information related to them, as well as the path of their use.

The report on the Authority of the United Nations High Commissioner for Human Rights and the promotion of civil and political rights[2] clarified the role of technology in promoting human rights, particularly rights related to society and peaceful protests, and emphasized the need for democratic societies to strengthen the principle of protecting personal data, particularly those with a political orientation and where fragile governments track individuals.

Additionally, the industry of personal data protection laws is based on international standards as a foundation and reference, such as Convention 108, the Organization for Economic Cooperation and Development's guidelines OECD, and the General Data Protection Regulation of the European Union's Regulation "GDPR," which has become a reference in the drafting of personal data protection laws.

The European Parliament and the European Commission adopted the GDPR, which aims to legalise the process of large companies using individuals' data or businesses that are based on the possession or processing of individuals' data by establishing a legal framework that protects that relationship. Additionally, it establishes the presence of an independent body that supervises the mechanisms' correct implementation and works to advance the protection of individuals' data as well as the right to privacy, in tandem with data movement freedom.

The GDPR also confirms that companies shall not acquire user data without the prior consent of the data subject, and his right to review the personal data acquired by companies. The regulation also included and emphasised some of the subsidiary rights that guarantee the protection of personal data, such as the right to privacy, the right to deal with personal data, such as erasing or modifying data, the right to be forgotten, the right to know, the right to privacy according to its default design, the right to access data, and the possibility of transfer.

Access Now, one of the associations that participated in the civil dialogue leading up to the adoption of the European regulation, presented a guide outlining the fundamental principles that legislators should consider when drafting a law governing the protection of personal data and the organisation of the processing process between the various parties, as well as what should be taken in order to avoid repeating previous mistakes which is:

[1]A/HRC/48/31: The right to privacy in the digital age - Report of the United Nations High Commissioner for Human Rights, https://www.ohchr.org/en/documents/thematic-reports/ahrc4831-right-privacy-digital-age-report-united-nations-high. Last visited, 24 April 2022.

[2]OHCHR Annual Report, The Impact of New Technology on the Promotion and Protection of Human Rights in the Context of Assemblies, Including Peaceful Protests, 3 July 2020, https://www.nhrc-qa.org/wp-content/uploads/2014/01/-العهد-الدولي-الخاص-بالحقوق-المدنية-والسياسية.pdf. Last visited, 25 April 2022.

eISSN 1303-5150

Ensure Transparent and Inclusive Negotiations for all Parties

It is intended to involve civil society institutions, private companies, and consumer defence associations in the dialogue on drafting the law, provided that these discussions are free from pressure methods in any way, and have a high level of transparency and impartiality, and this is what the European Union countries have followed in drafting the regulation on the protection of personal data.

But with regard to the steps taken to issue the draught of Iraqi information crime law, as an example, it ignored this important point and ignored the involvement of different groups of society, after many members of Parliament submitted the draught resolution, and it was rejected for many years from 2011 to 2022, and it faced great criticism from the United Nations. In this way, it shows the legislator's lack of reliance on the involvement of various segments of society in drafting and preparing the law and a lack of respect for the recommended international standards.

Define a List of Binding Data Protection Terms and include them in the Legal Framework

According to this principle, the legislation must define all the related terms such as: personal data, sensitive personal data, data controller, data processor, consent, cookies and similar technologies, cross-border processing, data minimisation, data portability, data protection commission, data protection impact assessment, data subject, legal basis, legitimate interest, personal data breach, privacy by design, pseudonymisation, recipient, restriction of processing, retention, right to access, right to erasure, right to objection, right to rectification, right to restriction, and transparency. Defining all these related terms is obligatory to establish the processes for handling personal data during transmissions. It incorporates international standards, including Convention 108 and OECD Guidelines, on fairness and legality, purpose, data minimization, accuracy, and retention period, as well as users' rights, including the right to access and delete data, as well as integrity and confidentiality, and finally, compatibility with data transmission to other countries or territories that provide an adequate level of protection.

Determine the Legal Basis for Data Processing

In Iraq According to a statement released by the Iraqi Digital Media Centre, a non-governmental organisation based in Baghdad, "there is a noticeable growth in the number of active social media users, as measured by the most recent data for this year." According to the statement, social media users reached 28.35 million active users this year, an increase of 3 million and 350 thousand people over the previous year. In addition, according to the centre, there are 18.85 million active users on "Facebook," 15.45 million active users on "Instagram," and 13.8 million active users on "Snapchat," 1.9 million active users on "Twitter," and 1.4 million active users on "LinkedIn," as well as 16.15 million active users on the Messenger app.[3]

Generally, processing refers to the act of performing one or more operations on private data, such as gathering, organizing, recording, storing, altering, formatting, retrieval, usage, publishing, disclosure, blocking, transfer, disposal, deletion, and cancellation.[4] The processing is always connected with personal data in this content, so it is critical to understand what personal data is.

The GDPR Article 6(1): Processing should be legal only if and to the degree that at least one of the following is applicable:[5]

1. The data subject has agreed to their personal data being used for one or more specific reasons.
2. In order for a contract to be carried out, or for a person to make an appeal before agreeing, processing must be done.
3. Processing is necessary to comply with a legal requirement imposed on the controller;
4. Processing is necessary to protect the data subject's or another natural person's vital interests;
5. Processing is needed to carry out a task in the public interest or to do what the controller is supposed to do.
6. To protect the controller's or a third party's interests, but not if the data subject's or other person's rights and freedoms require the

[3]Iraqi Digital Media Center DMC report of April 2022, non-governmental organization, https://www.alaraby.co.uk/entertainment_media/العراق-28-مليون-مستخدم-نشط-لمواقع-التواصل. Last visited, 25 April, 2022.

[4]El-Madawy, "Protection of the Information Privacy of the User through Social Networking Sites, a Comparative Study."

[5]Art. 6 GDPR ,Lawfulness of Processing General Data Protection Regulation (GDPR).

protection of personal data. This is mostly true if the data subject is a child.

Unless the processing is essential for attaining the objective, the data controller might only deal with personal data with the subject's consent. The individual has the right to complain against the processing act if it is not essential for the data's objectives.

However, Iraq does not recognise the international data processing principles, which leads to jeopardising the data subject's consent to be leaked or used without their consent. The DMC report indicated the data leakage of a number of Iraqi government websites. The report mentioned that Stealer Malware caused the leak of thousands of private data stored on government websites belonging to different countries, and it was offered for sale on the "Dark Web." As well as including the data of the officials and users of 49,880 websites alike, as well as the leak of 1,753,658 official documents, the leaked Iraqi data belonged to sites affiliated with the Ministry of Higher Education, the Ministry of Education, and the Council of Ministers Federal Service. The researcher believes that Iraq will stay weak in the absence of laws safeguarding personal data from violations that might result in damage to personal data stolen, processed, and used, whether medical, financial, or communication data.

Certain legal reasons for processing personal data are outlined by the GDPR and other evolving equivalent regulations throughout the globe. While consent is the most prominent legal basis for data processing, it is not the only one. Therefore, data processors should determine the legal basis for processing that they will depend on in each given case.

Consent is unquestionably a legitimate legal basis for processing in many instances, and is often gained by a signed consent form or, in certain situations, by implication. But the GDPR says that it should be just as easy to take away consent as it is to give it.

Some data processor operations may come within the realm of public interest or statutory obligations if the processor is an employee or contractor of a public authority or government agency. Article 89 of the GDPR stipulates that Member States may allow derogations to permit processing for scientific or historical research purposes. Another legal basis that may be applicable is that of legitimate interest, provided that the individual rights of data subjects who may be the subject of the study do not override the legitimate interest of the research organisation to conduct the data processor.

Inclusion of a List of Users' Rights that are Binding in Law

This guarantees users the ability to control their data in accordance with fundamental rights, which the law must mention as the GDPR sets these rights in several articles, such as:

1. The Right to Access Personal Data: GDPR provides data subjects with the right to view the data that a data controller has gathered on them. Within 30 days, the data controller must reply to that request.[6]
2. Right to Rectification: Individuals have the right to request that their data be modified, including the correction of mistakes and the updating of insufficient information.[7]
3. Right to Erasure: often known as the right to be forgotten enables a data subject to request that all processing of their personal data be halted and that their personal data be deleted.[8]
4. The Right to Restrict Data Processing: In certain situations, data subjects have the right to request that all processing of their personal data be halted. [9]
5. Right to be Notified: Data subjects must be informed clearly about the purposes for which their personal data will be used and about the remedies available to them if they believe their rights are being violated. Additionally, data subjects must be notified of any corrections or deletions of their personal data according to sections 16, 17, and 18.[10]
6. Right to Data Portability: A data subject has the right to request the electronic transmission of their personal data file to a third party. If physically practicable, data must be delivered in a generally used, machine-readable format.[11]
7. Right to Object: If a data controller denies a request to cease data processing, the data subject has the right to object to the denial of their Article 18 right.[12]
8. The Right to Reject Automated Individual Decision-Making: Individuals have the right to object to automated processing of their

[6]Article 15 of GDPR.
[7]Article 16 of GDPR.
[8]Article 17 of GDPR.
[9]Article 18 of GDPR.
[10]Article 19 of GDPR.
[11]Article 20 of GDPR.
[12]Article 21 of GDPR.

personal data for the purpose of making choices about them if the processing has a material impact on them or results in legal consequences – for example, profiling .[13]

These rights are essential and were enacted by the European Union to protect personal data, which is essential to be enjoyed by the Iraqi individual when legislating the personal data protection act to guarantee the individual's rights to access, modify, delete, and restrict access to personal data.

Define a Clear Scope of Application

Given that violations related to digital rights and the protection of personal data are violations that go beyond the traditional form of many crimes, which are related to specific facts of time and place, and most of them are within the geographical territory over which the sovereignty of the state is located, but the matter here is different and a problem arises when formulating personal data protection laws around the world. There are those who tend to expand the scope of the application to include any individual or entity on the territory of the state, as well as any entity anywhere else in the world, whether it belongs to the state, or it processes the data of its citizens. But in that case, more complications and potential conflicts of law arise. Which is important to take into account when drafting legislation. As the GDPR scope is applicable as follows:[14]

1. This Regulation applies to the processing of personal data in the context of the activities of a controller's or processor's establishment in the EU, no matter where the processing takes place.
2. This regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor who is not based in the Union, when the processing activities are related to
3. The provision of goods or services to such data subjects in the EU, regardless of whether payment by the data subject is required; or
4. The monitoring of their behaviour is permitted as long as it takes place within the EU.
5. This regulation applies to the processing of personal data by a controller not established in the EU, but in a place where Member State law applies by virtue of public international law.

When drafting a bill to safeguard personal information, legislators should focus on this aspect first. First, its relevance to organizations, entities, offices, and agencies in both the public and commercial sectors. Second, its implementation for cross-border processing, in order to prevent ambiguity. Whereas the 2011 Iraqi Information Technology Crime Law Bill did not address this issue and did not specify the extent of its applicability, the draught must be revised to be more transparent.

The GDPR applies, for instance, to the processing of personal data entirely or partially by automated means, as well as to the processing of personal data that is or is intended to be part of a file system but is not processed by automated means. The GDPR does not apply to an individual's processing of personal data in the context of a purely personal or domestic activity.

The GDPR only applies if the processing is carried out in the context of an establishment of the controller or processor in the EU, or if the controller or processor does not have an establishment in the EU but processes personal data in relation to the offering of goods or services to individuals in the EU, or monitoring of the behaviour of individuals in the EU to the extent that their behaviour occurs within the EU. This implies that many non-EU businesses with EU consumers will be required to comply with the GDPR's data protection rules.[15]

The bill's broad application is an essential characteristic. If enacted, it will apply to all businesses in Iraq with the exception of those expressly exempted. This would cover any business that collects data via automated techniques. The DPA will have the authority to classify small organisations depending on revenue, data volume handled, and data collection reasons.[16] This includes not just technology corporations and e-commerce platforms, but also real estate firms and brokers, banking business correspondents, automobile dealers, hotels, and restaurants. For background, 23 million small enterprises in the European Union are impacted by the GDPR. The expansive nature of the measure needs a thorough understanding of its contents and their anticipated effects.

In addition, the Iraqi legislator needs to clarify the scope of its application to include anyone who committed one of the stipulated actions when

[13] Article 22 of GDPR.
[14] Article 3 of GDPR.
[15] Article 3(2) of the GDPR.
[16] "Millions of Small Businesses Aren't GDPR Compliant, Our Survey Finds," GDPR.eu, May 20, 2019. https://gdpr.eu/2019-small-business-survey/

the processer is inside Iraq or outside, or was a non-Iraqi residing inside the country, or was a non-Iraqi outside the country as long as the processing is related to Iraqi data subject in cross-border.

Reducing the Exceptions

The General Data Protection Regulation GDPR in the second article includes data that are subject to this law as the law does not apply to the processing of data related to public security and criminal law as well as treatment by natural persons in the context of purely personal and domestic activities.[17] Article 3 of the same law stipulates the region and who is responsible for viewing and processing data, as any processing that takes place outside the borders of the European Union is not subject to it unless the data of a citizen belonging to the European Union is processed.[18]

As is the case with the general data protection legislation, the Iraqi draught law must include specific exclusions to the types of personal data not covered by the personal data protection principles and other measures exempting certain scenarios from the notice and consent requirements. Where they are similar to the European regulation and the standards cited by the researcher, it is necessary to identify who is responsible for granting such authorizations for the processing of personal data.

Establish Adequate Level of Protection in Iraq for Securely Transferring Data to Third Countries

Article 45 (1) of the GDPR states that data transfers to a third country or international organisation are only permitted if the third country, territory, or one or more specified sectors within that third country or international organisation provides an adequate level of protection. The European Commission adopted the concept of an adequate level of protection to ensure the transfer of data from the European Union to third countries or an international organisation. It must be equivalent to the degree of protection found in the European Union, where robust and enforced data protection measures are required. These regulations were referenced in the GDPR article 45 (2).

The European Commission shall take into account the legal system, the respect for humanitarian law, relevant laws, the presence and effectiveness of one or more independent supervisory authorities, and the third country's or international organization's international obligations.[19]

According to the European Regulation, it is prohibited to share personal data with any third country that does not have a sufficiency decision which is a decision issued by the European Commission, indicating that counties need sufficient protection according to its internal law or in accordance with its international obligations, the European Commission has the authority to grant a third country a sufficiency decision or not, and many countries seek to obtain one. This principle includes refraining from sharing personal information with third countries via space agencies or others if those countries do not have a sufficiency decision, and the law must specify the procedures for data transfer to those countries.

Main Personal Data Principles

Fundamental principles of data protection should exist. These do not have to be identical to the GDPR language, but they should reflect and be compatible with the notions entrenched in European data protection legislation to protect personal data and sensitive personal data and determine the obligations of the data controller and data processor.

1. Grounds for lawful and fair processing for legitimate purposes: the legal grounds for processing personal data lawfully, fairly, and legitimately should be adequately obvious. The European framework recognises many of these legitimate grounds, including rules in national law, the data subject's permission, the fulfilment of a contract, or the data controller's or a third party's legitimate interest that does not outweigh the individual's interests.
2. The purpose limitation principle: Data should be processed for a defined reason and then utilised only in ways that are consistent with the processing purpose.
3. The data quality and proportionality principle: personal data must correct, the data collected should be appropriate, relevant, and not overwhelming in connection to the processing aims.
4. Data Retention principle: As a general rule, personal data should be retained for no longer

[17]Article 2 of the GDPR.
[18]Article 3/2 of the GDPR.
[19]Article 29 data protection working party, adequacy referential, dopted on 28 November 2017 As last Revised and Adopted on 6 February 2018. https://ec.europa.eu/newsroom/article29/items/614108. Last visited, 27 Apr. 22.

than is required for the reasons for which it is processed.

5. The security and confidentiality principle: Any entity that processes personal data must guarantee that the data is treated securely, especially protection against unauthorised or illegal processing and accidental loss, deletion, or damage, by implementing adequate technological or organisational safeguards.
6. The transparency principle: every person should be notified in a clear, readily available, succinct, transparent, and understandable manner about all material aspects . This statement should contain the objective of the processing, the data controller's identity, the rights granted to data subject, and any other information essential to guarantee fairness. Particular exemptions to this right may arise under certain circumstances, such as to protect investigations, national security, judicial decision or other significant public benefit purposes, as is the case with Article 23 of the GDPR.

These are vital principles that should be included into the Iraqi data protection legislation. There must be a legal basis for processing the data and the data must be addressed to that specific reason. Additionally, there must be a principle of data quality, which means that the data must be accurate and relevant to the purpose without going beyond the purpose; furthermore, the data should not be retained for longer than the time specified in the processing; moreover, the confidentiality of the data must be guaranteed, particularly against unauthorised interference. Finally, the idea of transparency is required because the data subject must be informed explicitly of the purpose of the processing, the identity of the data controller, and the data subject's rights in connection with the processing.

Develop Mechanisms to Prevent and Report Data Breaches

This approach promotes a spirit of continual progress toward mechanisms that safeguard data and prevent breaches by keeping with technical advancements and using professionals in the fields of communications, data, and technology to construct electronic work mechanisms. Among these mechanisms is the existence of an independent authority; accountability; remedies; liability; and penalties.

1. Independent Supervisory Authority

This principle emphasises the importance of an independent authority overseeing the law's strict implementation and the imposition of fines on companies that fail to adequately comply with international law and standards when processing personal data. It is a requirement of the European Union for all states to provide an independent authority that is responsible for monitoring the application of the law and protecting the basic rights of individuals.[20]

Iraq needs to set up an independent supervisory. Its main qualities will be impartiality and independence, and it will have the power and ability to carry out the missions needed to make sure that human rights standards for data protection are being met.Additionally, it has its own budget and the authority to undertake investigations as needed. The proposed legislation should authorise the minister to form an independent commission to safeguard personal data in order to carry out the bill's specified duties. This organisation is comprised of officials and staff who carry out their duties under the guidance of the minister.

In the majority of statutes, the researcher discovers that the law grants the minister the authority to select personnel working under the minister's supervision in order to carry out the activities specified in the statute. It is natural that this paragraph creates a barrier between the law and its execution by an independent commission, since this body must be independent of the government, the biggest processor of personal data, in order to adequately safeguard personal data and perform its statutory responsibilities.

For instance, there are models of international data protection legislation for different countries, such as Canada, France, and the United Kingdom, where they have specialised commissions that regulate the flow of data and work to protect it, as Article 51/1 of the General Data Protection Regulation stipulates.

2. Accountability

Article 5(2) of the GDPR says: The controller shall be responsible for, and be able to demonstrate compliance with, paragraph1.

The principle of accountability requires the data controller to verify compliance with all Privacy Principles obligations. Such measures may include,

[20]Article 51 of GDPR.

but are not limited to, policies and procedures. individuals' rights, transparency, processing records and lawful basis, contracts and data sharing, risks and data protection impact assessments, records management and security, breach response and monitoring.[21]

To demonstrate accountability, the controller must have appropriate policies and procedures in place, including not only the privacy notice, but also a record of processing activities, a process for dealing with individuals' requests to exercise their rights, a process for using data protection impact assessments, a data retention and destruction policy, and a policy for the control of subcontracted research organisations and any international transfers of personal data in the course of the research.

Data protection is very important for any data protection bill because it defines the functions of data controllers and to ensure the legitimacy of data flow by data processors. These movements must be ensured through privacy tools and policies in a transparent manner while determining the legal basis for such processing. Otherwise, data violation will be very easy and without any accountability.

3. Remedies, Liability and Penalties

Each data subject should have several rights for judicial remedies as stated in Article 75 of the GDPR that:

"Every natural person shall have the right to a judicial remedy if they consider that their rights under this regulation have been infringed as a result of the processing of their personal data in non-compliance with this regulation".[22]

a. The right to lodge a complaint with the data supervisory authority.
b. Right to an effective judicial remedy against a supervisory authority.
c. Right to an effective judicial remedy against a controller or processor.
d. Representation of data subjects.
e. Suspension of proceedings.
f. Right to compensation and liability.
g. General conditions for imposing administrative fines.

The law needs to provide the grounds to complain against and to the supervisory authority, against data controllers and data processors, and the right to represent the data holder, as well as compensation and liability, and impose fines on anyone who has violated the principles of personal data protection. This process requires a judiciary that is concerned with these violations and trained to deal with them.

Compliance Difficulties with New Technologies

Data protection is a rapidly evolving field that is continually influenced by technological advancements and business policy development. The age of the Internet and electronic information, which ushered in a new idea, influenced the notions of economics and commerce. The notion of the Internet has increased people's awareness of e-commerce, or business conducted via the network and websites.[23]

The link between data protection and technology advancements is always evolving, but three recent advancements highlight this issue: cloud computing, the internet of things, big data analytics. Every one of those methods poses new difficulties for data protection, notably in the areas of the definition of personal data and the administration of cross-border data transfer.

1. Cloud-computing

Numerous jurists and academicians have described cloud computing, but with the finest description being at the 2013 United Nations Conference on Trade and Development, UNCTAD, which defined cloud computing as a way of delivering applications, services, or content remotely to end users, rather than requiring them to hold data, software, or applications on their own devices, a process known as "virtualization."[24]

During the forecast period, the cloud computing market is expected to grow at a compound annual

[21]Article 29 data protection working party, adequacy referential, dopted on 28 November 2017 As last Revised and Adopted on 6 February 2018.
https://ec.europa.eu/newsroom/article29/items/614108.
Last visited, 27 Apr. 22.

[22]Article 75 of GDPR.

[23] Männistö, L. (1999). Electronic commerce in Asia. Asia and the Future of the World Economic System, March, 1-13.

[24]Information Economy Report 2013: The Cloud Economy and Developing Countries, https://unctad.org/system/files/official-document/ier2013_en.pdf. Last visited 11 May 2022.

growth rate (CAGR) of 16.3 percent, from USD 445.3 billion in 2021 to USD 947.3 billion in 2026.[25]
Cloud computing services remain to provide certain issues for data security, particularly in terms of cross-border data transfers. The desire to protect personal data in cloud computing in Iraq needs legislation and severe data localisation standards to follow the data flow cross-border. The capabilities and advantages of the cloud inspire the discovery of potential risks to user privacy and personal data security:[26]

1. Multi-tenancy: A group of users share services and use the components of the cloud infrastructure which could be risk for:
   - Confidentiality, smart phones and programmes provide a wide number of people access to the stored data;
   - Integrity, since it is feasible for certain cloud users to try to modify data without authorization;
   - Availability, giving access to public services, data, and capabilities everywhere and at any time might pose a challenge.
2. Data location: the data subject is unaware of the location of data storage.
3. Regulatory compliance: It is difficult to ascertain whether the cloud service provider is the data controller or the data processor, and whether it is subject to an external assessment to evaluate the legality of its acts.
4. Privacy: there is no information what capacity of system restoring is provided.
5. Right to be forgotten: the data usually migrate among different nodes in the cloud and it is difficult to prove if the data are erased in the all places where they have been stored or not.

Cloud computing services don't really introduce any novel data protection challenges, but they still add to the difficulty of existing issues, particularly in terms of cross-border data transfers. Few governments have tried to establish legislation specifically geared to controlling the supply of cloud computing to date.

2. The Internet of Things (IOT)

Anything that connects to the Internet and exchanges data is called an internet of things device. There is also a clear link between the internet of things and personal data.
It is difficult to predict exactly how much the Internet of Things will develop in terms of value-added services in the future, but one piece of research predicted that by 2020, there could be anywhere from 20 to 50 billion linked devices, and between $3.9 and $11.1 trillion might be generated in 2025, according to another estimate.[27]
According to an Internet of Things (IoT) investigation by the Federal Trade Commission (FTC), health and fitness monitors, home security gadgets, linked vehicles, and household appliances are just a few examples of how the Internet of Things is already having an influence on the everyday lives of millions of Americans. Other possible benefits include greater health monitoring, safer roads, and more efficient use of household energy.[28]
The Internet of Things (IoT) has two primary privacy and data protection concerns:
a) Confidentiality: the system might be disrupted due to the fact that all objects and things have unique identifying codes and can freely interact over the internet or other networks. There is no way to guarantee the secrecy of all data supplied from end points, but the analysis of data that is often received by multiple points may include sensitive information for a person. Despite this, the proliferation of sensors raises the possibility of security and privacy breaches because of the collection of data. It is possible to learn about a person's habits, health and religious beliefs, and more by hacking smart sensors.
b) Traditional passwords are used to setup a variety of computers and internet gadgets, which might be vulnerable to a variety of different assaults. Components with poor levels of "cyber hygiene" are targeted by the assaults, which seek to exploit these components' vulnerabilities to hacking and manipulation. Traditional methods of identity verification are often employed in IoT security and don't provide the level of access restriction needed. Devices with unchangeable factory default passwords may also be used.

[25]Cloud Computing Market by Service Model (Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)), Deployment Model (Public and Private), Organization Size, Vertical, and Region - Global Forecast to 2026. Cloud Computing Market by Service Model (Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)), Deployment Model (Public and Private), Organization Size, Vertical, and Region - Global Forecast to 2026. Last visited 12 May 2022.

[26]Romansky, R.P., & Noninska, I.S. (2020). Challenges of the digital age for privacy and personal data protection. Mathematical Biosciences and Engineering, 17(5), 5288-5303.

[27]Manyika, J., Chui, M., Bisson, P, Woetzel, J., Dobbs, R., Bughin, J., & Aharon, D. (2015). The Internet of Things: Mapping the value beyond the hype (Vol. 24). New York, NY, USA: McKinsey Global Institute.

[28]Gathani, M. (2016). Internet of Things Report: The FTC Overstepped its Agency Rulemaking Authority. Business and Public Administration Studies, 10(1), 27-36.

It is possible to state that Iraq has to grasp the IOT's nature in order to forecast and pass a legislation that can deal with this new technology.

3. Big Data Analytics (BDA)

"Big Data analytics" is a methodology for analysing large data sets to reveal patterns, trends, and associations. The report of the United Nations conference mentioned several privacy concerns arising from the use of Big Data analytics. It is often cited as the "future" or the "solution" to myriad current problems and issues in society, technology, and the economy.[29]

- The enormity and worth of the data sets involved makes them a subject for security breaches.
- It is possible that the data was originally acquired for a variety of reason.
- Because they are "public registries," certain data sets are exempt from typical data protection regulations.
- A key principle of the Big Data approach is that all data should be collected and stored in case it proves to be "useful" at some point in the future.
- In certain cases, Big Data analysis and decision-making entails the employment of standards and mechanisms that are not clear or visible to the public.

Using the BDA in a different way than it was intended would be a violation of the crucial concept of data accuracy, "Defining the aim." What is the assurance that the obtained data is accurate, exact, and complete as required by the GDPR? Another GDPR criterion of data accuracy, “data minimization," is violated because of the huge quantity of the acquired data. As a result of incorrect "big data" interpretation, In addition, the GDPR criteria for anonymization and pseudonymization of personal data cannot be met by BDA in corporate marketing research, which might lead to inaccurate results and jeopardise the reputation of people, for example, when recruiting personnel.[30]

In summary, cloud computing, IOT, and BDA bring data protection challenges, but they do so with the difficulty of existing issues, particularly in terms of international data transfers. Few governments have tried to establish legislation specifically geared to controlling the supply of cloud computing to date. It is possible to state that Iraq has to grasp the IOT's nature in order to forecast and pass legislation that can deal with this new technology. It is not obvious what techniques and tools (algorithms, software, programmes, etc.) are utilised for the BDA and this would breach the requirement of data processing openness.

Findings

In the first section of this paper, the researcher examined the standards that are crucial for the implementation of a complete legal framework, beginning with:

1. The legislation must define all relevant terms, including personal data, sensitive personal data, data controller, data processor, consent, cookies and similar technologies, cross-border processing, data minimisation, data portability, data protection commission, data protection impact assessment, data subject, legal basis, legitimate interest, personal data breach, privacy by design, pseudonymisation, recipient, restriction of processing.
2. The GDPR and other worldwide standards justify some data processing practices. Consent is the most common legal basis for processing personal data. Data processors must specify the legal basis for each processing instance. Consent is frequently sought by a signed permission form or, in certain cases, via implication. Under GDPR, consent must be revoked as simply as it is given.
3. The GDPR sets out seven principles for the lawful processing of personal data. Processing includes the collection, organisation, structuring, storage, alteration, consultation, use, communication, combination, restriction, erasure or destruction of personal data. Broadly, the seven principles are: lawfulness, fairness, and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; accountability. These principles are at the heart of the GDPR; they are the guiding principles of the regulation and compliant processing. Data controllers are responsible for complying with the principles and letter of the regulation. Data controllers are also accountable for their processing and must demonstrate their compliance.

[29]United nations conference on trade and development report 2016. https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf. Last visited 14 May 2022.

[30]Romansky, R.P., & Noninska, I.S. (2020). Challenges of the digital age for privacy and personal data protection. Mathematical Biosciences and Engineering, 17(5), 5288-5303.

4. In addition, there are many rights of data subjects that Iraqi legislators need to recognize, such as: the right to be informed; the right to access information; the right to rectification; the right to erasure; the right to data portability; the right to object to processing of personal data; the right of restriction; the rights in relation to automated decision making, including profiling.
5. The scope of application is divided into two branches of applicability to individuals, companies, institutions, offices, and agencies in the private and governmental sectors. Second, its implementation for cross-border processing to avoid ambiguity. The Iraqi legislator must specify the extent of its application to include anybody who has committed one of the prescribed activities, whether the processer is within or outside Iraq, or a non-Iraqi resident inside or outside the nation. The Iraqi legislator needs to clarify the scope of its application to include anyone who committed one of the stipulated actions when the processer is inside Iraq or outside, or was a non-Iraqi residing inside the country, or was a non-Iraqi outside the country, as long as the processing is related to Iraqi data subject cross-border.
6. Excluding policy needs to be determined under certain articles in the enacted law when excluding some parties from data processing principles. It is important to know who is responsible for authorising their processing.
7. The need to establish specific procedures to assure the implementation of the law, such as the existence of an independent authority, determining accountability, and ensuring the legality of data flow via data processors
8. The legislation must establish the reasons for complaints against and to the supervisory authority, against data controllers and data processors, as well as the right to represent the data owner, compensation and accountability, and sanctions for anybody who has breached the principles of personal data protection. This procedure necessitates a court that is concerned with and equipped to deal with these infractions.

In the second section of this paper, the researcher looked at the compliance issues with new technologies in Iraq:

1. The researcher discovered that one of the challenges of cloud computing's presence is that millions of users use the same cloud computing service, posing a challenge to the problem of secrecy. In addition, some users may edit or remove personal data, which affects the integrity value. In addition, the data location is unknown, which raises the law applicability issues. Moreover, the right to be forgotten is merely impossible due to the data transition in different places, which makes the deletion of data not certain.
2. The internet of things IOT can be defined as anything that connects to the Internet and exchanges data. This raises the same issues in cloud computing such as confidentiality issues, as no assurance exists that all personal data will remain private and confidential from the beginning of the personal data life cycle to the end point when hacking these devices may identify a person's habits, beliefs, health, and religious data.
3. Big Data analytics (BDA), as explained previously, is a methodology for analysing large data sets to reveal patterns, trends, and associations. This technology captures and saves the maximum amount of public data that may be utilised in the future since it has a high monetary value. Because they are public documents, they are exempt from the rules governing the protection of personal information.

Therefore, Iraq must comprehend the nature of emerging technologies in order to anticipate and enact laws that can accommodate them.

Conclusion

The Iraqi legislator should be aware of these advanced purifies that process data and develop mechanisms to ensure the flow of data in accordance with the international standards we have set earlier because technological development continues and it is directly linked to the country's economy. In light of Iraq's status as a third-world nation, this development presents the Iraqi legislature with formidable obstacles and challenges. It will not be simple to pass.

The most important situation that the Iraqi legal framework will face is the contentious reality.

- Create a bill that does not comply with human rights standards, as it guarantees the rights and freedoms of individuals, and otherwise will make the legal draught unconstitutional.
- If Iraq wants to follow in the footsteps of international human rights standards, the best

way is to establish cross-border comprehensive legal rules.

- In the event that any law for privacy and protection of personal data has been established, the inefficiency of this law will put Iraq on the brink of danger, as happened with the draught Iraqi cybercrime law, where he received much criticism from the United Nations envoys for its inefficiency.

The researcher emphasises that the legislator must intervene in the enactment of a law to preserve the privacy of personal data, elaborating on the rules and limits applicable to the handling of such data. A legal rule must criminalise its assault, destruction, modification, or falsification, as well as its disclosure or tampering. Specifies how entry, modification, addition, and deletion are permitted. There is no option but to establish a comprehensive law that protects personal data in accordance with the international standards.

References

Article 29 data protection working party, adequacy referential, dopted on 28 November 2017. As last Revised and Adopted on 6 February 2018. https://ec.europa.eu/newsroom/article29/items/614108. Last visited, 27 Apr. 22.

A/HRC/48/31: The right to privacy in the digital age - Report of the United Nations High Commissioner for Human Rights, https://www.ohchr.org/en/documents/thematic-reports/ahrc4831-right-privacy-digital-age-report-united-nations-high. Last visited, 24 April 2022.

El-Madawy, "Protection of the Information Privacy of the User through Social Networking Sites, a Comparative Study", Faculty of Law - Benha University, https://mksq.journals.ekb.eg/article_30623_1ab2f80af612aa4568dbf6239b535ac2.pdf. Last visited, 10 May, 2022.

Gathani, M. (2016). Internet of Things Report: The FTC Overstepped its Agency Rulemaking Authority. *Business and Public Administration Studies*, *10*(1), 27-36.

Iraqi Information Crimes Law, Poorly drafted law and brutal penalties that violate the right to due process and violate freedom of expression, 2012. https://www.hrw.org/reports/iraq0712ar.pdf.

Iraqi Digital Media Center DMC report of April 2022, non-governmental organization. https://www.alaraby.co.uk/entertainment_media/العراق-مليون-مستخدم-نشط-لمواقع-التواصل-28. Last visited, 25 April, 2022.

Information Economy Report 2013: The Cloud Economy and Developing Countries. https://unctad.org/system/files/official-document/ier2013_en.pdf. Last visited 11 May 2022.

"Millions of Small Businesses Aren't GDPR Compliant, Our Survey Finds," GDPR.eu, May 20, 2019. https://gdpr.eu/2019-small-business-survey/.

Männistö, L. (1999). Electronic commerce in Asia. *Asia and the Future of the World Economic System, March*, 1-13. http://ftp.unpad.ac.id/orari/library/library-ref-eng/ref-eng-1/application/e-commerce/e-commerce-asia-1998.pdf

Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J., & Aharon, D. (2015). *The Internet of Things: Mapping the value beyond the hype* (Vol. 24). New York, NY, USA: McKinsey Global Institute.

OHCHR Annual Report, The Impact of New Technology on the Promotion and Protection of Human Rights in the Context of Assemblies, Including Peaceful Protests, 3 July 2020, https://www.nhrc-qa.org/wp-content/uploads/2014/01/العهد-الدولي-الخاص-بالحقوق-المدنية-والسياسية.pdf. Last visited, 25 April 2022.

Organisation for Economic Cooperation and Development guidelines annex to the recommendation of the Council of 23 September 1980, guidelines governing the protection of privacy and transborder flows of personal data, https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/OECD_Privacy_Guidelines_1980.pdf

Romansky, R.P., & Noninska, I.S. (2020). Challenges of the digital age for privacy and personal data protection. *Mathematical Biosciences and Engineering*, *17*(5), 5288-5303.

United nations conference on trade and development report 2016. https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf