Research Journal in Advanced Humanities

RJAH

https://doi.org/10.58256/1akswg81

Open Access

Check for updates

RESEARCH ARTICLE

Section: *Philosophy & Religion*

Civil protection of personal electronic data in the Emirati legislation

Abdulla Rashed Ali Bin Shahein Alhefeiti[1], Saif Khamis Mohammed Marzooq Aldahmani[1], Alyaa Ali Khameis Rashed Alyammahi[1], Saadah Saif Saeed Ahmed Alzeyoudi[1] and Ahood Abdulla Mohamed Shaml Alraeesi[1]

[1]College of Law-Fujairah University, Fujairah, United Arab Emirates

*Correspondence: 202410022@fu.ac.ae

ABSTRACT

That digital revolution has transformed industries, but privacy protection challenges persist. Countries like the UAE have established legal frameworks for civil liability that balance the benefits of technology with individual rights. However, classification raises issues like contractual breaches, tort liability, and jurisdictional conflicts. Research on civil liability is crucial for ensuring legal certainty and trust. The Protection of Electronic Personal Data is deemed one of the fundamental pillars of digital security in the modern era. It plays an essential role in protecting individuals' privacy and preventing the misuse of their information for illegal activities, such as fraud and identity theft. Besides, it strengthens the users' trust in the electronic transactions and supports compliance with local and international laws and regulations related to information security. In fact, its significance extends to protecting community and national security, as data leaks might threaten stability or be used to manipulate public opinion. Therefore, securing data is a basic requirement for achieving safe digital transformation and ensuring that individuals and communities can benefit from electronic services efficiently and with confidence. The current research aims to provide a comprehensive understanding of "Civil Protection of Electronic Personal Data" by examining the national and international legal frameworks that regulate this field, in addition to analyzing the forms of civil liability that would result from violating such data, whether contractual or tortious, along with the resulting legal consequences. Moreover, it seeks to highlight the essential role of this protection in safeguarding the right to privacy, which is fundamental to human dignity, and to evaluate the effectiveness of the available judicial mechanisms that enable individuals to claim compensation for damages resulting from electronic attacks. Finally, this research aims to formulate legislative and practical solutions and proposals to strengthen the civil protection system and ....

Research Journal in Advanced Humanities

Volume 6, Issue 4, 2025

ISSN: 2708-5945 (Print)

ISSN: 2708-5953 (Online)

ARTICLE HISTORY

Submitted: **18 September 2025**

Accepted: **16 November 2025**

Published: **28 November 2025**

HOW TO CITE

Alhefeiti, A. R. A. B. S., Aldahmani, S. K. M. M., Alyammahi, A. A. K. R., Alzeyoudi, S. S. S. A., & Alraeesi, A. A. M. S. (2025). Civil protection of personal electronic data in the Emirati legislation. *Research Journal in Advanced Humanities*, 6(4). https://doi.org/10.58256/1akswg81

Published in Nairobi, Kenya by Royallite Global, an imprint of Royallite Publishers Limited

enhance individuals' and institutions' awareness of the importance of safeguarding personal data in the digital environment. The legal protection of electronic personal data under UAE Law is considered a pioneering step toward enhancing national security and preserving individual privacy. Federal Law No. 34 of 2021 reflects the state's commitment to keeping pace with technological developments and to addressing risks to personal data. In this study, we have concluded the following key findings and recommendations. Personal Data Protection Law No. (45) of 2021 is an essential step on the right path towards the economic development of the United Arab Emirates in general, and the digital economy and e-commerce in particular. Personal data refers to any information related to identified individuals or those who can be identified through it, such as name, address, national number, and others. Exposing electronic personal data poses risks, necessitating individual awareness and improved security measures. UAE Law penalties deter violations, promote compliance, and raise awareness. Violations of privacy laws result in criminal penalties and civil liability. Victims have the right to request cessation and compensation.

KEYWORDS: civil protection, personal data, digital technology, right to privacy

Introduction

In the wake of the modern digital revolution, personal data is considered an essential foundation of the digital economy and information society, where it is widely used across fields such as electronic trade, banking services, marketing, healthcare, and general affairs management. As a matter of fact, this unprecedented development in data collection and treatment has created unique and creative opportunities for evolution. In return, serious challenges to individual privacy protection have been raised. It is worth noting that an attack on personal data might take several forms, such as collecting and storing it without the owner's consent or disclosing it to unauthorized parties for illegal purposes. This type of violation not only damages the individual's reputation and emotional well-being, but it may also result in material and mental losses, such as identity theft, financial fraud, or the exploitation of data for extortionate or illicit commercial purposes. Many countries, indeed, including the United Arab Emirates, have sought to establish legal frameworks and advanced legislation to protect personal data. These laws strive to balance the benefits of technology with the protection of individuals' fundamental rights.

In this context, civil liability emerges as one of the most important legal mechanisms for protecting individuals and their rights, enabling them to claim compensation for any harm resulting from unlawful interference with their personal data. However, the classification of this liability raises multiple problems, such as breach of contractual obligations, tort liability for a wrongful act causing damage to others, or a distinct form of liability that combines traditional characteristics with those shaped by the particularities of the digital environment. The application of tort liability in this area confronts practical difficulties related to proving the wrongful act, the damage, and the causal link in a rapidly changing virtual world, where data can be copied and circulated across international borders in seconds, raising issues of jurisdiction and conflicts of law. Accordingly, the study of civil liability for electronic personal data is a rich field for research, as it brings together legal, technical, and ethical considerations, and requires legislators, jurists, and courts to seek solutions that would balance the protection of an individual‘s right to privacy on the one hand, and the encouragement of digital innovation and information exchange on the other, within a regulated framework that ensures legal certainty and preserves individuals' trust in the digital environment.

Importance of the Study

The Protection of Electronic Personal Data is deemed one of the fundamental pillars of digital security in the modern era. It plays an essential role in protecting individuals' privacy and preventing the misuse of their information for illegal activities, such as fraud and identity theft. Besides, it strengthens users' trust in electronic transactions and supports compliance with local and international laws and regulations related to information security. In fact, its significance extends to protecting community and national security, as data leaks might threaten stability or be used to manipulate public opinion. Therefore, securing data is a basic requirement for achieving safe digital transformation and ensuring that individuals and communities can benefit from electronic services efficiently and with confidence.

Research Objectives

The current research aims to provide a comprehensive understanding of "Civil Protection of Electronic Personal Data" by examining the national and international legal frameworks that regulate this field, in addition to analyzing the forms of civil liability that would result from violating such data, whether contractual or tortious, along with the resulting legal consequences. Moreover, it seeks to highlight the essential role of this protection in safeguarding the right to privacy, which is fundamental to human dignity, and to evaluate the effectiveness of the available judicial mechanisms that enable individuals to claim compensation for damages resulting from electronic attacks. Finally, this research aims to formulate legislative and practical solutions and proposals to strengthen the civil protection system and raise awareness among individuals and institutions of the importance of safeguarding personal data in the digital environment.

Research Problem

With the rapid pace of technological development and the growing use of digital media across various aspects of life, electronic personal data has become vulnerable to multiple threats, including hacking, leakage, and misuse. This raises fundamental questions about the extent to which civil liability rules respond to the requirements of protecting personal data in an electronic environment, and about the limits and mechanisms for activating this liability in a way that would achieve a balance between the individual's right to privacy and the demands of digital development.

Research Methodology

The researcher has mainly relied on a Descriptive-Analytical Method, describing the concept of "Electronic Personal Data," clarifying its characteristics, and analyzing relevant national and international legal texts on civil protection to identify the risks threatening the privacy of personal data and to address and protect it.

Research Plan

1. Nature of Electronic Personal Data Protection
1.1 Concept of Electronic Personal Data Protection
1.2 Characteristics of Electronic Personal Data Protection
1. 3 Legal Protection of Electronic Personal Data
2.1 Risks Faced by Electronic Personal Data
2.2 How the Law Addresses the Risks Faced by Electronic Personal Data

Nature of Electronic Personal Data Protection

In light of rapid technological developments, protecting electronic personal data has become a matter of great importance in the digital age, as the risks of privacy violations and attacks on personal information have increased significantly. This protection involves the legal and transparent collection and processing of data, along with defining the specific purposes for which the data is collected and retaining it for the necessary duration. The protection of electronic personal data is a modern topic that needs further clarification. Therefore, it is essential to define this concept and explain its most critical characteristics.

Concept of Electronic Personal Data Protection

Before discussing the concept of electronic personal data protection, it is necessary to clarify the idea itself, which revolves around information and data related to a specific natural person whose identity is, or can be, directly or indirectly identified.[1] The UAE Law has defined personal data in Article No. 01 as "any data related to a specific natural person or related to a natural person who can be directly or indirectly identified through linking data, and through the use of identification elements such as his name, voice, or more of his physiological, physical, economic, social, or cultural characteristics." The legislator has done well by specifying the types of personal data eligible for legal protection, giving examples that clarify the concept and making it more precise with a definition that easily encompasses the various types of personal data. Similarly, the Jordanian Law defines personal data as "any data or information from any source or form relating to a natural person, which can be

used to identify them directly or indirectly, regardless of its source or form, and includes data related to their person, social or family status, or location."[2]

Article No, 04 / 01 of the European Regulation on the Protection of Personal Data defines it as "any information relating to a natural person, directly or indirectly, in particular by reference to an identifier or one or more elements specific to them such as name, identification number, location data, online contact identifier, or physiological, genetic, psychological, economic, cultural, or social characteristics." On the other hand, the Interpol defines personal data as "any information relating to an identified person whose identity can be revealed directly or indirectly by reference to an identification number or one or more elements related to their physical, physiological, genetic, psychological, cultural, social, or economic descriptions." Others have defined it as "the individual's ability to control the cycle of information related to them, i.e. the individual has the right to prevent thers from accessing their personal data and information and to be managed as per their wishes."[3]
These personal data include the following:

1. **Name & Surname**: an individual is identified and distinguished from others by their name, which is often divided into a given name, a nickname, and a surname. While the given name is the one registered on the birth certificate and identity card, the nickname is a name different from the given name by which the person is popularly known. As for the surname, it is the family name to which the individual belongs.
2. **Image & Voice**: one's image is deemed part of personal data that should be protected. Similarly, his voice is part of his personal data. Modern Digital Technology has enabled the processing of images and voices and their placement on a single platform alongside text, leading to their treatment as personal data.[4]
3. **Personal Numbers**: Every individual is distinguished and identified through an identity card number specifically assigned to them by the concerned authorities.
4. **Address**: one's address is considered part of the personal data, and it could be their residence or work.
5. **Marital Status**: This information pertains to the individual's family status and is considered personal data as well, such as married, unmarried, divorced, widowed, etc.
6. **Physical Characteristics**: Physical characteristics are also considered personal data, such as height or shortness, and other features.
7. **Nationality**: nationality is deemed personal information as well and is subject to legal protection.
8. **Fingerprint:** an individual's fingerprint is considered personal data, regardless of the fingerprint type, whether it is a fingerprint or a palm print.
9. The car number, bank account number, email address, and computer address can also be taken as personal data.

Characteristics of Electronic Personal Data Protection

Electronic personal data in the digital age is one of the most important strategic resources, as it has become a central focus for both government and private institutions. Daily transactions, electronic services, and communication through digital platforms all rely on the collection, processing, and storage of vast amounts of personal information, including individuals' names, addresses, financial or health data, and even biometric data, geographic location, and internet behaviour records. In this context, Federal Decree-Law No. 45 of 2021 regarding Personal Data Protection in the United Arab Emirates has been issued to establish a set of fundamental principles and characteristics that regulate how data is collected and processed, in addition to defining the responsibilities of controllers and processors, achieving a balance between individuals' right to privacy and the requirements of technological and economic development. Hence, the importance of analyzing these characteristics with scientific accuracy is evident, as they serve as the pillars upon which the Privacy Protection System in the UAE is based. The most important of these characteristics is listed below:

1. **Legitimacy, Transparency, and Justice**: These characteristics are deemed the cornerstone of any legal data protection system, as they require that all data collection and processing operations shall depend

on a specific legal basis. Besides, it forces institutions to practice transparency by clearly informing data owners of the purposes for which data are collected.

2. **Restriction & Confidentiality of Data**: The UAE Law emphasizes the necessity of implementing appropriate technical and organizational measures to protect data from any security breach, loss, or unauthorized alteration. This includes the use of encryption, access controls, and continuous employee training to ensure the confidentiality and integrity of data.
3. **Purpose of specification and storage duration**: Data collection must be for specific, clear, and legitimate purposes, and not to be used for other purposes unless the controller obtains approval for such action.
4. **Personal data must be accurate, secured, and confidential**: Data requires legal protection to ensure the accuracy of personal data and regular updates, with steps taken to correct or delete inaccurate information. Necessary measures shall be taken to protect data by implementing a specific system that enhances security and prevents unauthorized access, modification, disclosure, or unlawful destruction of the data in question.
5. **Responsibility and accountability**: It is required to establish strict laws and regulations regarding the protection of personal data, through written policies, processing records, appointing a data protection officer when appropriate, as well as conducting periodic risk assessments when necessary.
6. **The right to destruction & objection**: Individuals have the right to request the deletion of their personal data when it is no longer needed for processing, taking into account the relevant regulatory provisions. Individuals can also object to the processing of their personal data in certain circumstances, primarily if the processing relies on the data controller's legitimate interests.[5]
7. **Impact of data transfer & assessment protection**: Individuals can obtain their personal data in an organized and machine-readable format, in addition to transferring it to another party without obstacles. Moreover, periodic assessments can be conducted to identify potential risks to individuals' privacy and to take appropriate measures to mitigate them.
8. **Registration of activities process**: Detailed records of how personal data is collected, processed, and stored shall be registered.
9. **Monitoring & Supervising**: Independent bodies shall be appointed to monitor compliance with data protection standards and ensure the effective implementation of policies and procedures.[6]

Legal Protection of Electronic Personal Data

In the era of digital technology, electronic personal data has become one of the most critical assets that must receive legal protection. These data include sensitive information, such as identities, electronic signatures, and financial records, which are highly vulnerable to breaches and unlawful exploitation. There is a need for legislation that would ensure the protection of individual privacy and effectively regulate the collection, use, and storage of this data by institutions and individuals. Legal protection includes imposing strict rules on data processors to achieve a balance between technological development and the need to protect individuals' privacy. Accordingly, we shall address in this section the risks to electronic personal data, as well as the laws that address them.

Risks Faced by Electronic Personal Data

Electronic Personal Data is a fundamental issue in economic and social activity, as the Government and Private Institutions continuously collect and process this data to provide services, improve performance, and support their strategic decisions. However, this increasing reliance on data has created a fertile environment for the emergence of multiple risks that would threaten individuals' privacy and information security. These risks manifest in various forms, including technical issues such as cyberattacks, breaches, and malware, as well as information security infringements involving unauthorized attempts to access databases or electronic systems. There is also malicious software, including illegal encryption or the disabling of data to demand ransom, as well as phishing, where attackers deceive individuals into disclosing passwords or banking information through fake messages or websites. Lastly, security vulnerabilities in systems may arise from outdated or poorly designed

software, rendering data susceptible to exploitation. Accordingly, these threats vary depending on the stages that personal data goes through, and these risks can be classified into multiple categories, including:

1. **Hacking & Piracy**: These actions are illegal, attempting to access electronic systems or data to steal or disrupt them, and they are implemented through security vulnerabilities or by using malicious software to gain unauthorized access to data. These operations are often used to achieve financial gain, engage in espionage, or harm certain entities. To combat piracy, strict laws must be enforced, and continuous development of information technology must be adopted to protect digital data. Cyberattacks and piracy are among the most dangerous threats, as hackers target the theft of personal data —such as names, addresses, and credit card numbers — to use for illegal purposes and to harm others by compromising mobile phones, websites, and bank accounts.[7] IT specialists have confirmed that the technological development sweeping the world has raised concerns about networks following breaches. Experts also agreed that hacking and piracy would threaten the national security of all countries. This issue, however, has legal, security, economic, social, and political dimensions, and it is reasonably necessary to address the legislative gap to confront hacking activities. Many countries resort to applying traditional laws to cybercrimes, even though these laws are not capable of addressing them.[8]
2. **Phishing**: it relies on sending fake messages or links aimed at deceiving the user to obtain sensitive information, such as passwords or financial data. Therefore, phishing is considered one of the most common methods of economic crime, in which attackers create fake websites for banks, electronic payment companies like PayPal, and cryptocurrency trading platforms to deceive users and convince them to enter their personal data and login information. Tools like Evilginx or Modlishka are used to carry out advanced phishing attacks, intercepting login data in real time— including the two-factor authentication code —so attackers can access bank accounts and withdraw money without the victim's knowledge. BlackEye is also used to create professional phishing pages that mimic the official design of investment platforms and banks. Attackers can send links to these pages via email, text messages, or social media, leading the victim to believe they are logging in to their account.[9]
3. **Unauthorized Use**: This type of use is one of the most prominent challenges that confront societies in the digital age, as it directly affects an individual's right to privacy and raises complex legal, ethical, and technical issues. Such unauthorized use is any procedure for accessing, processing, storing, or sharing personal information without the owner's explicit permission or outside the established legal and regulatory framework. This means the issue is not just about data theft or system breaches, but also about cases where institutions or individuals use data in ways not approved by the owners, even if the data are initially obtained legally. Unauthorized use is also considered a violation of data protection principles established by many international and national legislations. Laws such as the UAE Personal Data Protection Law and the European Union General Data Protection Regulation (GDPR) emphasize the necessity of any data processing being based on clear legal grounds, such as consent, contract execution, or legal obligation. Any breach of these grounds constitutes unlawful use, exposing the violating party to accountability and penalties.
4. **Accidental Data Leakage**: This type of leakage occurs when personal data is lost or disclosed unintentionally due to human errors or security system failures. Examples include sending sensitive information to the wrong recipients, leaving unencrypted data on the internet, or weak server security. Accordingly, it exposes individuals to the risk of having their data exploited in fraudulent or illegal activities. Accidental leakage often results in significant reputational damage to institutions and financial losses, making it necessary to implement strict measures to protect data and reduce human error. Weak security measures in institutions can lead to the leakage of customers' personal data, leaving them vulnerable to breaches.
5. **Digital Tracking**: This process refers to the collection and analysis of data related to users' activities

on the internet, using tracking technologies such as cookies to gather information about users' online activity, which violates their privacy, along with digital analytics tools.

This tracking is used to understand the user behaviour, improve targeted advertisements, and customize the user experience. However, digital tracking raises many privacy concerns, as sensitive information is collected without the user's knowledge or consent. These practices may lead to the exploitation of data for commercial purposes or its use in illegal ways. Therefore, it has become necessary to regulate digital tracking through clear laws that ensure transparency and protect users' privacy.

6. **Identity Theft**: This type of theft intends to impersonate another person to deceive others, whether to achieve personal or financial gains or even to harm certain people. This may occur by using personal information, including names, photos, or official documents, without the owner's permission. This act constitutes a legal and ethical violation, as it threatens individuals' privacy and security. Identity theft includes various forms, such as document forgery and the creation of fake online accounts. These crimes indeed spread online through techniques such as phishing, malware, and identity theft, causing significant damage, including financial losses, reputational damage, and legal complications for victims.[10]
7. **Weak system protection**: such a system is often vulnerable to hacking and cyber threats that may result in data loss, information leakage, or disruption of vital operations. It also indicates vulnerabilities in software or technical infrastructure that make it susceptible to cyberattacks. This weakness, however, can result from outdated software, incorrect security settings, or a lack of regular updates. To prevent these breaches, systems must be continuously updated, protection programs must be used, and strong security policies must be implemented.[11]
8. **Electronic Signature Breach**: It is considered a serious threat that challenges information and data security in the digital age. These signatures are used to verify identity and authenticate digital transactions, banking operations, digital contracts, and official correspondence, making their breach a threat to individuals and companies alike. In general, hackers rely on techniques such as phishing to access private encryption keys or use malware to extract electronic signature data, through identity forgery, executing illegal transactions, or manipulating electronic contracts, causing significant financial losses and loss of trust.

It should be noted that the UAE has imposed penalties on anyone who attacks data without the consent of the parties involved, as these crimes target commercial operations conducted over an international network. Accordingly, electronic signature crimes and data breaches are among the most significant threats to the growth of e-commerce and the expansion of its user base, as they weaken users' trust in these means for concluding commercial agreements.[12]

9. **Digital Identity Hacking**: Digital identity hacking is an illegal process through which the data related to a user's digital identity, such as passwords, identification numbers, or bank accounts, is seized by using advanced and modern technologies.

Summary

In short, these risks indicate that protecting electronic personal data is not purely a technical issue but a multi-dimensional matter, which requires integration between technical measures, such as encryption and protection systems, organizational procedures, like internal policies and training, and the legal framework that includes the UAE Data Protection Law, along with considering ethical and social aspects. Understanding and analyzing these risks is a fundamental step in developing effective cybersecurity and digital governance strategies.

Laws & Electronic Personal Data Risks

Several legal procedures have been put in place to minimize or avoid the risks to electronic personal data. They can be listed as follows:

1. **Enactment of Legislation regarding Individuals' Privacy Protection**: The UAE Federal Decree-Law No. 45 of 2021 constitutes the main legislative framework for protecting individuals' privacy. It provides definitions of the key principles that govern the collection and processing of data, such as the necessity of obtaining explicit consent before taking any action, as well as specifying the legal purpose behind the collection of data. Moreover, it obligates institutions to implement security and technical controls to prevent unauthorized access or misuse. This law also grants individuals fundamental rights, including the right to access their personal data, to correct or erase any part of it, and to object to its processing in some instances. Thus, it establishes oversight mechanisms through the UAE Personal Data Protection Office to ensure compliance and accountability, thereby achieving a balance between encouraging innovation and digital transformation on the one hand, and protecting privacy and individual freedoms on the other.
2. **Application of the UAE Personal Data Protection Law**: The application of this law aims to protect individuals' privacy, enhance digital trust, and regulate the processes of collecting, using, and storing data, ensuring that everything is implemented with explicit consent and for specific goals. Besides, the law requires companies and institutions to maintain transparency and provide the security and accuracy of data, obliging relevant entities to report any data breaches to the competent authorities. Implementation of this law is supervised by the Personal Data Regulatory Authority to ensure compliance with these standards. A Data Protection Officer might be appointed to monitor compliance with the regulations.
3. **Personal Data Processing Controls**: They represent the legal and ethical framework that aims to regulate the processes of collecting, using, and addressing data to ensure their compliance with relevant laws. Among these controls are
    a. **Legality & Transparency**: data processing must be based on a clear legal basis, such as obtaining explicit consent from the individual or the existence of another legal justification, with the necessity of providing clear and transparent information about how the data is used. Additionally, data must be collected and processed for specific, pre-declared purposes, with the prevention of their use for any purpose other than those for which they have been collected.
    b. **Accuracy & Correctness of Data**: According to these controls, data shall be accurate and correct, being regularly updated to avoid errors or outdated information that could affect decisions based on them.
    c. **Effective Technical & Organizational Measures**: these measures must be adopted to protect data from unauthorized access, use, or disclosure, including encryption mechanisms, monitoring, and internal information security policies.
    d. **Granting Individuals a Set of Rights**: they incorporate the right to access data, correct and delete it, in addition to objecting to its processing, which reinforces the principle of self-control over personal information.
    e. **R**esponsibility & Accountability: they are integrated with the processing entities that are responsible for establishing clear data management policies, conducting periodic assessments of the processing operations to ensure compliance with laws and controls, and bearing responsibility in case of a breach or violation.
4. **Obligations Related to Personal Data**: Obligations related to personal data represent legal and ethical duties imposed on entities that collect and process data. They aim to enhance privacy protection and ensure compliance with laws such as the UAE Personal Data Protection Law. These obligations include adherence to lawful processing and data transparency, ensuring that data collection is for specific and justified purposes, minimizing data to what is necessary, maintaining their accuracy, and taking technical and organizational measures to ensure their security. These obligations include respecting individuals' rights to access, correct, and delete their data, being notified of any breaches, adhering to clear documentation and policies for data management, and bearing responsibility for any violations.[13]
5. **Commitment to Confidentiality**: Commitment to the confidentiality of personal data is a legal and ethical principle that requires entities collecting or processing personal data to maintain its privacy

and prevent its disclosure or use in unauthorized ways. This commitment means that data must be handled within a framework that ensures its protection from unauthorized access or viewing, using appropriate technical and organizational measures such as encryption, access control, internal security procedures, as well as including employee training and ensuring their adherence to confidentiality policies to guarantee that data processing complies with laws such as the Personal Data Protection Law in the United Arab Emirates, thereby enhancing individuals' trust and protecting their rights.[14]

6. **The right to access information**: It is one of the fundamental rights of individuals in the field of personal data protection and constitutes an essential pillar to ensure transparency and accountability in processing. Therefore, individuals have the right to access all personal data collected and retained by the relevant entities, to know how it is used and the purpose for which it is maintained, enabling them to control their data and make informed decisions.

According to the Personal Data Protection Law in the United Arab Emirates, this right includes several key elements:

1. Access to data, where an individual has the right to request a copy of their personal data processed by the concerned entity, including details about the nature of the data and their source.
2. Knowing the purpose of processing, meaning that the individual must be informed of the objectives for which the data have been collected.
3. Access to retention periods, meaning knowing the length of time the entity will retain the data.
4. Knowing the parties with whom the data is shared, i.e., whether the data has been exchanged with other entities, and the purpose of that.[15]

Conclusions

The legal protection of electronic personal data under UAE Law is considered a pioneering step toward enhancing national security and preserving individual privacy. Federal Law No. 34 of 2021 reflects the state's commitment to keeping pace with technological developments and addressing risks that threaten personal data. In this study, we have concluded the following key findings and recommendations. Personal Data Protection Law No. (45) of 2021 is an essential step on the right path towards the economic development of the United Arab Emirates in general, and the digital economy and e-commerce in particular. Personal data refers to any information related to identified individuals or those who can be identified through it, such as name, address, national number, and others. This data is used to identify or communicate with individuals in personal or professional contexts. Electronic personal data is exposed to a wide range of risks that require individual awareness and improved security measures by institutions. Enhancing laws and adhering to modern security standards are key to ensuring data protection and privacy in the evolving digital world. The penalties stipulated in the UAE Law help deter violations and enhance compliance, providing a safe and sustainable digital environment. They also highlight the role of regulatory authorities in monitoring the law's implementation and raising awareness of the importance of data protection. Legal liability arises from any infringement on such data that constitutes an assault on the privacy of its owners. The violator is subject to criminal penalties resulting from breaching a related legal obligation and is civilly liable for damages caused by that assault. Consequently, they are required to compensate the injured party for the resulting harm. The person whose data has been violated has the right to request that the violation cease and to seek compensation for any damages incurred.

Recommendations

The necessity of continuous awareness about the importance of legal protection for electronic personal data as an application of the right to privacy. The necessity of regularly reviewing legislation on the protection of personal data to keep pace with technological developments and rising electronic threats, ensuring the continuity of legal protection for data. The necessity of launching national awareness campaigns to educate individuals and institutions about their rights and duties to protect their data, and to inform them about the latest methods of data breaches, thereby increasing compliance and achieving digital security.

15

References

Abdel Haq, Khaled & Abdel Aal, Doaa (No Date). Cyber Crimes and Criminal Investigations, Al-Yazouri Scientific Publishing House.

Abdel Haq, Kaled & Abdel Aal, Doaa (No Date). Network Monitoring and Documentation, Al-Yazouri Scientific Publishing House.

Abdel Haq, Khalid & and Abdel Aal, Doaa (2025). Information and Network Security Protocols, Al-Yazouri Scientific Publishing House.

Abdel Sadeq, Adel (2018). Personal Data: The Struggle Over the Oil of the 21st Century, Arab Center for Research in Cyberspace.

Al-Ahwani, Hossam El-Din (2000). The Right to Respect for Private Life, The Right to Privacy: A Comparative Study, Al-Nahda Al-Arabiya Publishing House, 2nd Edition.

Al-Ashqar Jabour, Mona (2016). Cybersecurity: The Concern of the Era, Arab Center for Legal and Judicial Research, Beirut.

Al-Rasheed, Adel (2022). Big Data, Thesis Submitted to the Department of Jurisprudence at Imam Muhammad bin Saud Islamic University.

Al-Sanhouri, Abdul Razzaq (1997). Al-Wajeez in Explaining Civil Law, Part One, Theory of Obligation, Dar Al-Nahda Al-Arabiya, Cairo, 2nd edition.

Al-Shaibi, Fouad (2021). Civil Protection of Personal Data from Unlawful Processing in Light of the UAE Federal Decree-Law No. (45) of 2021 on the Protection of Personal Data, Journal of Judicial Studies, Issue 24, Year 14, 2023.

Al-Tahami, Sameh (2018). The Scope of Legal Protection of Personal Data and Tort Liability for Its Processing, Journal of Legal and Economic Research, Issue 67.

Hussein Al-Jubouri, Salah (No Date). Personality Rights and Means of Their Protection, Dar Al-Fikr Al-Jami'i, Alexandria.

Khalifa, Ihab (2021). Cyber Warfare, Al-Arabi Publishing and Distribution House.

Mira, Shelwah & Kahina, Bashiri (2020). Civil Liability for Violation of the Right to Privacy in the Digital Domain, Master's Thesis, Abdel Rahman Mira University - Algeria.

Sakkikar, Mohammed (2010). Cybercrime and How to Confront It, Al-Jumhuriya Publishing.

Salsapil, Bin Ismail (2020). Criminal Protection of Informational Privacy in Algerian and French Legislations, Journal of Judicial Ijtihad, Volume 12, Special Issue.

Zain Al-Abdiyah Saleh, Marwa (2016). International Legal Protection of Personal Data on the Internet Between International Treaty Law and National Law, Arab Studies Center, 1st edition.

Laws & Legislations

- Federal Decree-Law No. 45 of 2021 concerning the Protection of Personal Data (UAE).
- Jordanian Law No. 24 of 2023 concerning the Protection of Personal Data.