Mesopotamian journal of Big Data
Vol. **(2025)**, 2025, **pp**. 429-447
DOI: https://doi.org/10.58496/MJBD/2025/026 ISSN: 2958-6453
https://mesopotamian.press/journals/index.php/BigData

Research Article

Virtual Personalities and Smart Analytics in the Digital Environment: Legal and Applied Framework for Big Data and Financial Transaction

Hazim Akram Sallal [1], Faris Kamil Hasan Mihna [1], Lobna Abdalhusen Easa Al-Seedi [1,2], Mustafa Abdulfattah Habeeb[3], Yahya Layth Khaleel[3,*]

[1] *College of Law, Imam Jaafar Al-Sadiq University (IJSU), Baghdad, Iraq*
[2] *College of Law, University of Baghdad, Baghdad, Iraq*
[3] *College of Computer Science and Mathematics, Tikrit University, Tikrit 34001, Iraq*

ARTICLEINFO

Article History
Received 02 Sep 2025
Revised 24 Oct 2025
Accepted 04 Nov 2025
Published 09 Nov 2025

Keywords
Virtual Personalities
Digital Identity
Data Protection Law
Privacy and Ownership Rights
Digital Forensics
Transparency and Explainability

ABSTRACT

The rapid progress of artificial intelligence (AI) has altered the very nature of the digital systems that ground today's legal and financial institutions. This study is cross-discipline research that constructs an integrated framework that connects digital identity, AI-based digital wallets, and information governance across a singular legal-technological approach. It considers the consequences of AI reshaping economic exchange, digital identity management, and communication and its mediation by autonomous virtual identities that can carry out actions characteristic of observable real-world social and economic experiences. The study uses a comparison of the regulatory mechanisms in Iraq, Europe, and the US context to convey the efficiency, transparency, security while in need of mitigating regulatory concerns about ownership, privacy, liability, and intellectual property. The findings concede that while virtual identities are devoid of any independent legal status, someone related to those identities is liable. Lastly, the research concludes by recommending Egypt establish a national comprehensive legal framework for AI and big data legislation that gives consideration to protection of data, transparency of algorithmic decision making, and ethical use. Ultimately, the study promotes a hybrid legal and technical regulatory approach to focusing on human values and innovative responsibility.

1. INTRODUCTION

In recent years, the world has undergone an incredible explosion of applications of artificial intelligence (AI) and processing of big data. These technologies have moved far beyond what was previously thought to be the exclusive domain of computer processing or industrial assistance; they have moved to creative, intellectual, and social domains that were once thought to be totally human [1]. One of the most significant is the emergence of virtual personalities, which are digitally created entities utilizing AI and data modeling to imitate human appearance, voice, and behavior [2]. These virtual personalities have been employed for marketing, entertainment, education, and even political communication [3].

The synergistic working of computer driven systems, big data processing, and the expanding world of financial systems like e wallets [4] and virtual transactions [5] gives rise to many more complex and interdisciplinary questions in the field of legal, computer technological and ethical implications. This study is an investigation into the several areas of laws, technicality of laws, and data governance of digitized or virtual personalities and of AI driven digital transactions and how they are affected in regards to issues such as identity and privacy, accountability in the digital environment.

1.2 Research Idea

This research stems from the sudden proliferation of AI-generated virtual entities on social networks. To think of them as toys is an error. They are autonomous digital entities capable of influencing world public opinion, managing their own

*Corresponding author. Email: yahya@tu.edu.iq

financial portfolios and creating their own content. These phenomena lead to a reconsideration of the old legal concepts of personality and responsibility:

- Is it possible for virtual personalities to be recognized as legal entities?
- If these had personalities, who would be liable if they damaged property, committed fraudulent acts or libeled?
- How should the enormous data bases that provide the raw material for their personality be categorized from a legal perspective?

This research combines legal comparative analysis and empirical research based on machine learning. It bridges the gap between the theoretical regulation of the entities and their practical implementation.

1.3 Problem Statement

The main problem can be seen in defining the nature and legality of the personal virtual personalities and the financial systems that follow AI usage. That causes the emergence of the following important questions:

- What is the legal character for AI made digital models which act on behalf of the natural personalities or organization?
- How could be affirmatively stated the protection of a person against the stealing of his identity or his defamation or the illegal usage of the data in case it happened as appearing?
- Are the present rules satisfied by the civil and the criminal responsibility well to encounter all the above-mentioned questions or should there be written laws by the legislative power?

These questions extend the deal on to the side of the ownership of the data, the private life of the others and till where we should assume AI systems to be independent decision makers in the social or financial treatments.

1.4. The Significance and Contributions of this Study

The significance of the study emanates from its endeavor to respond to a two-pronged legislative gap in Iraq’s regulatory and legal framework concerning artificial intelligence, big data, and digital identity. The first gap is the absence of explicit and comprehensive legislation that governs the use, processing, and protection of big data and personal information stored in AI systems. The second gap is that legal provisions defining and governing virtual personalities' existence and accountability in the digital space do not exist.

In contrast to advanced economies, such as the European Union and the United States, which have developed structured (and in some cases multi-layered) legislation, such as the General Data Protection Regulation (GDPR), Digital Services Act (DSA), and even the proposed (AI Act), Iraq's frameworks continue to rely on a patchwork of antiquated legislation that does not reflect current technologies or societal realities. This has created an urgent need for a coherent legal vision that balances the need for technological innovation with the need for data protection in the Iraqi context.

The study aims to establish a comprehensive national framework, positioning artificial intelligence, big data, and digital identity together within an overarching legislative framework. In so doing, we contribute to the foundation to support the development of a constructive legal basis that does not lose sight of relevant international standards while remaining mindful of Iraq's context and socio-legal environment.

In respect to our contributions, the study provides both theoretical and practical contributions. On a theoretical basis, we contribute toward enhancing our understanding of how AI and big data can be regulated in newly devised legal frameworks that presently have not had experience with digital governance. This also demonstrates how legal analysis can meet technological practice, in the form of an analytical model that connects principles of accountability, transparency, and ethical use of AI.

On a practical level, the study provides a foundation of empirical insights and recommendations for Iraq's policymakers and policymakers that can be leveraged toward developing contemporary, mature laws around (a) artificial intelligence; (b) data protection; and (c) digital identities. The study also draws comparisons to the Iraqi situation from international legislative examples (the payer experiences), and highlights best-practice evidence that can potentially (or should) be adapted to Iraq's national context. The ultimate goal of the study is to support Iraq's journey towards becoming a digitally governed society, in which the advancement of technology and innovation is mindful and balanced with individual rights and data protection.

1.7 Structure of the Study

The research is organized into five chapters. Chapter One includes the general premise of the research including the background, significance, and the goals. Chapter Two addresses the regulatory nature of virtual personalities by wordsmithing their conceptual and legal bases. Chapter Three discusses big data and the protection of digital identity, in terms of ownership, privacy, and regulation. Chapter Four discusses AI information contained in digital wallet transactions to explain the technical models and experimental results. Chapter Five advances both the legal and technical aspects of the research to propose a governance model contextually relevant to Iraq.

2. CONCEPT AND TECHNICAL FOUNDATIONS OF VIRTUAL PERSONALITIES

Virtual personalities are defined as digitally created entities (visual, auditory, or hybrid) generated or simulated by humans or AI systems in a manner that creates the illusion of autonomous, human-like existence. These entities interact across digital and social media platforms through advanced technologies such as computer-generated imagery (CGI), animation, and generative AI models (e.g., face-swap, voice cloning, text-to-video).

They rely heavily on large-scale data processing, combining human features, behaviors, and preferences collected from real individuals or synthesized algorithmically [6].

Since, realistically, users frequently believe these embodiments to be real, self-existing entities that communicate, express emotion and influence, these virtual personalities subsume great power in industry as instruments to be exploited for marketing, digital entertainment and even political and cultural influence His manifestly weak simulation of human nature nevertheless makes its challenge to contemporary ethical attitudes vividly interesting and replete with opportunity for speculation as to the ultimate value of an altered and more exact (or real) world.

2.1 Legal Foundations of Virtual Personality

The advent of virtual personalities calls into question the classical notion of personality from a juridical point of view by which it is traditionally limited to real persons and collective bodies (corporations, associations, etc.).

Being really the key question whether a virtual personality, identifiable and able to act through AI, can possess rights or juridical duties.

In the various legal systems of the world is that personality derives from real human or institutional existence and not from autonomous algorithmic capacity.

A virtual personality therefore does not have acquired an autonomous juridical status, and consequently the liability and property rights rest with the person or company which operates or finances the same [7].

It is to be noted that the Courts and regulating bodies therefore make a distinction between:

- An “account under user control”, where the liability rests with the human directories.
- A “corporate Digital Product”, where a liability would rest on the company operating the virtual personality as an instrument, marketing or commercial.

The above distinction is useful for discovering the quality of the various action claims arising from the criminal acts committed through virtual personalities whether civil, criminal or administrative.

2.2 Applicability of General Legal Principles

2.2.1 Capacity and Accountability

Legal capacity is dependent on possession and control. When a virtual personality uses some identifiable human characteristic e.g. voice, image, or modality of behavior, it may infringe personal rights which include:

• The right to image.

• The right to privacy.

• The right to reputation and dignity.

With respect to the process of any identifiable personal or biometric data used for the purposes of AI modelling, the EU (GDPR) strictly controls and regulates the use of such data. The European Data Protection Board (EDPB) has ruled that any use of personal data for training AI is still regulated because it is subject to the principles of the GDPR i.e. the lawfulness, transparency and purpose limitation, particularly given that the resulting output is synthetic in nature [8].

It follows therefore that, even if human data has been converted into digital form or synthetic form, the protection of such human data is still in place because the result remains susceptible of identification tracing back to a person [9].

In Iraqi Law Article (17) of the 2005 Constitution guarantees the right of personal privacy and Article (46) restricts the limitations on fundamental rights save by law. While Iraq does not have any comprehensive data protection statute in place similar to that of the GDPR, the Civil Code No. 40 of 1951 while dealing with tort liability (Articles 202 onwards) does give indirect protection through tort liability as a means of compensation for the infringement of personal rights such as image and reputation or dignity, which rights are now being assailed if due to an infringement of personal privacy the virtual personality is generated.

Consequently, while Iraq accepts and acknowledges the basic principles of data privacy, it does not have a comprehensive legal framework in place to deal with the effect of AI generated content or simulation of virtual identity.

2.2.2 Ownership and Intellectual Property

The key question is who owns the creative product of a virtual personality or artificial intelligence?

• The Berne Convention (1886) and TRIPS Agreement, recognize only human authorship of the copyright in literary and artistic works [10], [11],[12].

• The U.S. Copyright Office (2023) , has expressly stated that works produced wholly by AI are not registrable, unless they show “a sufficient degree of human creativity” [13].

• In the EU, Directives 2001/29/EC indicates that the legal protection is operative where the work presents “the author’s own intellectual creation” [14].

In Iraq, both the Copyright Protection Law No. 3 of 1971 (as amended) and Civil Code No. 40 of 1951 restrict legal personality and authorship to natural and/or legal persons enabled only. Therefore, works produced by AI without human involvement are outside the definition of works in law being eligible for protection.

This comparative analysis would lead to the conclusion that virtual personalities themselves are unable to control and/or own, intellectual property, since they are but extensions of their human or corporate creators.

2.3 AI, Big Data, and Their Legal Implications

AI refers to the academic and applied field of science and technology that focuses on establishing engineered systems to replace human intelligence and respond successfully to tasks related to human interactions [15] reasoning, perception [16], learning [17], and decision-making [18]. AI extends machine functionality to retrieve and analyze information, detect underlying relationships, and present predictions or actions, with minimal human involvement or mediation [19], [20]. AI may leverage two useful expectations, including a broad spectrum of AI subcategories or present options that were not popular in the past, such as machine learning [21], deep learning [22], natural language processing [23], computer vision [24], expert systems [25], and more.

AI has been directly applied to practical applications in many research domains to facilitate improved analytical and decision-making capabilities. For example, decision-making processes using AI methods are used to select and rank complex decision alternatives [26], [27]; specifically, multi-criteria decision-making (MCDM) methods [28]. AI has been used with predictive modeling [29], classification of consumer behaviors, real-time fraud detection, health risk analysis , and optimized resource-allocation methods [30]. AI engines consider many variables at once, each time updating the priorities in their computations, which is generically much harder to do using a statistical approach rather than AI tools. Each of these examples shows how reliable AI can be as an analytical partner, supporting ethical evidence-based decision-making in any number of sectors.

The efficacy of any AI solution, however, relies first on the quality of the data that is available [31]–[33]. From this, it is clearly possible to reach the definition of Big Data. Big Data describes not only large but also continually expanding data sets generated from human digital activities, online purchased behavior, sensor data, and assembled databases of web-connected devices and services [34]. Big Data is described based on three or more main characteristics: volume refers to the huge amount of data; velocity refers to the speed of generation and processing of the data; and variety refers to the different formats of data. Of course, two additional features that are sometimes added to the conversation about Big Data and its implications are: veracity concerning trustworthy data; and values concerning the capacity for actionable data [35], [36].

Big Data is the very basis for which AI intelligence models are trained and validated [37]. The ability of AI to identify patterns, forecast, and make suggestions from Big Data is an improvement over human cognitive capacities across any diverse area [38], including finance, health care and education, industrial production, and even agriculture. Yet, the dependency on Big Data to train and validate AI models, creates ethical and legal complications [34]. When Big Data includes personal information, financial information, or behavioral information for AI learning, the extremely sensitive and complex issues of ownership, privacy, accountability, and fairness become unavoidable when AI systems developed based on Big Data or informed by Big Data are deployed in communities.

Nonetheless, the combined interaction between AI and Big Data creates both possibilities and risks [39]. On the one hand, AI and Big Data creates both unprecedented opportunity for efficiency, effectiveness, and innovation. On the other hand, AI and Big Data creates legal confusion because of possible violations of data protection, consent, and intellectual property laws, as well as because of lack of accountability by algorithms [40]. The automated nature of AI decision- making brings into question the boundary between human and machine accountability when errors, biases or harm occur [41], [42]. Likewise, the continuous collection and analysis of data related to individuals creates the risk of violating privacy, and if deployed without regulations, sensitive and private data could be misused even in the hands of a seemingly ethical business [43].

Therefore, the interrelationship of AI and Big Data is important for any legal system for modern times. Addressing any impact is an integrated approach, and it is vital that technology advances to keep up with ethical principles and guarantees an effective legal system. The legal system ought to strive to clarify definitions, clarify lines of accountability, and develop standards for transparency and data protection, so that the benefits of AI and Big Data will not become a risk to individual rights or undermine social trust.

2.4 The Impact of Civil and Commercial Law Principles

In the traditional civil and commercial law systems, the responsibility for the harm caused by a virtual personality be it through libel, invasions of privacy, use of identity, etc. - lies with the person or institution controlling that personality. This is done because no direct human personality may be attributed to AI systems, the doctrines of agency and vicarious liability, still being applicable where the artificial personality is concerned. But these doctrines will give rise to problems when it is considered that autonomous decision-making algorithms have been created, ones which are capable of self-learning, and also of adapting themselves, in respect of which it is impossible for human involvement to be found, so producing possible gaps, so far as accountability is concerned. The general trend of the world is to look for “algorithmic accountability”, to impose responsibilities upon those who create algorithms and the owners of the platforms upon which they are placed, to ensure that the resultant AI activity is the kind which it is lawful, and which, in the ethical sense, is desisted from. This concept is the basis of any future regulatory bodies which must of necessity be created in any legal system, including the proposed Virtual Personality and Big Data Law for Iraq.

3. The Right to Image, Identity, and Data Protection

The use of personal and biometric data (such as facial features, voice patterns and behavioral signals) for the creation or training of virtual personalities raises fundamental legal and moral issues. Present-day data protection legislation considers such data as highly sensitive and requires explicit consent or an appropriate legal basis for processing. Commercial and/or political exploitation of such virtual models, without consent, may infringe:

• the right to publicity,
• the right to image and reputation,
• the right to privacy.

In this context, big data plays a central role. It is the raw material through which human identity is reconstructed or simulated by A.I. systems. The mere aggregating, processing and reutilizing of huge datasets (often containing traces of identifiable persons), gives rise to a double-edged legal dilemma: on the one hand, innovation and creativity, on the other, intrusion, profiling and manipulation concerning identity [44].

3.1 Big Data and Legal Personality in the Virtual Environment

Big Data refers to big and complex data items produced in response to different sources such as commercial transactions, social media transactions, health and biometric record and behavioral analytics. They lead to the development of virtual personalities and they help to improve the predictive capability of AI systems. The legal problem consists of:

1. Who owns the data, the person from whom it is derived or the gathering and feeding person of the data.
2. How far can it be used including especially its use in the area of profiling and manipulation of individuals.

These factors are important since under international standards such as GDPR dealing with identifiable personal data will only be able to be processed in a form in accordance with the following principles lawfulness, transparency and proportionality, using specified legal bases such as express consent or legitimate interest [45]. In the case of Iraq there is no specific law protecting ‘Big Data’ use, but under the provisions of the Civil Code (Articles 202 et seq) and Article 17 of the Constitution of Iraq (2005), some indirect protection exists to individuals in that they may sue for damages for the misuse of their personal data which would cause moral or material injury. This provides a framework, notwithstanding that it is fractured, in which the creation of a national law or statute providing a national day framework could be developed compliant with international standards.

3.2 Legal Challenges of Big Data in Constructing Virtual Personalities

3.2.1 Ownership and Responsibility in Data Exploitation

Big data is the basis for the construction of virtual identity and its value does not arise solely through the data operated on but through dealing with and reapplying it to produce individual self-sufficient digital equivalents. A major question arises here: who is liable in law when the type of use made of data in the process of building a virtual personality, leads to some detriment, such as identity fraud or damage to image and reputation? [46] Traditionally, civil law does not recognize “ownership” of data as a clearly defined legal right but rather the data belonging either to the owner of the data base, or to the agency which controls it. But now, with big data and AI the relation becomes more complex, the data becoming a productive asset by being reused and reinterpreted by algorithms which can work or operate away from the supervision of direct manual operation. This having been used in a way which can cause injury to persons through defamation of character, invasion of privacy, or even exploitation of individual attributes, leads to the question of liability: is it

1- the technical system?
2- the corporate entity making profits from the operation of its processing?
3- or the individual who directed or sanctioned this operation? When there is no explicit legislation there is no clear position understanding…etc.”

This leads to the necessity of having special legal provisions regulating the relations between data subjects, data controllers and AI operators to fulfil the necessity of the balance created in allowing innovation tempered with safeguarding to some extent the rights of individuals.

3.2.2 Privacy and Identity Protection in the Era of Big Data

The use of large data sets to create or enhance virtual personalities presents very serious problems related to privacy. The use of biometric or sensitive personal data in this context is considered high risk processing under the law, requiring prior consent and strong legal justification [47]. The European Union has provided a comprehensive model:

• The GDPR imposes strict obligations with respect to biometric data and disclosure and accountability obligations [48].
• The AI Act (2024) provides for rules relating to disclosure, labelling and risk classification, requiring that any AI system which generates synthetic media or deepfakes must disclose the fact clearly and the sources of data used [49].

• The DSA complements this by imposing obligations of removal of content and notification of digital platforms. The United States both lacks a federal uniformed framework of its own [50]. Data protection is sectoral and state based, governed by law such as:
• California Consumer Privacy Act (CCPA, 2018) [51].
• The Health Insurance Portability and Accountability Act (HIPAA).
• The Children's Online Privacy Protection Act (COPPA) [52].
As far as Iraq is concerned, privacy protection proceeds mainly from constitutional principles (Article 17) and along the lines of tort law provisions, and there is an absence of a regulatory authority or enforcement mechanism.
This leaves users open to the dangers of the possible misuse of personal or biometric data and therefore need for a comprehensive Big Data and Digital Identity Protection Law in urgent prospect.

3.3 Comparative Legal Overview

3.3.1 Iraq

Currently in Iraq there is no unified legal framework for the regulation of big data and virtual personalities whose protection is dispersed in:

- • Article (17) of the 2005 Constitution (right to privacy).
- • Among the provisions of the Electronic Transactions Law No. 78 of 2012
- • General liability rules enshrined in the Civil Code.

This renders it extremely difficult for the victims to enforce their legal rights when the data is used to make misleading or dangerous virtual identities. It is therefore recommended in the study to adopt a comprehensive data protection act to define the responsibilities of data collection and processing and dissemination.

3.3.2 European Union

The EU has developed the most advanced model of law, embedding three main coordinating instruments:
1. The GDPR (2016/679) – which regulates lawful processing and user rights concerning data of the data subject.
2. The AI Act (2024) – which establishes the transparency and accountability of requirements for AI systems.
3. The DSA 2022/2065 which obliges the responsibility of digital platform users with respect to the AI-driven and data-rich content.
This three-dimensional framework regulates the lawful use of data, guarantees transparency in the algorithmic generation thereof and opposes the user to any manipulation, in particular in respect to cases concerning deep-fakes and synthetic identities.

3.3.3 United States

The U.S. framework is open fragmentation and decentralization. Federal and state regulations coexist that regulate specific fields or regions:

- CCPA (California Consumer Privacy Act) allows individuals the right to information access and deletion of personal identification information.
- HIPAA (Health Insurance Portability and Accountability Act) allows control over medical information. COPPA (Children's Online Privacy Protection Act) protects children.
- Recent legislative efforts like the NO FAKES Act and DEEPFAKES Accountability Act are designed to control over digital identity theft and computer-generated disinformation.

The U.S. Copyright Office (2023) states that "works produced by AI and computer programs whose production does not require human beings are not protected." Thus, more importance must be put on human authorship [13], [53].
The debate concerning Section 230 of the Communications Decency Act is ongoing. In the news has been the question of platform liability for AI-enhanced content [54].

3.4 The Role of Digital Forensics and Accountability

Legal safeguards cannot be separated from the ability to trace and verify the origin of data [55]. Therefore, modern regulatory tendencies favor the use of:
• Generation logs and provenance records.
• Watermarking and labeling of synthetic materials.
• Fast takedown and notice systems for cases of misuse.
These mechanisms assure that individuals and authorities can ascertain the origin of the data used to create virtual personalities enhancing the legal enforceability and accountability.

3.5 Digital Wallets in the AI and Virtual Identity Environment

At present, information technologies that compute the transactions to transfer or accept funds employ much of the consumer's personal and biometric data and through AI-enhanced cyber algorithms determine such things as:

• User preferences.

• Deviation or fraudulent activities.

• Decision-making with respect to transactions through behavioral analytics.

In some instances, the wallets of which he had purchased the assets are integrated with his virtual assistant or avatar who can through voice command, facial recognition or gesture command purchase, make transfer of funds or subscribe to services. This wholly removes the individual with respect to his traditional concept of "self" and introduces new concepts of consent, liability and thus identity wherein autonomous digital entities conduct transactions in any of its variants through the virtual assistants.

4. PROPOSED METHODOLOGY

The quick growth of financial technology has changed how people and organizations conduct cash transactions drastically. To the maximum extent, digital wallets, which utilize AI instruments and systems, data analysis of abilities as systems, and encryption, represent one of the prime innovations digitally and do not require cash transactions [56]. Thus, in the sphere of AI and virtual environments, digital wallets are not merely means of cash, but they also contributed substantially to the fabrication of digital environments necessary for electronic business and automated systems, virtual assistants, or even fictitious personalities possessing the capacity of manual income adaptation right in itself. In this chapter we will analyze how the digital execution as per AI-based analysis systems applies to digital wallets and their reactions, behavior, and spending. We shall discuss issues associated with data protection in the use of wallets as transactions in algorithms, algorithmic presentation value, and legal responsibility.

4.1 Dataset Description and Preparation

In order to illustrate the functionalities of AI that improve security and efficiency in this digital financial ecosystem, a large data set of digital wallet transactions was analyzed via machine learning (ML) and deep learning (DL) models.

• Source: The data set was obtained from a public repository on Kaggle [57].

• Content: This consists of thousands of transaction records, each with variables such as transaction amount, timestamp, merchant stripe, payment channel, type of device, user location, account balance history, and status of transaction classification (legitimate or fraudulent).

Engineered features which were created to improve model performance included transaction frequency, daily spending limit, time intervals of payments etc. All data were cleaned, normalized, pseudonymized in order to prevent identification of individuals, and were consistent with GDPR-type principles for privacy and data minimization.

4.2 Exploratory Data Analysis (EDA)

The EDA phase provided a statistical and visual understanding of the transaction behavior. (Histograms or boxplots presented spending distributions and heatmaps showed correlations). Figure 1 provides a horizontal bar plot showing the counts of product categories for the transaction category for the digital wallet. Each bar represents a category, with the longer bars indicating greater counts. The counts indicate that the categories "Education Fee" and the category "Streaming Service" are the most frequently used categories suggesting that they are frequently used while such categories as "Bus Ticket" and "Internet Bill" show smaller frequency of transactions. This gives insight into spending behavior regarding different categories in the product categories for the digital wallet transactions.

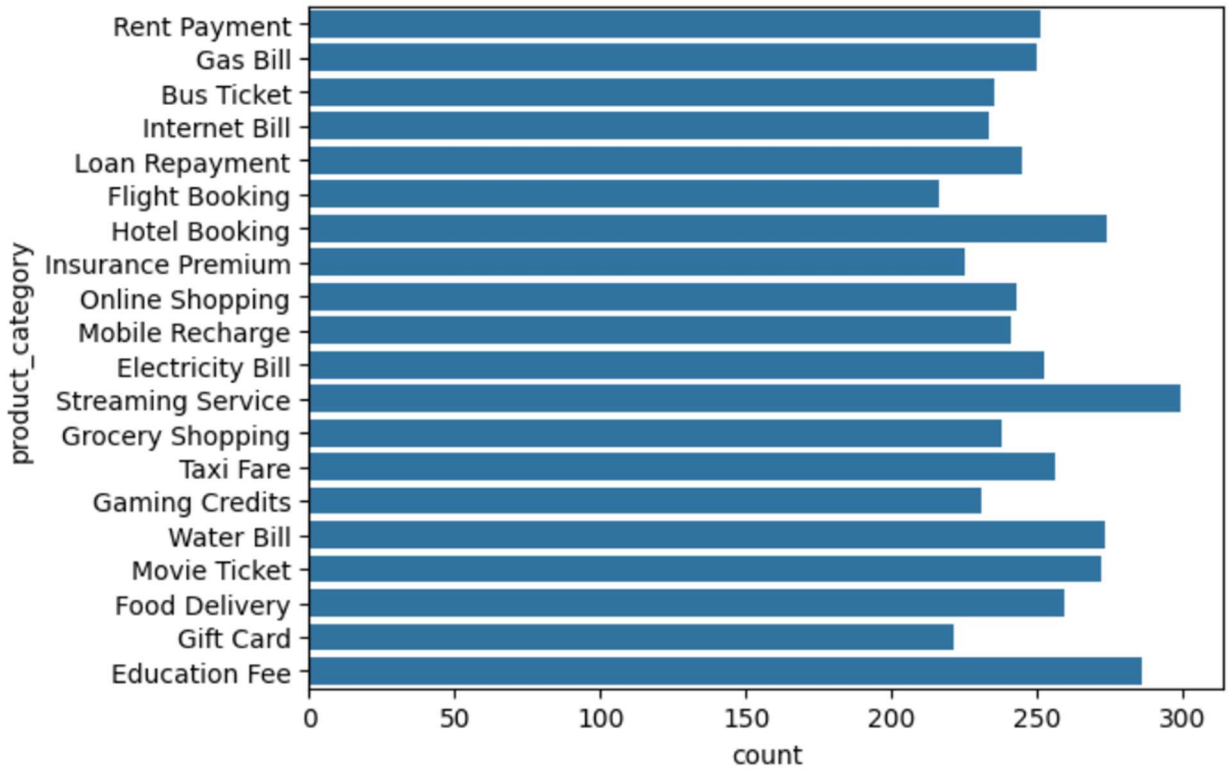

Fig. 1. The counts of various product categories in digital wallet transactions

Transactions are categorized into three status types in Figure 2. The three status types are defined as "Successful," "Failed," and "Pending." The number of operations indicated for "Successful transactions" far outweighs the number indicated in the "Failed" transactions and "Pending" transactions categories. The data presented clearly indicates that in the totality of transactions, the "Successful status" is markedly true for the great majority of transactions. The count of "Failed transactions" and "Pending" transactions categories convey a much lower count, indicating very few failures and even fewer pending transactions. The effect of this representation is complete reliability and workable efficiency of the digital wallet system represented.

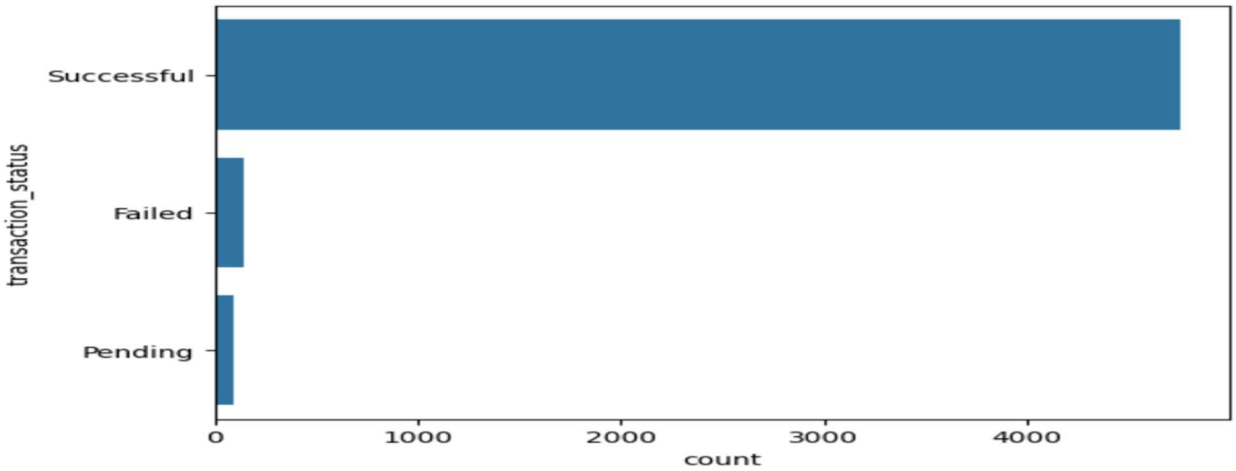

Fig. 2. The counts of different transaction statuses within digital wallet transactions

The various modes of payment used in the wallet transactions, as per the counts of transactions of each mode of payment, are a visualized form in the Figure 3. The modes of payments being "Bank Transfer", "credit card", "Wallet Balance", "UPI"

and "Debit card". The lengths of each bar representing the counts of transactions in that mode of payment which show that the modes of payments "Debit card" and "Bank Transfer" give the maximum in number of counts. These modes of payments are thus popular modes of payments. The rest of the modes of payments have also a significant number of transactions but count of these is a bit lesser in number. The visual gives the ideology of users towards the various modes of payments in the digital wallet system.

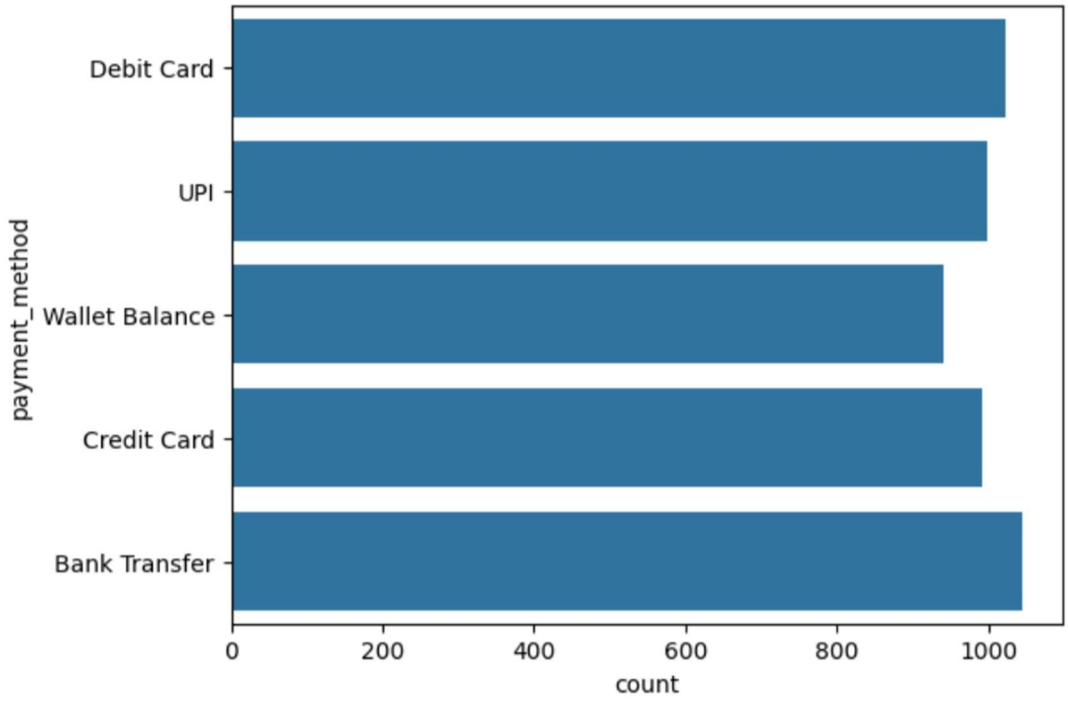

Fig. 3. *The counts of various payment methods used in digital wallet transactions*

The number of digital wallets transacted by each of the various types of devices is given in figure 4. There are three types into which the devices of use are divided: namely, "Android," "iOS," and "Web." The "Android" devices appear to considerably exceed in the amount of transaction numbers to any other class, showing that this is the most popular platform for users. The next class of devices "iOS" occupies a medium amount, while the number of transactions of devices "Web" is the larger class. This gives some idea of the class of devices preferred by users for use in obtaining service through digital wallets. There is a definite preference shown for mobile devices as opposed to web devices.

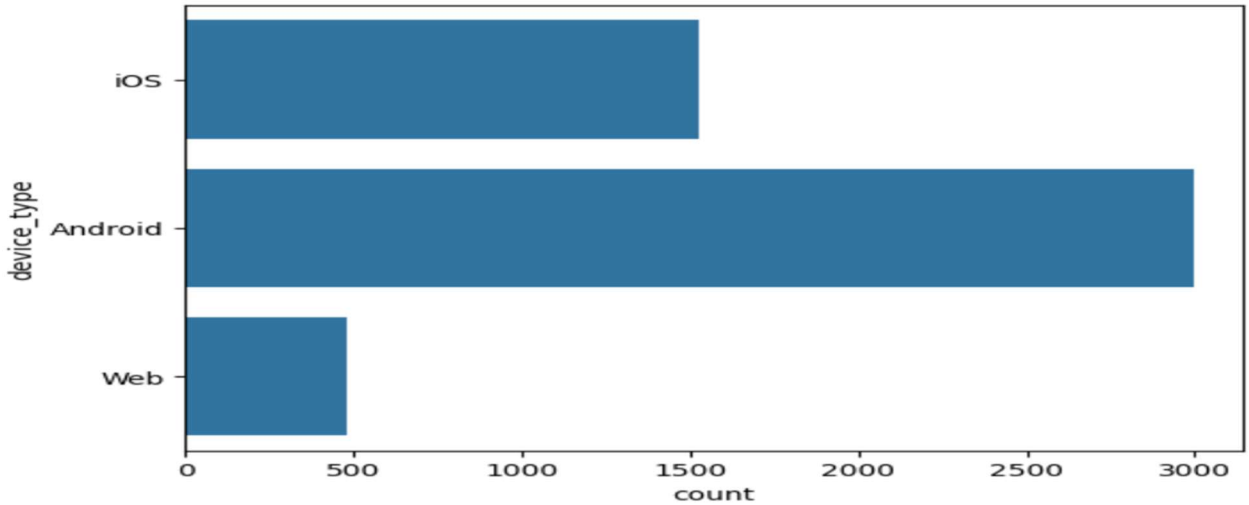

Fig. 4. The counts of different device types used for digital wallet transactions

This implies that customers dealing with digital wallets have a more favorable attitude to transactions that are more convenient, repetitive and service oriented, with a sounder payment infrastructure. Accordingly, the EDA stage has built a good foundation for the machine and deep learning analytical techniques which follow, in that the resultant training of any model should be undertaken with all the clear behavioral and transactional patterns which have been extracted from the dataset.

4.3 Machine Learning and Deep Learning Models

4.3.1 Preprocessing and Feature Engineering

To deal with the numerical and categorical variables separately, the pre-processing pipeline made use of a Column-Transformer:

* Numerical variables were normalized through StandardScaler (that is, transaction amount, cashback, fees and transaction length).

* Categorical variables which included payment method, merchant category, device type, region were encoded through OneHotEncoder.

The dataset was split into 80% training and 20% testing subsets.

4.3.2 Machine Learning Model: Random Forest (RF)

The Random Forest Classifier (RFC) [58] was implemented with 100 estimators. Its ensemble structure averages multiple decision trees to minimize overfitting and handle mixed data efficiently. The RF model achieved:

TABLE 1. RESULTS OF ML AND DL MODELS

Model	Accuracy	Precision	Recall	F1-Score
RF Classifier	0.96	0.96	1.00	0.98
ANN	0.95	0.96	0.99	0.98

This indicates exceptional performance in identifying legitimate versus anomalous transactions, though sensitivity to class imbalance remained a minor limitation.

4.3.3 Deep Learning Model: Artificial Neural Network (ANN)

To model nonlinear relationships, the ANN (artificial neural networks) [59] model is created and implemented using the TensorFlow Keras API.

Architecture consisted of:

- Input layer matching the preprocessed features.
- Two layers of the hidden layer (128 and 64 neurons with ReLU activation functions).
- Dropout layers with a dropout rate of 0.3 to prevent the occurrence of overfitting.
- Output layer with a softmax activation function for multi-class classification of the results.
- Optimizer: Adam, Loss function: Sparse Categorical Cross-Entropy, Epochs: 50, Batch size: 32.

Results:

- ✓ Accuracy: 95%
- ✓ Precision: 96%
- ✓ Recall: 99%
- ✓ F1-score: 98%

The ANN model showed balanced good performance in all transaction categories without the model losing its effectiveness in capturing the behavioral subtleties gained by the RF (random forest) model.

4.4 Comparative Results and Interpretation

Random Forest and ANN models demonstrated a high degree of accuracy in predicting unknown instances, which validates the effectiveness of AI in the areas of fraud detection, transaction classification, and behavioral analytics. The Random Forest model had superior accuracy at dealing with structured data, while the ANN model was able sufficiently to express the non-literal and dynamic nature of the relationships displayed between the various features of transactions, indicating its ability to adapt to real-world financial behavior (see Table 2).

TABLE 2. COMPARATIVE RESULTS AND INTERPRETATION

Model	Accuracy	Precision	Recall	F1-Score
Random Forest	0.96	0.96	1.00	0.98
ANN (Deep Learning)	0.95	0.96	0.99	0.98

4.5 Legal and Ethical Implications

The increase in transparency for financial operations and prevention of fraud through AI also creates the need for new regulation:

1. Data Protection: AI financial transaction monitoring requires constant access to sensitive financial and biometric data. Thus, sovereignty of that data and its protection are involved.

2. Algorithmic Responsibility: The decisions made by artificial financial systems (for example, refusal to make a financial transaction) should be explainable under Art. 22 of the GDPR and similar due-process principles.

3. AI Liability: If a virtual personality or an AI agent transacts on its own, the big issue is who is liable: the system operator, the designer of the automated system or the controller of the data?

In Iraq, the Electronic Business Transactions Law N. 78 of 2012 provides a partial basis for the regulation of electronic payments but is wholly lacking in provisions dealing with AI automation, biometric identification verification or data interoperability.

Future legislative efforts should deal with AI and financial data governance in an integrated way in one model of regulation. This can best be done under a proposed regulation dealing with “Virtual Personalities and Big Data”.

4.6 Discussion: The Role of AI in Regulatory Enablement

It is important not only to regard AI as a technical enabler but also as regulatory tool to foster transparency, accountability and consumer protection in relation to digital finance. AI systems can:

- Provide for the detection of money laundering and fraudulent activity by means of anomaly detection.
- Assist in the compliance of Know Your Customer (KYC) and Anti-Money Laundering (AML) requirements.
- Provide audit trails resulting in the enhancement of oversight of financial authorities.

However, the regulatory functions of AI have to be subject to the obligations of:

- Transparency (algorithm explainability),
- Minimization of data,
- Proportionality in the utilization of biometrics and personal identifiers.

It is thus important to achieve a balance between innovation and regulation in order to enable trustworthy AI to be engaged in the developing digital economy of Iraq.

5. RESULTS

The integration of artificial intelligence, big data analytics and digital financial ecosystems has created huge innovation opportunities on the one hand and new regulatory and ethical challenges on the other. This chapter aims to synthesize the

results indicated in the present chapters through a comprehensive analytical framework that connects technical efficiency with legal liability, making the use of AI in virtual and financial environments transparent, responsible and rights-oriented.

5.1 The Role of AI in Enhancing Financial Transparency and Governance

AI provides a large opportunity for financial oversight and regulatory compliance. Through enhanced analytics, it is possible to:

- Identify patterns of money laundering, terrorist financing and fraudulent activity in real time.

- Enhance Know Your Customer (KYC) and Anti-Money Laundering (AML) processes through continuous monitoring.

- Automate reporting and audit systems to boost the efficiency of regulatory oversight.

However, this incorporation also increases risks regarding the invasiveness of the system, algorithmic bias and centralization of data. Therefore, the efforts of AI to enhance financial governance must be based on a human-centered legal system that ensures principles including fairness, explainability and proportionality.

5.2 Algorithmic Accountability and Legal Responsibility

As these autonomous decision-making systems increasingly employ A.I. technologies, especially in economic and identity-affected decision systems, questions of accountability inevitably emerge. Traditional liability doctrines that speak to human actors often are improper vehicles for the apportionment of responsibility for the mistakes or harms caused by learning algorithms. To close this gap, legal scholars espouse the doctrine of algorithmic accountability which requires that:

1. The developer or designer provides accountability, explaining transparency, safety, and ethicality in the architecture of the system.

2. The operator or platform is responsible for its continuing supervision and risk management of the decision-making A.I. elements.

3. The government or regulatory authority creates a clear routine of auditing processes for the algorithmic systems concerned.

In this tripartite accountability, no humanly effected decision rendered by A.I. decision-making e.g. economic or characteristically behavioral can lie outside the properly treated area of human supervision nor of human accountability.

5.3 Virtual Personalities as Financial Actors

As automated digital agents and AI influencers become commonplace, virtual personages are now being used for economic purposes, such as entering into contracts, receiving consideration or payment, or administering digital assets. When linked to digital wallets, these entities can affect transactions autonomously, invest in virtual goods, or interact with consumers through marketing campaigns. The emergence of these autonomous personalities brings with it an assault on the established view of legal capacity. Since virtual personages lack stand-alone personality, it is the natural or juristic person controlling the algorithm who will be responsible for acts done by the system. The obligations of the legislator are to clarify:

- The extent of vicarious liability for act performed by ways and means of algorithms.

- The disclosure it expects to be made as to who it is users are interacting when they effect transactions with an ai personality.

- The data governance obligation on personages applying those systems.

These obligations must be made a part of national law so as to rapidly halt the misuse of these vehicles for fraud, identity theft or deception in commerce.

5.4 Toward a National Legal Framework for AI and Big Data Governance in Iraq

Iraq is presently ruled by disparate statutory provisions which govern only partially the area of electronic transactions and privacy protection. In order to bring itself in line with world developments there should be instituted a complete law

touching on AI and big data possibly named the Virtual Personalities and Big Data law. The laws would be based on the following components:

- Transparency & Disclosure:
  - Labeling of AI text etc. generated material and virtual images must be required.
  - Publicly announcing sources and methods of generative models.
- Data Privacy & Protection:
  - Extend privacy protection to biometric and physical data.
  - Establish an independent National Data Protection Authority with investigative and enforcement powers.
- Civil and Criminal Liability:
  - Liability must be provided which attaches in the case of damage caused by autonomous systems.
  - Sanctions imposed for use of data without permission, identity theft and slander by genocidal means.
- Technical Standards & Forensic Traceability:
  - Requirements for data and tracking and watermarking and logs showing how it was generated so investigations into it can be conducted.
  - Support for the auditing of AI by effective public and private sectors.
- International Co-Operation:
  - Data protection measures in Iraq must be consistent with types of matters dealt with in GDPR, AI Act and Digital Services Act in order that data flows are possible across borders at security levels acceptable.

A comprehensive structure such as this will enable that Iraq establishes the law needed to protect newly developed innovations in digital finance and the rights of citizens in the field of digital rights as a unified legal and technological ecosystem.

5.5 Ethical Considerations and Human-Centered AI

The application of AI in financial and social systems must take account of ethical values. A human-centered framework for AI must ensure that:

• Algorithms are directed toward human good, not toward replacing the judgment of human beings.

• The use of data declares an allegiance to the values of necessity, consent and purpose limitation.

• AI systems receive audits for bias and assessments for impact to avert discrimination.

In this context ethics accompany the law, orienting the moral responsibilities of developers, users and lawmakers toward a sustainable and social good effect of AI application.

5.6 Synthesis of Legal and Technical Perspectives

The interdisciplinary nature of this research highlights that effective governance of the AI sector and big data requires mutual reinforcement between the various legal norms and the different types of technological safeguards. While the law lays down the boundaries and accountability, technology offers the means of securing compliance with the law by way of encryption, traceability and the explainability of AI.

Table 1 illustrates the complementary nature and functionality of these various dimensions of compliance. Legal liability applies to systems of audit for AI, permitting traceable decision pathways; data privacy achieved by encryption and pseudonymization; regulatory transparency by explainable AI systems; enforcement mechanisms by automated fraud detection; and public oversight through AI generated analytics dashboards.

TABLE 3. THE COMPLEMENTARY NATURE AND FUNCTIONALITY OF A VARIOUS DIMENSIONS

Legal Dimension	Technical Dimension	Integration Outcome
Legal liability and accountability	AI auditing and logging systems	Ensures traceable decision-making
Data privacy and protection	Data encryption and pseudonymization	Preserves confidentiality
Regulatory transparency	Algorithmic explainability	Promotes trust and fairness
Civil & criminal enforcement	Automated fraud detection	Enhances legal compliance
Public oversight	AI-driven analytics dashboards	Enables real-time supervision

Ultimately, it is this ensuring that the development of AI is consistent for the major legal values, turning technology as a vehicle for promoting justice, fairness and accountability rather than an uncertain or dangerous phenomenon.

6. CONCLUSION AND RECOMMENDATIONS

6.1 Conclusion

This paper examined the intricate relationship among artificial intelligence, big data, electronic wallets, and virtual personalities and how these technologies interact in relation to legal relations and social activities in the digital realm. It illustrated how innovation and regulation need to develop hand in hand based on a mixture of comparative legal studies and empirical studies of AI if technology is to be used for its benefits rather than for its harms. The study's important findings can be summarized as follows:

1. virtual personalities, do not have legal personality as separate entities, they are merely extensions of their human or corporate developers and actions committed by or with virtual personalities are locus standee of the responsible human or corporate individual
2. big data is the structural basis for virtual and financial ecosystems but it has many challenges associated with privacy and ownership rights, as individuals can be manipulated and exploited through their characterized and mediated identities, thus legal rules on the ownership of the data will be imperative.
3. AI analysis of electronic wallet transactions demonstrated just how effective neat AI protocols can be at augmenting the security, dependability and efficacy of digital financial systems, yet such systems must also be regulated by law in the interests of transparency, equity , and explainability.
4. Iraq's present law provides some limited protections because of existing legal regimes in the Constitution, the Civil Code, and the Electronic Transactions Act, but are ad hoc and inadequate to deal with the regulation, biometric verification, and exploitation of big data within the warp and woof of AI advances.
5. The EU provides the most comprehensive model of a regulatory system for big data and AI through the General Data Protection Regulation, the AI Act, and the Digital Services Act, while the US has a sectoral and fragmented approach. The best from either system may be suggested for an appropriate Iraqi model that balances innovation with individual protection.
6. Digital and regulatory change need to embrace both legal and technological disciplines to achieve a sustainable digital transformation, with the legal norm to deter and hold individuals accountable, and the technological systems enforce compliance through, encryption, traceability, and algorithmic transparency.

Ultimately this paper demonstrated that neither legal nor technological was sufficient, and must draw together to form a hybrid regime with human dignity, privacy and justice at the very heart of technological advancement.

6.2 Recommendations

On the basis of its comparative analysis and empirical findings this study develops a proposed series of integrated recommendations and guidelines for the advancement of legislation and implementation of policy measures in Iraq and similar emerging contexts. The first priority should be the enactment of a comprehensive national law on AI and big data, which would, in its provisions, specify uniform standards for the collection, processing, and use of data throughout the

various sectors, whilst at the same time being in complete harmony with the framework of international norms set down in legislation such as the GDPR and the European Union's AI Act. Clarity of provision regarding the outputs of AI, virtual identities, and digital financial ecosystems must be given, so that accountability and transparency can be assured in the forthcoming digital environment.

A major consideration will be the establishment of a National Data Protection Authority, which would operate wholly independently and be empowered to audit and monitor adherence to the data protection laws and regulations, conduct regular inspections, and impose sanctions in case of abuse of personal or biometric information. This Authority, whilst enforcing the provisions laid down, should also be made responsible for fostering a culture of data ethics and algorithmic fairness and user-awareness. In this manner technological development can be assured of remaining compatible with principles of human rights.

Transparency and traceability will be important tenets of responsible AI governance. Labeling of AI-generated products, such as the virtual identities, synthetic media, and automated advertisements, should be made compulsory, in order to avoid deception and impersonation in the digital environment. Furthermore, a sound framework for algorithmic accountability should be developed, whereby developers, operators, and digital platforms will be responsible for any harm which may be done by AI systems. These responsibilities should in particular include statutory duties of explainability, bias assessment, and human decision making on all issues relating to fairness and trust on the part of the public.

Equally important is cross-sector cooperation in promoting and supporting a sustainable AI ecosystem. Universities, research facilities, and government institutions should work closely together to develop a knowledge-based environment, in support of innovation-based regulation and technological advancement. In the interests of continuing trust in the legal environment provided, integrated into AI requirements must also be the development of digital forensics, requiring that logs of creation as to generative protocols and traceability be kept (by all developers) as well as that means of recordation as to e.g. provenance, and watermarking for evidential and traceable purposes in case of dispute, are put in place.

The study also promotes the means by which ethical AI-developing strategies can be advanced, as well as building trust through public information campaigns, and educational guidelines which will set out vibrant and human/individual-centered standards of development, safeguarding privacy, and providing access to the technological benefits to be derived. These should enable the public to become aware of their digital rights as well as of the ways in which those rights are advanced/protected. International agency/mutuality is also important: Iraq should engage seriously in regional and global initiatives as regards matters of cybersecurity, digital governance and AI ethics, whilst taking exemplary lessons from other nations, which enjoy far more developed data protection frameworks. Overall, therefore, it becomes important to devise a holistic framework, which meets the criteria of transparent, accountable, and ethically-structured AI governance.

.

Conflicts of Interest

The authors declare no conflicts of interest.

Funding

This research received no external funding.

REFERENCES

[1] Y. K. Dwivedi *et al.*, So what if ChatGPT wrote it?' Multidisciplinary perspectives on opportunities, challenges and implications of generative conversational AI for research, practice and policy," *Int. J. Inf. Manage.*, vol. 71, p. 102642, 2023, doi: 10.1016/j.ijinfomgt.2023.102642.

[2] J. Yu, A. Dickinger, K. K. F. So, and R. Egger, "Artificial intelligence-generated virtual influencer: Examining the effects of emotional display on user engagement," *J. Retail. Consum. Serv.*, vol. 76, p. 103560, Jan. 2024, doi: 10.1016/j.jretconser.2023.103560.

[3] A. Mazurkiewicz-Pizlo, "Virtual Influencers (VIs) As Marketing Communication Tools," *Eur. Res. Stud. J.*, vol. XXVIII, no. Issue 1, pp. 472–492, Feb. 2025, doi: 10.35808/ersj/3955.

[4] Ş. BABUŞCU and A. HAZAR, "Financial Technologies: Digital Payment Systems and Digital Banking. Today's Dynamics," *J. Res. Innov. Technol.*, vol. 2, no. 16, p. 162, Dec. 2023, doi: 10.57017/jorit.v2.2(4).04.

[5] S. Scarle, S. Arnab, I. Dunwell, P. Petridis, A. Protopsaltis, and S. de Freitas, "E-commerce transactions in a virtual environment: virtual transactions," *Electron. Commer. Res.*, vol. 12, no. 3, pp. 379–407, Sep. 2012, doi:

10.1007/s10660-012-9098-4.
[6] G. Liyanaarachchi, M. Mifsud, and G. Viglia, "Virtual influencers and data privacy: Introducing the multi-privacy paradox," *J. Bus. Res.*, vol. 176, p. 114584, Apr. 2024, doi: 10.1016/j.jbusres.2024.114584.
[7] J. Doomen, "The artificial intelligence entity as a legal person," *Inf. Commun. Technol. Law*, vol. 32, no. 3, pp. 277–287, Sep. 2023, doi: 10.1080/13600834.2023.2196827.
[8] A. Roosendaal, "Digital Personae and Profiles in Law: Protecting Individuals' Rights in Online Contexts," *SSRN Electron. J.*, 2013, doi: 10.2139/ssrn.2313576.
[9] "Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models," *European Data Protection Board*, 2024.
[10] W.-A. Treaties, "Berne Convention for the Protection of Literary and Artistic Works," *wipo*, 1994.
[11] "Agreement on trade-related aspects of intellectual property rights," *Bus. Guid. to World Trading Syst.*, pp. 237–255, 2000, doi: 10.18356/281a0e2d-en.
[12] "Convention Establishing the World Intellectual Property Organization," *Int. Organ. Integr. Annot. Basic Doc. Descr. Dir. Int. Organ. Arrange.*, pp. 1–8, 2023, doi: 10.1163/9789004634121_027.
[13] U.S. Office of the Federal Register National Archives and Records Administration, "Copyright Registration Guidance: Works Containing Material Generated by Artificial Intelligence," *Govinfo.Gov*, pp. 16190–16194, 2023.
[14] R. Burrell and A. Coleman, "Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society," *Copyr. Except.*, pp. 355–374, 2010, doi: 10.1017/cbo9780511666964.015.
[15] A. Jaboob, O. Durrah, and A. Chakir, "Artificial Intelligence: An Overview," in *Engineering Applications of Artificial Intelligence*, A. Chakir, J. F. Andry, A. Ullah, R. Bansal, and M. Ghazouani, Eds., Cham: Springer Nature Switzerland, 2024, pp. 3–22. doi: 10.1007/978-3-031-50300-9_1.
[16] A. Bag *et al.*, "Bio-Inspired Sensory Receptors for Artificial-Intelligence Perception," *Adv. Mater.*, vol. 37, no. 26, p. 2403150, 2025, doi: https://doi.org/10.1002/adma.202403150.
[17] A. M. Vieriu and G. Petrea, "The Impact of Artificial Intelligence (AI) on Students' Academic Development," *Educ. Sci.*, vol. 15, no. 3, 2025, doi: 10.3390/educsci15030343.
[18] Y. L. Khaleel *et al.*, "An analytical framework for baby milk products selection using decision making techniques," *Appl. Food Res.*, vol. 5, no. 2, p. 101411, 2025, doi: https://doi.org/10.1016/j.afres.2025.101411.
[19] D. E. Mathew, D. U. Ebem, A. C. Ikegwu, P. E. Ukeoma, and N. F. Dibiaezue, "Recent Emerging Techniques in Explainable Artificial Intelligence to Enhance the Interpretable and Understanding of AI Models for Human," *Neural Process. Lett.*, vol. 57, no. 1, p. 16, 2025, doi: 10.1007/s11063-025-11732-2.
[20] M. Asif and Z. Gouqing, "Innovative application of artificial intelligence in a multi-dimensional communication research analysis: a critical review," *Discov. Artif. Intell.*, vol. 4, no. 1, p. 37, 2024, doi: 10.1007/s44163-024-00134-3.
[21] H. M. Abdulfattah, K. Y. Layth, and A. A. Raheem, "Enhancing Security and Performance in Vehicular Adhoc Networks: A Machine Learning Approach to Combat Adversarial Attacks," *Mesopotamian J. Comput. Sci.*, vol. 2024, pp. 122–133, 2024, doi: 10.58496/MJCSC/2024/010.
[22] M. A. Habeeb, Y. L. Khaleel, R. D. Ismail, Z. T. Al-Qaysi, and A. F. N., "Deep Learning Approaches for Gender Classification from Facial Images," *Mesopotamian J. Big Data*, vol. 2024, pp. 185–198, 2024, doi: 10.58496/MJBD/2024/013.
[23] Supriyono, A. P. Wibawa, Suyono, and F. Kurniawan, "Advancements in natural language processing: Implications, challenges, and future directions," *Telemat. Informatics Reports*, vol. 16, p. 100173, 2024, doi: https://doi.org/10.1016/j.teler.2024.100173.
[24] X. Zhao, L. Wang, Y. Zhang, X. Han, M. Deveci, and M. Parmar, "A review of convolutional neural networks in computer vision," *Artif. Intell. Rev.*, vol. 57, no. 4, p. 99, 2024, doi: 10.1007/s10462-024-10721-6.
[25] A. Shehadeh, O. Alshboul, K. F. Al-Shboul, and O. Tatari, "An expert system for highway construction: Multi-objective optimization using enhanced particle swarm for optimal equipment management," *Expert Syst. Appl.*, vol. 249, p. 123621, 2024, doi: https://doi.org/10.1016/j.eswa.2024.123621.
[26] J. Więckowski, J. Wątróbski, and W. Sałabun, "Toward robust decision-making under multiple evaluation scenarios with a novel fuzzy ranking approach: green supplier selection study case," *Artif. Intell. Rev.*, vol. 58, no. 1, p. 3, 2024, doi: 10.1007/s10462-024-11006-8.
[27] P. Mandal, L. Mrsic, A. Kalampakas, T. Allahviranloo, and S. Samanta, "Pythagorean linguistic information-based green supplier selection using quantum-based group decision-making methodology and the MULTIMOORA approach," *Artif. Intell. Rev.*, vol. 58, no. 7, p. 199, 2025, doi: 10.1007/s10462-025-11205-x.
[28] A. Albahri *et al.*, "Evaluating date fruit varieties for health benefits using advanced fuzzy decision-making," *Expert Syst. Appl.*, vol. 281, p. 127656, 2025, doi: https://doi.org/10.1016/j.eswa.2025.127656.

[29] Y. L. Khaleel, M. A. Habeeb, and G. G. Shayea, "Integrating Image Data Fusion and ResNet Method for Accurate Fish Freshness Classification," *Iraqi J. Comput. Sci. Math.*, vol. 5, no. 4, p. 21, 2024.
[30] F. N. A. Yahya Layth Khaleel, Fadya A. Habeeb , Mustafa Abdulfattah Habeeb, "Leveraging Artificial Intelligent for Optimized Crop Production: An ANN-Based Approach," *Mesopotamian J. Comput. Sci.*, vol. 2025, pp. 1–16, 2025, doi: 10.58496/MJCSC/2025/001.
[31] W. Liang *et al.*, "Advances, challenges and opportunities in creating data for trustworthy AI," *Nat. Mach. Intell.*, vol. 4, no. 8, pp. 669–677, 2022, doi: 10.1038/s42256-022-00516-1.
[32] S. E. Whang, Y. Roh, H. Song, and J.-G. Lee, "Data collection and quality challenges in deep learning: a data-centric AI perspective," *VLDB J.*, vol. 32, no. 4, pp. 791–813, 2023, doi: 10.1007/s00778-022-00775-9.
[33] A. Aldoseri, K. N. Al-Khalifa, and A. M. Hamouda, "Re-Thinking Data Strategy and Integration for Artificial Intelligence: Concepts, Opportunities, and Challenges," *Appl. Sci.*, vol. 13, no. 12, 2023, doi: 10.3390/app13127082.
[34] K. Kaushik, A. Khan, A. Kumari, I. Sharma, and R. Dubey, "Ethical Considerations in AI-Based Cybersecurity," in *Next-Generation Cybersecurity: AI, ML, and Blockchain*, K. Kaushik and I. Sharma, Eds., Singapore: Springer Nature Singapore, 2024, pp. 437–470. doi: 10.1007/978-981-97-1249-6_19.
[35] N. Seliya, A. Abdollah Zadeh, and T. M. Khoshgoftaar, "A literature review on one-class classification and its potential applications in big data," *J. Big Data*, vol. 8, no. 1, p. 122, 2021, doi: 10.1186/s40537-021-00514-x.
[36] W.-T. Wu *et al.*, "Data mining in clinical big data: the frequently used databases, steps, and methodological models," *Mil. Med. Res.*, vol. 8, no. 1, p. 44, 2021, doi: 10.1186/s40779-021-00338-z.
[37] D. Dai and S. Boroomand, "A Review of Artificial Intelligence to Enhance the Security of Big Data Systems: State-of-Art, Methodologies, Applications, and Challenges," *Arch. Comput. Methods Eng.*, vol. 29, no. 2, pp. 1291–1309, 2022, doi: 10.1007/s11831-021-09628-0.
[38] M. A. Azer and R. Samir, "Overview of the Complex Landscape and Future Directions of Ethics in Light of Emerging Technologies," *Int. J. Adv. Comput. Sci. Appl.*, vol. 15, no. 7, pp. 1459–1481, 2024, doi: 10.14569/IJACSA.2024.01507142.
[39] J. Li, Z. Ye, and C. Zhang, "Study on the interaction between big data and artificial intelligence," *Syst. Res. Behav. Sci.*, vol. 39, no. 3, pp. 641–648, 2022, doi: https://doi.org/10.1002/sres.2878.
[40] O. Renuka, N. RadhaKrishnan, B. S. Priya, A. Jhansy, and S. Ezekiel, "Data Privacy and Protection," in *Emerging Threats and Countermeasures in Cybersecurity*, John Wiley & Sons, Ltd, 2025, pp. 433–465. doi: https://doi.org/10.1002/9781394230600.ch19.
[41] H. Cossette-Lefebvre and J. Maclure, "AI's fairness problem: understanding wrongful discrimination in the context of automated decision-making," *AI Ethics*, vol. 3, no. 4, pp. 1255–1269, 2023, doi: 10.1007/s43681-022-00233-w.
[42] A. Berber and S. Srećković, "When something goes wrong: Who is responsible for errors in ML decision-making?," *AI Soc.*, vol. 39, no. 4, pp. 1891–1903, 2024, doi: 10.1007/s00146-023-01640-1.
[43] L. L. Dhirani, N. Mukhtiar, B. S. Chowdhry, and T. Newe, "Ethical Dilemmas and Privacy Issues in Emerging Technologies: A Review," *Sensors*, vol. 23, no. 3, 2023, doi: 10.3390/s23031151.
[44] J. T. McCarthy, *The Rights of Publicity & Privacy*. 2024.
[45] L. Thomas, *Thomas On Big Data: A Practical Guide To Global Privacy Laws, 2025 ed*. LegalWorks, 2025.
[46] W. Xiao, Y. Tu, P. Wan, M. Li, and J. Ma, "Analysis of Data Ownership Rights in the Big Data Era," in *Proceedings of the 2020 4th International Symposium on Computer Science and Intelligent Control*, New York, NY, USA: ACM, Nov. 2020, pp. 1–5. doi: 10.1145/3440084.3441210.
[47] M. Fadler and C. Legner, "Data ownership revisited: clarifying data accountabilities in times of big data and analytics," *J. Bus. Anal.*, vol. 5, no. 1, pp. 123–139, Jan. 2022, doi: 10.1080/2573234X.2021.1945961.
[48] General Data Protection Regulation, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data," *Off. J. Eur. Union*, 2016.
[49] European Commission, "Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence act) and amending certain union legislative acts," *Eur. Comm.*, vol. 0106, pp. 1–108, 2021.
[50] European Parliament and The Council of the European Union, "REGULATION (EU) 2022/2065 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)," *Off. J. Eur. Union*, vol. 2022, no. October, pp. 1–102, 2022.
[51] G. Duties *et al.*, "California Consumer Privacy Act of 2018," no. April, pp. 1–63, 2024.
[52] F. T. Commission and F. T. Commission, "Children's online privacy protection rule ('coppa')," *Child. Online Priv. Prot. Act*, vol. 15, pp. 6501–6505, 1998.

[53] U. Copyright Office, “Copyright and Artificial Intelligence, Part 1 Digital Replicas Report,” 2024.
[54] Gabe Regan, “The State of Deepfake Regulations in 2025: What Businesses Need to Know,” 2025.
[55] D. J. H. B. Al-Saadi, “The Authenticity of Blockchain Contracts in Proof,” *Coll. Law Polit. Sci. - Aliraqia Univ.*, 2023.
[56] J. Nwoke, “Digital Transformation in Financial Services and FinTech: Trends, Innovations and Emerging Technologies,” *Int. J. Financ.*, vol. 9, no. 6, pp. 1–24, Sep. 2024, doi: 10.47941/ijf.2224.
[57] H. Rai, “Digital Wallet Transactions,” *Kaggle*, 2025.
[58] M. K. Yaqoob, S. F. Ali, M. Bilal, M. S. Hanif, and U. M. Al-Saggaf, “ResNet Based Deep Features and Random Forest Classifier for Diabetic Retinopathy Detection,” *Sensors*, vol. 21, no. 11, p. 3883, Jun. 2021, doi: 10.3390/s21113883.
[59] M. A. Habeeb and Y. L. Khaleel, “Enhanced Android Malware Detection through Artificial Neural Networks Technique,” *Mesopotamian Journal of CyberSecurity*, vol. 5, no. 1 SE-Articles. pp. 62–77. doi: 10.58496/MJCS/2025/005.