LEGAL PROTECTION OF DATA IN COMMERCIAL COMPANIES AGAINST ARTIFICIAL INTELLIGENCE RISKS: A COMPARATIVE STUDY BETWEEN IRAQI AND EUROPEAN UNION LAW (GDPR)

Hamid Thabat Ajab

Assistant Lecturer/ Wasit University

College of Administration and Economics, Department of Banking and Financial Sciences

Wasit, Iraq

Abstract: This study will title commercial companies' legal protections against developing risks associated with the use of AI technology for their data. This research includes a comparative analysis of current Iraqi law and the EU's General Data Protection Regulation to evaluate how well traditional and specific Iraqi laws will protect against new forms of algorithmic digital threats (such as: black box issues, trade secret leaks through reverse engineering, and data corruption) in comparison to the rigorous protections and principles set forth by the European legislature; and to compare liability and privacy laws from a comparative analytical perspective. The research reached several conclusions, the most notably is the existence of a deep legislative and structural gap in Iraqi law, which renders the general rules insufficient to establish the fault and determine the civil and criminal liability for algorithmic damages, in addition to the absence of preventative measures and specialized oversight. The study concluded with a set of recommendations, the most important of which was the need for the Iraqi legislature to draft a unified and advanced data protection law that regulates the dimensions of Artificial Intelligence (AI) and codifies the right to interpretation and human oversight. It also recommended the establishment of an independent national body for digital data governance and urged companies to voluntarily adopt self-compliance strategies.

Keywords: Data protection; Commercial companies; Artificial intelligence; European GDPR; Iraqi law; Algorithmic liability

Правовая защита данных в коммерческих компаниях от рисков, связанных с искусственным интеллектом: сравнительное исследование законодательства Ирака и Европейского союза (GDPR)

Хамид Сабат Аджаб

ассистент преподавателя, Васитский университет

Колледж управления и экономики, кафедра банковских и финансовых наук

Васит, Ирак

Аннотация. Настоящее исследование посвящено вопросам правовой защиты данных коммерческих компаний от возрастающих рисков, связанных с использованием технологий искусственного интеллекта. В работе проводится сравнительный анализ действующего законодательства Ирака и General Data Protection Regulation (GDPR) Европейского союза с целью оценки эффективности традиционных и специальных правовых норм Ирака в противодействии новым видам алгоритмических цифровых угроз, таким как проблема «чёрного ящика», утечка коммерческих тайн посредством обратного инжиниринга и повреждение данных. Кроме того, исследование рассматривает вопросы ответственности и защиты конфиденциальности с позиции сравнительно-правового анализа. В ходе исследования был сделан ряд выводов, наиболее важным из которых является наличие существенного законодательного и институционального пробела в иракском праве. Данный пробел делает общие правовые нормы недостаточными для установления вины и определения гражданско-правовой и уголовной ответственности за ущерб, причинённый алгоритмическими системами. Также выявлено отсутствие превентивных механизмов защиты и специализированного надзорного регулирования. По результатам исследования сформулирован ряд рекомендаций. Наиболее важной из них является необходимость разработки и принятия в Ираке единого современного закона о защите данных, регулирующего вопросы применения искусственного интеллекта и закрепляющего право на объяснение алгоритмических решений, а также право на человеческий контроль. Кроме того, рекомендуется создание независимого национального органа по управлению цифровыми данными и стимулирование коммерческих компаний к добровольному внедрению механизмов внутреннего комплаенса и саморегулирования.

Ключевые слова: защита данных; коммерческие компании; искусственный интеллект; GDPR Европейского союза; законодательство Ирака; алгоритмическая ответственность.

Introduction

Today, we are experiencing a digital transformation that is changing how companies operate and conduct business at all levels. This change has come about through the use of artificial intelligence (AI), which has not only allowed businesses to improve their day-to-day operations, but has also greatly increased their ability to collect and analyze data and assist with making investment decisions. At the same time, however, these same technologies present serious cybersecurity and legal issues with respect to protecting the core asset of a company — its data — and can be considered an intangible capital asset and a competitive advantage for a company, which must be legally protected from breaches, data leakage, or improper or unauthorized use of AI algorithms by third parties. Therefore, the danger of AI is its ability to rapidly process very large amounts of data using machine learning and deep learning models, resulting in possible breaches of trade secrets, breaches of customers' personal data, and breaches of intellectual property owned by companies. As the digital landscape continues to rapidly progress, both national and international legal systems are forced to revise their legal frameworks to effectively respond to the risks emerging from this transition while also ensuring that they have a level playing field for commercial innovation and ensuring protection of corporate data security.

The European Union's General Data Protection Regulation (GDPR) represents one of the toughest and broadest legal regulatory system for data privacy. GDPR has established definitive rules around how organisations must prevent the generalised usage of automated decision making and to limit the risks created out of entirely automated decision making, while also providing organisations with very specific requirements in relation to protecting the confidentiality of personal data, under the threat of significant financial penalties. Rather than establishing a modern legislative framework that correlates to the modern digital transformation of the business community; the legislature in Iraq appears to continue to abide by outdated

traditional laws (for example, the Penal Code and the Commercial Code) and modern legislative frameworks such as legislative provisions related to cyber crime and data privacy. In terms of the fit and adaptability of the laws in Iraq to effectively deal with the new generation of sophisticated risks that are not defined by a geographical boundary, Iraq's existing legal framework raises significant concern.

This study is significant because of its relevance to the changing nature of the business world, which is undergoing a digital transformation. The study provides a comparative analysis that helps to combine different countries' laws into one set of laws, as well as giving a basic perspective to benefit businesses' administrative and legal decision-makers.

In order to accomplish its objective, the study will use a comparative analysis as an analytical tool; this will involve analysing the Iraqi legislative framework's legal texts and comparing them to the European general data protection regulation's (GDPR) rules and principles. The comparison will allow for the identification of strengths and weaknesses in each regulation, which could then lead to recommendations that help create a secure and sustainable legal environment for commercial businesses in light of technological developments..

Section One: The Conceptual Framework and Emerging Risks of Artificial Intelligence on Business Data

The First Requirement: The Nature of Business Data and its Investment Importance in the Age of Artificial Intelligence

First: Defining Business Data:

In today's digital environment, data has become the lifeblood of the economy and the business world. Once simply a byproduct of business, it now serves as a strategic asset and an equal source of wealth to physical capital. Within the environment of artificial intelligence, the data used in the creation of algorithms has been greatly enhanced, due to the fact that it serves as the "food source" for algorithms, allowing them to predict future outcomes and make investment decisions. To determine how the data is protected legally, it is first necessary to

consider "business data" and then separate it by three primary classifications: (1) purely business data, (2) customer/consumer data, and (3) trade secrets. Each of these categories has different levels of legal protection and different responsibilities for protecting that data. (Al-Jubouri; 2025, 97).

1. **Company Commercial Data:** Commercial data encompasses all types of data that have been created or accumulated by an entity throughout the course of its normal activity. This can include information on a company's structure/operation, organizational data and financial data. Examples of commercial data are cash flow plans, supply chain data, performance reports, and logistics inventory..

Artificial Intelligence Perspective: The algorithm uses this data within RPA systems as well as in predictive models, which allows the organization’s senior management to make cost reductions, predict financial crises before they happen and enhance their ability to allocate resources efficiently. The data is exclusively owned by the Organization and is legally protected from commercial and intellectual property law. (Omar; 2024, 69).

2. **Customer Data:** All digital data that discloses either are identifiable as a person or provides Business with knowledge and insight about the behavior of individuals doing business with the Operational Unit includes this Digital Data. Examples of this Digital Data are names of individuals, IP addresses, purchase history, preferences, and credit and bank account information. The use of this Digital Data is generally limited to Business use, but may also have legal implications related to individual privacy..

From an AI perspective: Machine learning algorithms that use customer data are often the most valuable target of machine learning models because they use behavioral profiling to deliver personalized advertisements and help businesses predict what people want to purchase. The very nature of customer data is a hybrid between a company's property (commercial) and a private source of personally identifiable information (personal data) that complicates any attempt to develop appropriate legal standards. As such, businesses have a dual responsibility to protect

this type of data in order to avoid loss or damage as a business asset and also as a condition of compliance with privacy regulations (such as GDPR), which can carry significant penalties. (Al-Zubaidi; 2024, 224).

3. **Trade Secrets:** The most valuable and highly protected type of business information is the trade secret. Legally speaking, a trade secret is defined as the following: information about operation, product or service development, or other commercial, technical or organizational aspect that is not generally known to others involved in the same type of industry as the company developing the information; the information is valuable to the company because it is kept confidential; the company has taken reasonable steps to keep the information confidential; and the information would be damaging to the company if disclosed. Some examples of trade secrets would include proprietary software algorithms, customer lists, and chemical compositions for products.

From an Artificial Intelligence Perspective: Trade secrets face a double threat. On the one hand, they represent a "competitive advantage" that the companies seek to protect from breaches. On the other hand, the incorporation of these secrets into general generative AI models (such as feeding external algorithms with confidential software data or plans for processing) may lead to the loss of their legal confidentiality and their public disclosure. Legal protection in this case is subject to unfair competition rules and intellectual property laws (Mansour; 2024, 73).

Second: The Legal Nature of Data as an Intangible Asset and a Competitive Value for the Company

The legal nature of data is the subject of extensive scholarly debate in contemporary commercial law. The data is no longer merely a technological resource; it has become an intrinsic economic asset with monetary value. This necessitates moving it beyond the traditional framework of information and classifying it as an "intangible asset". An intangible asset is defined as a non-material asset that possesses an economic value, which is identifiable and legally controllable, and generates future financial benefits for the organization.

From a jurisprudential and legal perspective, the legal nature of data as an asset and a competitive asset is defined by the following three main dimensions:

1. **Exclusive Ownership and Control:** Traditional legal rules (such as the right of the ownership of physical property) struggle to encompass data because it is intangible and can be copied and accessed multiple times simultaneously without being exhausted. Therefore, modern jurisprudence tends to characterize the right to data as a type of "innovative intellectual property" or as an "exclusive right" that grants the company the power to prevent others from exploiting it unlawfully, thus providing it with protection under unfair competition rules (Chagal-Feferkorn; 2024, 347).
2. **Competitive Advantage: Data represents a company's market power.** Companies with large, organized data streams operating within stable legal frameworks possess a unique advantage that their competitors lack. This competitive advantage is clearly evident in the financial valuation of companies during the mergers and acquisitions, where the "databases" are valued as a key component of intangible assets (the physical store or digital platform) (Wachter; 2023, 107).
3. **Protection through Contractual and Technical Obligations:** Due to the fluid nature of data, its legal status necessitates that the companies protect it through two complementary means: Technical means (encryption and firewalls) and legal, contractual means (non-disclosure agreements (NDAs) and confidentiality clauses in employment and cloud service contracts) to legitimize their control over that data (Hacker; 2023, 590).

Third: The Role of AI in Processing and Utilizing This Data: Predictive Analytics and Process Automation

The relationship between data and AI is existential and complementary; data is the lifeblood, and AI is the intelligent engine that transforms that data from mere "silent, stored numbers" into "productive power and investment decisions". This

investment role is embodied in the following two main mechanisms that the modern commercial companies rely on:

1. **Predictive Analytics:** Predictive analytics relies on the use of machine learning algorithms and mathematical statistics to extrapolate from historical and current data in order to predict future behavioral and economic events with high accuracy.

Investment Impact: AI enables the businesses to move from a reactive to a proactive approach. For example, algorithms can analyze the consumers' past purchasing data to predict the demand for a particular product in an upcoming season or forecast a customer's likelihood of defaulting on their financial obligations (intelligent credit scoring). Legally, this investment raises concerns about the automated behavioral profiling and its legality in relation to individual rights (Al-Hassani; 2024, 222).

2. **Process Automation:** Automation in the AI era transcends the traditional concept of automatic data entry to what is known as Intelligent Process Automation (IPA). Here, algorithms can process and interpret unstructured data and make operational decisions based on it without direct human intervention.

Investment Impact: Automation of supply chains, warehouses, processing returns, responding to customer inquiries using virtual assistants and drafting and reviewing commercial standard contracts are all applications for AI. Such automation has been shown to significantly lower operating costs, increase speed and decrease human error. However, complete automation of processes presents companies with considerable risk from a legal standpoint, especially when dealing with data breaches or algorithmic errors resulting in an adverse or unfair automated decision, leading to an increased risk of the employer having legal liability to a third party. (De Hert; 2023, 980).

The second requirement: Legal and Cyber Risks of AI Technologies on Data Security

First: Risks of Data and Trade Secret Leaks via Machine Learning Algorithms:

Deep neural networks and generative models represent a new source of risk due to unintentional backtraining of data. There are three primary ways in which unintentional backtraining can occur:

1. When employees and engineers who work for a company input sensitive data into the AI system (cloud-based large language models) for either analysis or optimization purposes, they do so with the understanding that their sensitive information will be included in algorithmic weights along with the data continuously updated/reprocessed throughout its life-cycle.
2. Data Reversion (Data Inversion Attacks) is an example of how a user may reverse engineer or develop an alternative querying method to extract sensitive data used to develop the model from the original training data set was processed for a given model user's input request.
3. Legal Repercussions: The dissemination of data through algorithms deprives "trade secrets" of their most significant legal protections; notably, "confidentiality and reasonable safeguards." Any trade secret placed into the hands of a third-party algorithm results in the loss of the right to support by sabotage laws and leaves the business vulnerable to significant competitive disadvantage with little or no chance of legal recourse. (Al-Shamarti; 2024, 319).

Second: Feeding AI Models with Unauthorized Data and Violating Intellectual Property Rights

The philosophy behind building and developing AI models relies on collecting astronomical amounts of data through digital scraping techniques (Web Scraping). This process places AI developers and users in a precarious position regarding the violation of intellectual property rights and privacy regulations in two ways:

1. **Infringement of moral and material rights:** Databases, digital works, protected economic reports, and software innovations belonging to other commercial companies are obtained without prior licensing (unlicensed data) and used as training material for machine learning models.

2. **Production of plagiarized output:** Algorithms may produce outputs (reports, designs, and software solutions) that closely resemble or are identical to the original works they were trained on, constituting an infringement of copyright and related rights.
3. **Legal implications:** This behavior raises a legal battle over the concept of "fair use" of data. Under this principle, companies are obligated to prove that the data has been used for transformative purposes and not for commercial reproduction. In the absence of explicit legal provisions, commercial companies using AI tools trained on pirated data become liable to prosecution for complicity in intellectual property infringement and obligated to pay substantial financial compensation to those affected.

Third: Intelligent Cyber Threats (AI-Powered Attacks and Penetration of Corporate Cloud Systems) (Borgesius; 2024, 38)

AI is no longer just a defensive tool for companies; it has been employed by cybercriminal organizations to develop a highly lethal offensive arsenal that surpasses the capabilities of traditional defense systems. These threats are manifested in the following ways:

1. **Automated and Adaptive Cyber Attacks:** Hacking software uses algorithms to scan corporate cloud networks, discover zero-day vulnerabilities in seconds, and automatically modify the attack code to bypass traditional firewalls.
2. **Intelligent Social Engineering and Deepfakes:** Highly specific phishing emails are crafted using AI, accurately mimicking the style of senior management or even forging the voice and image signatures of executives to solicit financial transfers or grant access to cloud databases.
3. **Data Poisoning:** This involves breaching company systems and subtly but intelligently modifying stored data, leading to disruptions in company

algorithms and disastrous investment or credit decisions that harm its financial standing.

4. **Legal Implications:** These threats expose companies to "negligence in cybersecurity". Modern legislation (most notably the GDPR) does not absolve the companies of liability simply because they fall victim to a sophisticated attack. Instead, it holds them accountable for their adherence to security standards that address the evolving nature of the threat. This means that the AI-powered attacks raise the legal threshold for exercising due diligence in protecting cloud data (Al-Ubaidi; 2024, 279).

The Third Requirement: Legal Challenges in Determining Civil and Criminal Liability for Data Damage

First: The “Black Box” Problem and the Difficulty of Proving Error in Algorithmic Decisions

The “Black box” phenomenon represents the most complex challenge to the traditional rules of legal liability (civil and criminal), which are primarily based on the concept of “presumed error or the burden of proof.” This technical and legal problem rests on the following:

1. **Lack of Transparency and Absence of Logical Traceability:** In deep learning systems, algorithms follow complex, non-linear paths to process data and produce outputs. The values of equations and internal weights change automatically without human intervention. This means that the outcome (whether a credit denial decision, a data leak, or an unfair discriminatory preference) cannot be legally explained as “how” it was reached, even by the engineers who designed the system.
2. **Inability to Prove the Material and Moral Elements:** When an affected company seeks compensation, it faces the burden of proving “error.” In traditional law, the plaintiff must prove a deviation from the behavior of a reasonable person. However, in algorithmic decision-making, it is impossible to determine whether the harm resulted from a design flaw, a defect in the

training data, or unpredictable automatic machine behavior. This leads, in legal terms, to «deficiency of causation», preventing the injured party from proving a link between the wrongful act and the harm caused by the «black box» (the machine) (Sultan; 2024, 67).

Second: Determining Liability among AI System Developers, Companies Using Them, and the End User

The production and operation of AI systems are not carried out by a single actor but rather are the product of an "intertwined digital value chain." This creates a significant overlap in determining the legal liability when a data breach or corruption occurs. The parties involved in this chain are distributed as follows:

1. **The system developer and data provider:** This is the party that writes the code and trains the prototype. Their liability arises if it is proven that the system has been built on faulty algorithms or contaminated training data that led to the destruction or leakage of company assets.
2. **The Deployer:** This is the organization that purchases or leases the system (as a cloud service) and utilizes it in its daily operations to process the customer data. This company bears responsibility for "putting the system into service," human oversight (human-in-the-loop), and its commitment to updating the system and protecting it from attacks.
3. **The End-User:** This is the employee or customer who interacts with the system. Damage may result from misuse, entering unauthorized data, or ignoring security warnings.
4. **Legal Implications:** This complex interplay presents significant challenges in apportioning joint and several liabilities. Each party attempts to shift the blame onto the other through adhesion contracts or disclaimer clauses. This necessitates contemporary legal scholarship developing a new theory of liability based on "the actual level of control over algorithmic risk" rather than personal fault (Kaminski; 2023, 435).

Third: The Absence of an Independent Legal Personality for AI and its Impact on Compensating Affected Companies

With the increasing autonomy of software and its ability to make independent financial and commercial decisions, legal scholars have raised the hypothetical question of whether the AI can be granted as an "independent electronic personhood", similar to the legal personality of companies. However, the current legislation generally rejects this approach, which has significant implications for compensation:

1. **Lack of independent financial standing:** Since AI is merely a tool and technology without legal capacity, it does not possess an independent financial standing that can be used to collect the compensation. Consequently, the "program" or "robot" itself cannot be sued for damaging the commercial databases belonging to others.
2. **Reversion to liability for things or custody of the building:** Due to the absence of independent legal standing, the courts are forced to revert to traditional concepts by shifting the liability to the «custodian of the thing» (the owner or operator of the system).
3. **Inadequate Compensation and Insurance Gap:** Traditional rules fail to provide a fair and adequate compensation for the damages in cases of "complete machine autonomy" (such as an intelligent financial trading system selling the company's assets based on a flawed data analysis). This legislative shortcoming is driving modern economies toward adopting "mandatory insurance against the AI risks" and establishing dedicated compensation funds to ensure that the companies harmed digitally are not penalized (Edwards; 2024, 113).

Section Two: Legislative Response to the Risks of AI on the Data (A Comparative Study between the European Union and Iraqi Law)

The First Requirement: Data Protection under the European General Data Protection Regulation (GDPR)

First: Fundamental Principles of Data Processing in the GDPR and Their Impact on the AI Algorithms (Transparency, Purpose-Specification)

The Article 5 of European Regulation forms the core of the legal framework for the data protection and the first legislative line of defense against the unchecked power of algorithms. The AI mechanisms have clashed with the following two fundamental principles of this article:

1. **The Principle of Lawfulness, Fairness, and Transparency:** This principle obliges the companies to fully disclose how they process the data. In the context of AI, this principle faces the «black box» dilemma of deep learning, where the algorithm is unable to explain its logical trajectory. Therefore, the GDPR, under Articles 13 and 14, mandates the "right to explanation," obligating the companies to provide users with clear and understandable information about the algorithmic logic governing their processing. This has pushed the digital industry toward adopting "explainable artificial intelligence (XAI)". The principle of "fairness" also requires the purging of training data to prevent discriminatory algorithmic bias.
2. **The principle of purpose limitation:** This principle prohibits processing the data for purposes other than those for which it was originally collected. It directly contradicts the philosophy of "big data" and AI, which rely on discovering unexpected connections and patterns through secondary processing and recycling. Under the GDPR, the companies are not permitted to use their aggregated customer data for profiling purposes and pass it onto the behavioral and marketing prediction algorithms without explicit, free, and independent consent. This provides proactive protection through the "Privacy by Design and by Default" principle (Al-Yassiri; 2025, 97).

Second: The Rights of Companies and Customers in the Face of Fully Automated Decision-Making

The European legislature dedicated a crucial provision in Article 22 to address the risks of completely eliminating human intervention in legal or financial decision-making, known as "fully automated decisions, including profiling".

The general right to refuse and not submit to an automated decision: The regulation grants individuals or institutions an inherent right not to submit to a decision that has legal consequences affecting them or significantly impacting them if that decision is based solely on automated data processing using AI (such as the automatic rejection of a bank loan application or the algorithmic filtering of job applications).

Exceptions and mandatory safeguards: This prohibition may only be waived in three specific cases: If the decision is necessary for the conclusion of a contract, permitted by federal law, or based on explicit consent. However, the GDPR stipulates that if these exceptions are applied, the companies must provide strict safeguards, including the right to human intervention to review the decision, the right of the individual to express their viewpoint, and the right to appeal the algorithmic decision before a human official. This prohibits a system of "absolute automation" and imposes the principle of "human-in-the-loop" decision-making (Al-Adli; 2023, 49).

Third: Protective Obligations (Impact Assessment, Appointment of a Data Protection Officer (DPO), and Deterrent Financial Penalties

The European regulation has moved from adopting the principle of "theoretical responsibility" to imposing strict procedural and regulatory obligations on companies using high-risk technologies such as AI, supported by a system of penalties that is historically the most stringent:

Data Protection Impact Assessment (DPIA): Under Article 35, the companies are legally obligated to conduct a prior technical and legal study called an "Impact Assessment" before launching or integrating any AI system that performs large-scale structural data processing or automated profiling. This assessment aims to identify

potential risks to privacy rights and implement technical measures (such as encryption and anonymization) to mitigate them.

Appointment of a Data Protection Officer (DPO): Companies, whose core activities include processing operations that require regular and systematic monitoring of large-scale users, are obligated to appoint a qualified and independent person to oversee internal GDPR compliance. This DPO plays a pivotal role in reviewing and auditing the inputs and outputs of AI systems.

Deterrent financial penalties: To ensure compliance, the regulation established a system of escalating financial penalties (Article 83). For serious violations (such as the breaches of processing principles or individual rights), the maximum administrative fines can reach €20 million or 4% of the company's total global turnover for the previous financial year (whichever is higher). This deterrent value has transformed the data protection from a supplementary measure into a strategic security and vital compliance issue at the forefront of European companies' management plans (Al-Fahd; 2023, 123).

The Second Requirement: The Reality of Legal Protection for Commercial Data in Iraqi Legislation

First: Traditional Rules for Protecting Data Confidentiality in Iraqi Civil and Commercial law

The Iraqi legal system currently lacks a unified law specifically for the protection of personal or digital data, unlike modern systems. This compels the judiciary and legal scholars to revert to the traditional rules stipulated in the Iraqi Civil Code No. 40 of 1951 and the Commercial Code No. 30 of 1984 for the protection of corporate data:

Civil Law Framework (Contractual and Tort Liability): The compensation for damages to corporate data is based on the general rules of liability. If the data leakage or destruction results from a breach by an employee or a contracted software company, the contractual liability is activated based on the contractual terms and privacy clauses. However, if the breach is by a third party, the tort liability is applied, based on proving "fault, damage, and causation" (Article 204 of the Civil Code:

Every fault that causes a harm to another obligates the perpetrator to provide compensation). The dilemma of AI here lies in the difficulty of proving the material element of error in the algorithm's decision (the "black box"), which weakens the effectiveness of these provisions.

Commercial Law Frameworks (Unfair Competition): The commercial Law provides indirect protection for trade secrets and data through the rules of "unfair competition" (Articles 96-101). Under these rules, the competitors are prohibited from using means that violate commercial ethics to obtain data and plans from another company. However, these provisions are formulated in a traditional, physical environment and are unable to provide proactive (preventive) protection against "automated digital scraping" (web scraping) carried out by AI algorithms to collect the market and company data covertly, without being explicitly criminalized in these provisions (Al-Dulaimi; 2023, 157).

Second: Criminal Protection of Corporate Data in the Iraqi Penal Code and its Applications to Digital Crimes

In the absence of comprehensive legislation specifically addressing cybercrimes, the Iraqi judiciary is attempting to adapt the provisions of Penal Code No. 111 of 1969 to protect the companies' information assets against hacking or sabotage. This protection manifests itself through several applications and avenues:

The crime of disclosing secrets: The Article 437 of Penal Code punishes anyone who discloses a secret entrusted to them by the virtue of their position or profession. This provision can be applied to the employees who feed the external AI systems confidential company data. However, the text requires "intentionality and criminal intent," which is difficult to prove if the leak resulted from technical negligence or a lack of understanding of how the cloud algorithms work.

Crimes of sabotage and intentional destruction: Articles related to the destruction of funds and records (such as Article 477) criminalize the physical destruction of assets. This provision has been legally adapted to include the digital destruction of databases. However, applying this provision to sophisticated AI-powered

cyberattacks encounters the obstacle of technical specification. The attack algorithms may not "destroy" the data but rather "poison" it (data poisoning) or slightly modify its mathematical values to steer the company decisions toward losses. This behavior falls outside the literal meaning of traditional "destruction and erasure," creating a gap in criminal deterrence (Al-Hadithi; 2023, 28).

Third: Special Laws and Recent Legislative Trends (The Draft Cybercrime Law and its Adequacy in Addressing AI)

By recognizing the seriousness of digital legislative vacuum, the Iraqi legislature has moved toward formulating special frameworks, most notably the "Electronic Signature and Electronic Transactions Law No. 78 of 2012," culminating in the ongoing proposals for the "Draft Cybercrime Law".

Strengths of the Draft Law: The draft cybercrime law aims to close criminal loopholes by criminalizing unauthorized access to websites and electronic systems, and imposing severe penalties for hacking cloud and banking systems and destroying the databases of commercial institutions.

Its adequacy in addressing the AI (shortcomings): Despite the importance of this project, it faces sharp academic and legal criticism for being written with a legislative mindset focused on "traditional cybercrime" (such as manual hacking, defamation, and personal digital extortion), without grasping the complex dimensions of the AI revolution. The law fails to regulate:

1. The issue of legal liability arising from the machine's independent self-inflicted damage.
2. The absence of a requirement for companies to conduct prior algorithmic risk assessments (DPIA).
3. **The lack of legal safeguards for users against "fully automated decisions" and behavioral data profiling, which places the proposed Iraqi legislative framework several** steps behind the rigorous European approach to the GDPR (Kanaan; 2023, 69).

The Third Requirement: Prospects for Developing the Iraqi Legislative System in Light of the European Experience

First: Shortcomings and Legislative Overlaps in Iraqi Law Compared to the Firm Guarantees of the GDPR

The comparative analytical study revealed a deep legislative and structural gap between the Iraqi legal reality and the firm guarantees established by the European GDPR. The most prominent shortcomings and overlaps are evident in the following points:

Fragmentation of Texts and Lack of Legislative Digital Awareness: The legal protection for the data in Iraq is distributed among disparate traditional texts (Civil Law, Penal Code, and Commercial Law). This fragmentation creates legislative overlap and procedural ambiguity before the judiciary, as these laws have not been designed for a digital environment and failed to distinguish between the "data as an inherent right of the individual" and the "data as a financial and competitive asset for the company" (Zarsky; 2025, 165).

The absence of Preemptive Protective Principles: The Iraqi law completely lacks principles such as "Privacy by Design" and the principle of "data limitation". Iraqi laws are reactive (waiting for a damage to occur before providing a compensation), while the GDPR adopts a proactive approach, requiring companies to engineer their algorithms to protect the data before implementation.

The lack of a specialized oversight mechanism and deterrent penalties: Iraq lacks an independent data protection authority (similar to the European data protection commissions) to monitor and audit the companies' algorithms and receive the user complaints. Furthermore, the traditional civil compensation based on the concept of "tangible material damage" offers no financial deterrent to companies compared to GDPR fines, which can reach 4% of global revenues. This makes the data protection in the local environment a secondary and practically non-binding issue (Floridi; 2024, 81).

Second: The Requirements for Drafting a Specific Iraqi Law for the Protection of Personal and Commercial Data That Keeps Pace with the Rapid Advancements in Data protection.

To bridge the legislative gap and keep pace with the technological revolution, the Iraqi legislature must abandon the piecemeal approaches to traditional laws and instead draft a comprehensive and advanced data protection law. This law should be based on the following principles:

1. **Establishing a National Data Protection Authority:** The law must stipulate the creation of an independent regulatory body with legal personality and financial and administrative autonomy. This body should include legal and technological experts and be responsible for granting licenses for big data processing, auditing the efficiency of AI algorithms, and combating algorithmic bias.
2. **Legislating the "Right to Interpretation" and Human Oversight:** The Iraqi legislature must incorporate the safeguards outlined in Article 22 of the GDPR by prohibiting the fully automated decisions made by AI tools without human oversight (human-in-the-loop decisions). Companies must also be obligated to provide legal mechanisms that guarantee the users' right to understand the "algorithmic logic" and challenge the intelligent decisions (such as automated hiring or credit rating decisions).
3. **Mandatory Impact Assessment and Proportional Fines:** Businesses should be legally obligated to conduct a Data Protection Impact Assessment (DPIA) before integrating any smart technology that could compromise the data privacy. A system of escalating financial penalties, calculated as a percentage of annual profits, should be adopted to ensure the compliance (Al-Khafaji; 2025, 48).

Third: Digital Governance and Self-Compliance Strategies for Iraqi Businesses to Adopt.

Pending a national legislative overhaul, the Iraqi businesses, (particularly banks, insurance companies, and telecommunications companies) cannot remain legally inactive. They must adopt voluntary self-compliance strategies to protect their competitive advantages and business reputation, as follows:

1. **Adopting Data Governance Frameworks:** Companies must develop robust internal policies that define the data access permissions and classify the data (public, confidential, and highly sensitive) while continuously monitoring how machine learning algorithms are fed with this data to ensure that the trade secrets are not leaked through the cloud.
2. **Creating a "Compliance and Data Protection Officer" Position:** Similar to the European Data Protection Officer (DPO), large companies should appoint legal and technical advisors whose primary task is to review the technology supply contracts with AI companies and ensure the inclusion of "mutual liability disclaimers" and clauses prohibiting the use of company data for training public models.
3. **A Proactive Cybersecurity and Digital Literacy Strategy:** Investing in the AI-powered cybersecurity systems is to detect the data poisoning attempts or sophisticated hacks early while simultaneously training and educating the company personnel about the risks of social engineering and deepfakes. This will ensure the development of a secure corporate environment capable of leveraging technological advancements with minimal legal repercussions (Guihot; 2024, 235).

Conclusions:

First: Study Findings

1. Inadequacies of the Traditional Liability Theory: This study demonstrated the inadequacy of the general rules of civil and criminal liability in the Iraqi law to establish the material element of error in the algorithmic decisions due to

the "black box" dilemma and the difficulty in distributing the responsibility among the developers, user companies, and end users.

2. **Lack of a Preventive Dimension in Iraqi Legislation:** The Iraqi legal system lacks the proactive protection mechanisms characteristic of the GDPR, such as the mandatory Data Protection Impact Assessment (DPIA) and the codification of the "Privacy by Design" principle.
3. **Limited Deterrence and Absence of Structural Governance:** The absence of an independent body specializing in the digital data protection in Iraq, and the reliance on limited traditional civil compensation, lead the companies to disregard the cybersecurity requirements due to the lack of proportionate and deterrent financial penalties commensurate with their commercial profits.
4. **The Threat of Trade Secrets through Reverse Training:** It has been portrayed that the uncontrolled use of the generative AI tools by company personnel legally leads to the removal of the "confidentiality" status from the commercial data and its exclusion from the protections afforded by unfair competition once it enters the public cloud databases.

Second: Recommendations

Based on the study's findings, the following procedural and legislative package to develop the Iraqi legal system and business environment are proposed:

To the Iraqi Legislature (Legislative Recommendations)

1. **Expediting the Enactment of a Specific and Unified Law for the Protection of Personal and Commercial Data:** This law should draw upon the advanced principles of the GDPR, including the specific provisions that criminalize unauthorized digital scraping and data poisoning by intelligent systems.
2. **Incorporating the Dimensions of AI into the Draft Cybercrime Law:** Specifically, This law should codify the «right to algorithmic interpretation» and impose mandatory human oversight (human-in-the-loop) on the fully automated commercial and credit decisions.

3. **Establishing the «Iraqi National Authority for Digital Data Protection»:** This is an independent regulatory body responsible for the technical audits of the major companies' algorithms, issuing the compliance guidelines, imposing the deterrent, and escalating the fines on violators.

To the Iraqi Commercial Companies (Administrative and Regulatory Recommendations)

1. **Voluntarily Adopting Self-Compliance Strategies:** Developing internal governance regulations and appointing a "Compliance and Data Protection Officer" to review the technology supply contracts and prohibit the feeding of company secrets to the public algorithms.
2. **Investing in the Proactive Cybersecurity:** Training the personnel in the social engineering and sophisticated deepfake scenarios to protect the administrative structures from the infiltration.

Sources:

1. Al-Ubaidi, Ali Hadi (2024). The General Theory of Obligations: A Comparative Study in Adapting Liability for Artificial Intelligence Damages. Dar Al-Thaqafa for Publishing and Distribution, Amman, First Edition.
2. Al-Fahad, Rana Mohammed (2023). "Civil Liability Arising from Fully Automated Decisions: A Comparative Study between Iraqi Law and the European General Data Protection Regulation." Babylon Journal of Human Sciences, Volume 31, Issue 4, pp. 112-140.
3. Al-Hadithi, Fakhri Abdul-Razzaq (2023). Explanation of the Iraqi Penal Code: Emerging and Cybercrimes. Al-Thakira Library, Baghdad, Second Edition.
4. Al-Hassani, Maryam Jassim (2024). "Legal Protection of Electronic Consumer Data from Automated Profiling Decisions." Journal of Law - College of Law, Al-Nahrain University, Vol. 26, No. 2, pp. 211-239.
5. Al-Jubouri, Marwan Hussein (2025). Digital Commercial Law: Protecting Trade Secrets and Data in the Age of Algorithms. The Legal Library, Baghdad, First Edition.

6. Al-Khafaji, Mustafa Jawad (2025). "Legal Challenges Facing Corporate Trade Secrets in Light of Machine Learning Algorithms." Al-Rafidain Journal of Law - College of Law, University of Mosul, Volume 27, Issue 84, pp. 19-53.
7. Al-Shamarti, Ali Kadhim (2024). "The Impact of Artificial Intelligence Mechanisms on the Principle of Transparency in Cloud-Based Commercial Transactions." Al-Muhaqqiq Al-Hilli Journal of Legal and Political Sciences - University of Babylon, Vol. 16, No. 3, pp. 310-345.
8. Al-Yasiri, Muhammad Abdul-Hussein (2025). "Commercial Data Governance and Cybersecurity Guarantees in Iraqi Banks." Iraqi Journal of Administrative Sciences - University of Karbala, Vol. 21, No. 81, pp. 89-118.
9. Al-Zubaidi, Ahmed Hassan (2024). "The Iraqi Cybercrime Bill in the Balance of Criminal Protection of Digital Data: An Analytical Study." Journal of the College of Law for Legal and Political Sciences - University of Kirkuk, Volume 13, Issue 50, pp. 201-235.
10. Al-Adli, Zeina Abdul-Amir (2023). The Problem of Liability for Things and its Application to Artificial Intelligence Software in Iraqi Law. Unpublished Master's Thesis, College of Law, University of Kufa.
11. Borgesius, F. J. (2024). "Data Protection, Artificial Intelligence, and Discrimination in Automated Decision-Making". European Data Protection Law Review (EDPL), Vol. 10, No. 1, pp. 33-49.
12. Chagal-Feferkorn, K. A. (2024). "Am I an Algorithm's Keeper? Assigning Liability for AI-Inflicted Torts and Data Breaches". Harvard Journal of Law & Technology, Vol. 37, No. 2, pp. 311-354.
13. De Hert, P., & Papakonstantinou, V. (2023). The GDPR in the Age of AI: Corporate Compliance and Data Protection Regimes. Oxford University Press, Oxford, 2nd Edition.
14. Edwards, L., & Veale, M. (2024). "Slave to the Algorithm? Why a Right to an Explanation is an Imperfect Shield Against Corporate AI". Duke Law & Technology Review, Vol. 22, No. 1, pp. 85-119.

15. Floridi, L. (2024). The Law of Big Data and Artificial Intelligence: Foundations and Corporate Governance. Routledge, London, 1st Edition.
16. Guihot, M., & Matthew, A. (2024). "Cybersecurity Threats in Cloud Computing Driven by AI: Legal Liabilities for Businesses". International Journal of Law and Information Technology, Vol. 32, No. 3, pp. 215-242.
17. Hacker, P. (2023). "Manipulating Machine Learning: Data Poisoning and the Boundaries of Product Liability Law under EU Regs". Artificial Intelligence and Law, Vol. 31, No. 4, pp. 589-623.
18. Kaminski, M. E. (2023). "The GDPR, Risk Management, and the Impact of Generative AI on Corporate Trade Secrets". Berkeley Technology Law Journal, Vol. 38, No. 2, pp. 401-445.
19. Kanaan, Nawaf (2023). The Legal System of Artificial Intelligence and Unfair Competition in Commercial Companies. Dar Wael for Publishing, Amman, First Edition.
20. Mansour, Khalid Abdul-Hamid (2024). "The Impact of the European Regulation (GDPR) on Cross-Border Commercial Contracts." Legal and Judicial Journal - Iraqi Ministry of Justice, Vol. 15, No. 2, pp. 55-88.
21. Al-Dulaimi, Yasser Thamer (2023). "The Black Box Dilemma and Proving Unintentional Error in Cybercrime." Journal of the Judiciary - Iraqi Bar Association, Vol. 78, No. 1, pp. 143-172.
22. Omar, Amani Taher (2024). Legislative Regulation for the Protection of Personal Data: A Comparative Study between Arab Legislation and the European Union (GDPR). Dar Al-Nahda Al-Arabiya, Cairo, First Edition.
23. Sultan, Haider Ali (2024). "The Adequacy of General Rules in Iraqi Civil Law for Compensating Damages Caused by Intelligent Systems." Journal of Legal Sciences - College of Law, University of Baghdad, Volume 39, Issue 2, pp. 45-72.

24. Wachter, S., & Mittelstadt, B. (2023). The Black Box Problem: Accountability, Transparency, and the Right to Explanation under GDPR. Cambridge University Press, Cambridge, 1st Edition.
25. Zarsky, T. Z. (2025). "The Privacy-Innovation Trade-off: Re-evaluating Purpose Limitation Under GDPR for Big Data Entities". European Journal of Legal Studies, Vol. 17, No. 2, pp. 167-198.