مركز البيان للدراسات والتخطيط
Al-Bayan Center for Studies and Planning

2026/2/24

Artificial Intelligence and Privacy in the Iraqi Digital Economic Space

Challenges and Solutions, with an Overview of Privacy Protection Measures in Iraq and Norway

Dr. Sanaa Abdul Qader Mustafa

● Policy Paper

Al-Bayan Center Studies Series

Policy Paper

2026/1/24

Artificial Intelligence and Privacy in the Iraqi Digital Economic Space

Challenges and Solutions, with an Overview of Privacy Protection Measures in Iraq and Norway

Series of publications of Al-Bayan Center for Studies and Planning
Research Department / Economic Studies

Publication / Policy Paper

Topic /Economy and Development

Dr. Sanaa Abdul Qader Mustafa / University Professor – Norway – PhD in Industrial Economics

Translation/ Milad Alnofali

About

Al-Bayan Center for Planning and Studies is an independent, nonprofit think tank based in Baghdad, Iraq. Its primary mission is to offer an authentic perspective on public and foreign policy issues related to Iraq and the region.

Al-Bayan Center pursues its vision by conducting independent analysis, as well as proposing workable solutions for complex issues that concern policymakers and academics.

www.bayancenter.org
info@bayancenter.org
Since 2014

I. Executive Summary:

- The deployment of artificial intelligence applications in Iraq is rapidly increasing, ranging from public service systems and health data analytics to surveillance systems and electronic marketing. This growth opens significant economic and social opportunities; however, it exposes citizens' privacy and digital governance practices to serious risks.

- The Iraqi reality indicates the existence of three main issues in the digital space: excessive data collection, weak legal frameworks, as well as cyber threats and a lack of digital awareness.

- Iraq requires a clear legal framework for data protection, along with technical practices such as privacy-by-design, encryption, algorithmic oversight, in addition to building institutional and societal capacities.

- Decision-makers must initiate a sequenced and coherent dialogue on the gradual implementation of legal information protection, emphasizing that engagement with the private sector and civil society is essential to ensure a balance between innovation and the protection of rights.

- There is no comprehensive law regulating data protection in Iraq, including within the private sector; nevertheless, some provisions regulate privacy in general and provide protection for personal data in telephone communications, telegrams, and government documents.

- The provisions currently in force in Iraq do not rise to the level of international data protection standards, such as those established by the General Data Protection Regulation (GDPR), the Organisation for Economic Co-operation and Development (OECD), the Asia-Pacific Economic Cooperation (APEC), and the Personal Information Protection Law (PIPL), rendering them inadequate to address data protection concerns amid rapid technological development.

- From an economic perspective, states are enacting laws to control various aspects of this field, such as jurisdiction and data localization. Therefore, the definitions and principles of the GDPR and other frameworks should be taken into account when determining online privacy and data protection in Iraq.

- The absence of international standards in Iraq hinders the establishment of controls consistent with global norms, leaving citizens vulnerable to data exploitation and cybercrime, and increasing the difficulty of international cooperation to address cross-border cybercrime and data breaches.

- The draft Cybercrime Law primarily addresses computer-related crimes and lacks substantial provisions related to data protection.

- The traditional laws currently applied in Iraq are unable to address or accommodate the new challenges imposed by the digital era, exposing citizens to risks that threaten national security and economic interests.

- Iraq urgently needs to exert rapid efforts to regulate and protect online data in order to address the growing risks in the digital domain.

- It is necessary to amend existing laws to address critical contemporary issues related to data protection and to ensure their compatibility with current technological and societal challenges.

- Iraq should conclude multilateral and bilateral agreements to enhance cross-border data protection and ensure security.

- The draft Cybercrime Law should be reviewed to include modern data protection principles.

II. **Introduction:**

The operational importance of artificial intelligence privacy in the Iraqi digital space lies in AI's reliance on data as a primary source for learning and development. The data used include users' behaviors, geographic locations, consumer preferences, and even biometric data. This intensive reliance makes data protection a strategic challenge. Privacy risks manifest in several aspects, including:

- **Covert surveillance:** Algorithms that track users online without explicit consent.

- **Re-identification:** The ability to link anonymized data to specific individuals.

- **Discrimination and bias:** In decision-making algorithms, potentially leading to unfair outcomes in areas such as employment and insurance.

- **Security breaches:** AI systems may become targets of cyberattacks aimed at sensitive data.

The European General Data Protection Regulation (GDPR), adopted in 2018, incorporated legal and ethical dimensions and established a stringent framework regulating data collection and use. In contrast, the legislation of many Arab and developing countries, including Iraq, has yet to keep pace with technological challenges.

From an ethical standpoint, the issue of data ownership and individuals' right to control their personal information is raised. Possible technical solutions include:

- Encryption, anonymization, and secure computing.

- Differential Privacy to ensure data protection during analysis.

- Transparency: obligating companies and institutions to disclose data collection policies.

- Accountability: establishing oversight bodies to hold entities that violate privacy accountable.

- Digital literacy: raising individuals’ awareness of the importance of protecting their data and how to control it.

III. Artificial Intelligence and Digital Privacy in the Era of Technological Transformation

Artificial intelligence technologies have entered the core of digital transformation in Iraq, ranging from improving the delivery of government services to automating processes in the private sector. Alongside these benefits, critical questions arise regarding the extent to which individuals’ privacy and digital rights are protected. This analysis addresses the main challenges in the Iraqi digital landscape and presents practical, implementable solutions. In 2025, artificial intelligence (AI) has become an essential part of daily life, being used across multiple fields such as healthcare, education, business, and security. With this expansion, concerns are increasing about how these technologies affect individuals’ digital privacy. Studies indicate that 57% of consumers consider AI to pose a significant threat to their privacy, while 27% feel neutral about the issue, and only 12% do not believe that AI negatively affects their privacy.[1]

The world is witnessing an unprecedented surge in the field of artificial intelligence, as it has come to be employed across various economic, social, security, and health sectors. This rapid development poses challenges related to the protection of personal data and individuals’ digital privacy, particularly in light of the massive growth in data volumes on which machine-learning algorithms rely.

The importance of this research lies in highlighting the relationship between artificial intelligence and information privacy in Iraq, and in

[1]**. 10 Under-the-Radar AI Companies to Watch in 2026**, https://www.eweek.com/news/under-the-radar-ai-companies-2026/

identifying risks and possible solutions to ensure a secure digital space that contributes to the development of the Iraqi national economy. The study also aims to shed light on the most significant challenges that may confront the protection of AI privacy in the Iraqi digital space, in terms of:[2]

1. Clarifying and identifying the real reasons that constitute obstacles to protecting AI privacy in the Iraqi digital space across public, private, and mixed sectors, based on scientific analysis as defined by the methodology of this research.

2. Proposing practical solutions to achieve AI privacy in the Iraqi digital space through long- and medium-term economic plans, ensuring comprehensive and sustainable economic development and the advancement of investment in the Iraqi national economy.

This paper addresses specific concepts for how to tackle the challenges facing AI privacy in the Iraqi digital space across public, private, and mixed sectors that hinder its development, while also identifying privacy protection measures in Iraq and Norway.

The paper advances the hypothesis that insurance companies and financial institutions exist in Iraq that aim to secure AI privacy in the digital space, within public, private, and mixed sectors that generally hinder its development. The paper also relies on long-term strategic planning (ten-year plans) and five-year economic plans that align with the nature of work in Iraq and its social environment, with the aim of achieving the desired economic and social development objectives.

Information systems within institutions and industrial production projects that are directly linked to the national economy constitute one of the fundamental pillars contributing to solving most of the problems related to providing and securing AI privacy in the Iraqi digital space across public, private, and mixed sectors that hinder its

[٢] **Data Protection in Iraq: Limitations of Existing Laws Amid the Tech Wave**, *TWEJER Journal*, Vol. 8, Issue 4, Nov. 2025, pp. 468–469. https://journals.soran.edu.iq/index.php/Twejer/article/view/2066/1081 development overall, through the adoption of sound decision-making, the elimination of administrative bureaucracy, and the reduction of overlapping administrative functions among different organizational units, in order to ensure AI privacy in the Iraqi digital space across public, private, and mixed sectors that hinder its development in general.

IV. Why Is Privacy Important in the Context of Artificial Intelligence?

Artificial intelligence relies on massive amounts of data, some of which are personal and sensitive. If such data are used without proper controls, this may lead to algorithmic discrimination, privacy violations, and the leakage of sensitive information, and may also deter individuals from using digital services, thereby reducing economic and social benefits. The main challenges in the Iraqi digital space in this context are as follows:[3]

1. **Lack of clear legislative frameworks and weak enforcement:** Existing laws are either incomplete or not strictly enforceable with respect to personal data protection, and there are no effective oversight mechanisms governing the use of AI technologies.

2. **Excessive data collection and the absence of the data minimization principle:** Many institutions collect data with no real need for processing them, or store them for long periods without clear purposes.

3. **Lack of transparency:** The use of closed algorithms hinders the ability to audit and intervene when bias or errors occur.

4. **Insufficient technical and security capacities:** Weak cybersecurity infrastructure and limited local expertise in data protection and AI risk management.

[3] Nadhim Hassan and Mayy Ablahad, Auditing Bias in Artificial Intelligence in Light of the Institute of Internal Auditors' Artificial Intelligence Audit Framework: A Theoretical Analytical Study, Journal of Contemporary Business and Economic Studies, Vol. 6, No. 1, 2023, various pages.

5. **Risks of surveillance and monitoring:** Surveillance tools or recognition systems may be used in ways that violate civil liberties, particularly in the absence of independent legal oversight.

6. **Low awareness among the public and institutions:** Limited understanding among citizens of their digital rights, and weak corporate practices regarding disclosure and obtaining valid consent.

Accordingly, measures require the enactment of a personal data protection law that defines data collection rules, purposes, individuals' rights (access, rectification, erasure), and penalties for violations; the establishment of an independent data and AI regulatory authority with investigative and sanctioning powers; the application of the principle of Privacy by Design, whereby government and private projects are required to embed privacy protection in the early design stages of AI systems; and the adoption of Data Protection Impact Assessments (DPIA) prior to deploying any new system that handles sensitive data.

It is necessary to impose practical constraints on data collection and storage by enforcing the data minimization principle and enhancing retention requirements (clear time limits), and to encourage anonymized or encrypted processing patterns wherever possible. Transparency and accountability in algorithms are also crucial, including requirements to publish explanatory summaries of how algorithms operate and their expected impacts on users' rights; independent mechanisms to review algorithms used in decisions that affect fundamental rights (such as employment, welfare, and social services); and the building of national capacities and cybersecurity through training programs for public and private sector workers on user data management and system security, alongside investments in cybersecurity infrastructure and robust encryption tools.

In addition, public education and the promotion of a culture of informed consent are necessary through awareness campaigns explaining users' rights, the risks of data sharing, and methods of protecting personal privacy. Concepts of digital rights should also be incorporated into university curricula and vocational training programs.

Achieving partnerships among the public sector, private sector, and civil society is an important step, through the establishment of joint institutions to formulate practical guidelines, conduct pilot testing of policies before full national implementation, and involve human rights organizations and technical experts in oversight mechanisms to ensure effective protection of privacy and users' rights.

V. **Economic Dimensions**

Protecting privacy in digital systems is not merely a burden; rather, it represents an economic opportunity, as it enhances users' trust in digital systems, encourages the adoption of artificial intelligence services, and increases investment in various economic projects. With well-designed transparency and governance regulation, technology companies can be attracted, which reduces the risks of financial losses resulting from the leakage of sensitive information and enhances the value of data as a sustainable resource.

The economic dimensions include the following:

1. **Data Collection and Use: The Foundation on Which Artificial Intelligence Relies**

Artificial intelligence algorithms depend on massive amounts of data to train models and improve their performance. These data include personal information such as:

- Interactions on social media.
- Search and browsing records.
- Health and financial data.
- Geographic location and personal preferences.

As the use of artificial intelligence expands, concerns increase regarding how these data are collected, who owns them, and how they are used and shared.

2. Privacy Risks: Challenges Facing Individuals and Societies

The most prominent privacy-related risks associated with artificial intelligence include:

- **Continuous surveillance:** The use of technologies such as facial recognition and geolocation tracking to monitor individuals without their knowledge or consent.

- **Discrimination and bias:** Training models on unbalanced data may lead to discriminatory decisions against certain groups.

- **Non-transparent decisions:** Difficulty in understanding how models make decisions, which reduces accountability and transparency.

- **Security breaches:** Exposure of personal data to breaches may result in the leakage of sensitive information that affects individuals and societies.

3. Possible Solutions and Policies: Enhancing Privacy in the Age of Artificial Intelligence

To address these challenges, a set of solutions and policies has been developed to enhance digital privacy:

A. Legal and Regulatory Frameworks

- **General Data Protection Regulation (GDPR):** One of the most prominent legislations aimed at protecting individuals’ privacy in the European Union.

- **European Union Artificial Intelligence Act (EU AI Act):** Aims to regulate the use of artificial intelligence and ensure its compliance with privacy and ethical standards.

- **Local laws:** Such as the California Consumer Privacy Act (CCPA) in the United States, which grants individuals additional rights regarding their personal data.

B. Modern Technologies for Privacy Protection

- **Federated Learning:** Enables model training on local data without the need to transfer them to central servers, thereby reducing the risks of data leakage.

- **Advanced encryption:** The use of techniques such as symmetric and asymmetric encryption to protect data during transmission and storage.

- **Differential Privacy:** A technique aimed at adding noise to data to ensure that individual information is not disclosed during data analysis.

- **Awareness and education:** Raising individuals' awareness of their digital rights and how to protect their personal data through:

  - Training programs and workshops.

  - Media awareness campaigns.

  - Providing tools and technologies that help individuals control their data.

VI. Real-World Examples: Artificial Intelligence Applications and Their Impact on Privacy

Clearview AI was fined €30.5 million by the Dutch Data Protection Authority for using images from social media without permission to train facial recognition models.[4] Company X (formerly Twitter) was also investigated by the Irish Data Protection Commission for using European users' data to train the "Grok" chatbot without explicit

[4] Dutch regulator slaps Clearview AI with $33 million fine and threatens executive liability, Dutch regulator slaps Clearview AI with $33 million fine, threatens executive liability | The Verge

consent.[5] In addition, Meta (META) was prevented from launching its advanced artificial intelligence model "Llama" in the European Union due to regulatory concerns, including strict data protection laws.[6]

While artificial intelligence offers enormous opportunities to improve our lives, it is essential to adopt policies and technologies that ensure the protection of digital privacy. A balance must be achieved between innovation and the protection of individuals' rights through:

- Developing flexible legal frameworks that keep pace with technological developments.
- Investing in technologies that protect data and ensure transparency.
- Enhancing awareness and education among individuals and institutions.

Through these combined efforts, it is possible to build a digital environment that respects privacy and enhances individuals' trust in the use of artificial intelligence technologies.

VII. Artificial Intelligence and Privacy Protection in Norway: Trends and Policies for 2025

A. Government Initiatives and National Strategies

Norway seeks to position itself as a leader in legally responsible artificial intelligence, with a strong emphasis on respect for privacy and data protection. In March 2025, the Norwegian government announced plans to implement the European Union Artificial Intelligence Act (EU

[5] EU Hits Elon Musk's X with 120 Million Euro Fine for Breaching Bloc's Social Media Law, https://apnews.com/article/x-elon-musk-twitter-european-union-regulations-0a135601e050518d5aa0a0155f973177

[6] Meta pulls plug on release of advanced AI model in EU, Meta pulls plug on release of advanced AI model in EU | Meta | The Guardian.

AI Act) and to develop a dedicated Norwegian artificial intelligence law, with the aim of enforcing the new legislation by the summer of 2026. The Norwegian Communications Authority (Nkom) oversees the implementation of these policies, including the regulation of artificial intelligence use in both the public and private sectors and ensuring compliance with European standards.

B. Domestic Legislation Related to Privacy and Data Protection

In January 2025, the new Electronic Communications Act (Ekomloven) entered into force, regulating the use of traffic data in communications networks. Under this law, traffic data must be erased or anonymized when they are no longer necessary for the specified purpose, with retention permitted only if the data are used to provide a value-added service and with the explicit consent of the user.[7]

C. Cooperation with the European Union and Compliance with International Standards

Norway is committed to implementing the European Union Artificial Intelligence Act (EU AI Act), which entered into force in August 2024. As Norway is part of the European Economic Area (EEA), European legislation applies directly to it, including legislation related to artificial intelligence and data protection.

D. Future Trends and Challenges

Despite progress in policy and legislative development, studies indicate that the adoption of artificial intelligence in Norway is proceeding at a slower pace than expected, in both the public and private sectors. Data derived from the 2024 "OKIOS" survey show that the use of artificial intelligence remains at an early stage, despite high expectations for its future application.[8]

[7] Data protection laws in Norway, Data protection laws in Norway - Data Protection Laws of the World

[8] Anvendelse av kunstig intelligens (KI) i Norge i norsk offentlig sektor 2024, [2412.19273] Anvendelse av kunstig intelligens (KI) i Norge i norsk offentlig sektor 2024

VIII. Applications of Artificial Intelligence in the Norwegian Public Sector in 2025: Innovation and Compliance

A. Government Initiatives and National Strategies

Norway seeks to position itself as a leader in responsible artificial intelligence, with a strong emphasis on respect for privacy and data protection. In March 2025, the Norwegian government announced plans to implement the European Union Artificial Intelligence Act (EU AI Act) and to develop a dedicated Norwegian artificial intelligence law, with the aim of enforcing the new legislation by the summer of 2026. The Norwegian Communications Authority (Nkom) oversees the implementation of these policies, including the regulation of artificial intelligence use in the public and private sectors and ensuring compliance with European standards.[9]

B. Domestic Legislation Related to Privacy and Data Protection

In January 2025, the new Electronic Communications Act (Ekomloven) entered into force, regulating the use of traffic data in communications networks. Under this law, traffic data must be erased or anonymized when they are no longer necessary for the specified purpose, with retention permitted only if the data are used to provide a value-added service and with the explicit consent of the user.[10]

C. Cooperation with the European Union and Compliance with International Standards

Norway is committed to implementing the European Union Artificial Intelligence Act (EU AI Act), which entered into force in August 2024. As Norway is part of the European Economic Area (EEA), European legislation applies directly to it, including legislation related to artificial

[9] AI in Norway: Innovation, KI-Norge, and Compliance in 2025, Norway AI 2025: KI Norge & Responsible Compliance, Nemko Digital.

[10] Data protection laws in Norway, Data protection laws in Norway - Data Protection Laws of the World

intelligence and data protection.[11]

D. Future Trends and Challenges

Despite progress in policy and legislative development, studies indicate that the adoption of artificial intelligence in Norway is proceeding at a slower pace than expected, in both the public and private sectors. Data derived from the 2024 "NOKIOS" survey show that the use of artificial intelligence remains at an early stage, despite high expectations for its future application.[12]

In 2025, Norway is witnessing notable progress in artificial intelligence applications within the public sector, with a focus on responsible innovation and sustainable infrastructure. The following are the most prominent leading government projects and initiatives in this field:

1. "Stargate Norway" Project – An Advanced Artificial Intelligence Data Center

Companies Aker and Nscale announced plans to build an advanced data center in the Narvik region in northern Norway, in partnership with OpenAI. The project, named "Stargate Norway," aims to establish Europe's first "AI factory," equipped with 100,000 NVIDIA processors and powered entirely by renewable energy. This project is expected to enhance Norway's capacity to develop advanced artificial intelligence models, including defense and security applications, within the framework of cooperation with NATO.[13]

2. KI-Norge: The National Coordination Center for Artificial Intelligence

[11] Key Data & Cybersecurity Laws, Key Data & Cybersecurity Laws | Norway | Global Data and Cyber Handbook | Baker McKenzie Resource Hub.

[12] Anvendelse av kunstig intelligens (KI) i Norge i norsk offentlig sektor 2024, [2412.19273] Anvendelse av kunstig intelligens (KI) i Norge i norsk offentlig sektor 2024

[13] Røkkes datasenter kan bli Natos nye AI-våpen, Røkkes datasenter kan bli Natos nye AI-våpen – E24

“KI-Norge” (Norwegian Artificial Intelligence) was established under the supervision of the Norwegian Digitalisation Agency (Digdir) as a national platform aimed at promoting the responsible use of artificial intelligence. The project includes an “AI Sandbox” that allows government institutions and small and medium-sized enterprises to test artificial intelligence solutions in a safe and controlled environment, thereby fostering innovation while ensuring compliance with legal and ethical standards.[14]

3. Support for Research and Development in Artificial Intelligence

Norway allocated funding of NOK 62 million (EUR 6.2 million) to support doctoral projects in the public and industrial sectors in the field of artificial intelligence for the year 2025. This initiative aims to enhance cooperation between universities and government institutions to develop innovative solutions in areas such as healthcare, public administration, and energy.[15]

4. Artificial Intelligence Applications in the Healthcare Sector

The healthcare sector in Norway is considered a pioneer in adopting artificial intelligence technologies, which are used in medical data analysis, improving disease diagnosis, and personalizing treatments. These applications are implemented through cooperation between public hospitals, universities, and technology companies, contributing to improved quality and efficiency of healthcare services.[16]

E. Norway’s Digital Strategy 2024–2030

Norway’s Digital Strategy aims to make the country the most digitalized in the world by 2030. The strategy focuses on enhancing the use of artificial intelligence in public administration, improving digital

[14] AI in Norway: Innovation, KI-Norge, and Compliance in 2025, Norway AI 2025: KINorge & Responsible Compliance | Nemko Digital

[15] The Artificial Intelligence Initiative, The Artificial Intelligence Initiative

[16] Artificial Intelligence 2025, Artificial Intelligence 2025 - Norway | Global Practice Guides | Chambers and Partners

infrastructure, and ensuring the protection of personal data. Initiatives include the development of fast and secure communication networks and facilitating data sharing across different sectors.[17] Through these projects and initiatives, Norway seeks to strengthen its position as a leading hub in artificial intelligence, with an emphasis on responsible innovation, sustainability, and privacy protection.

F. Norway's National Artificial Intelligence Strategy 2025

The Norwegian government announced a national strategy aimed at promoting the use of artificial intelligence in priority areas, including public administration. The strategy includes encouraging government entities to implement pilot projects to gain experience and better understand the technology. These pilot projects are considered an important step toward assessing the effectiveness of artificial intelligence in improving government services.[18]

G. National Research Centers in Artificial Intelligence

Norway has launched six specialized research centers in artificial intelligence, with government support amounting to NOK 1 billion, aimed at strengthening education and research in this field. Among these centers are:

- **AI Learn Center:** Focuses on enhancing human learning through artificial intelligence and includes the training of 16 doctoral researchers.

- **TRUST Institute:** Aims to develop trustworthy and secure artificial intelligence systems and works on capacity building in research environments and increasing societal competence in this field.[19]

[17] Norway's Digital Priorities, Norway's Digital Priorities

[18] The National Strategy for Artificial Intelligence, The National Strategy for Artificial Intelligence - regjeringen.no

[19] TRUST is one of six new research centres for artificial intelligence, TRUST is one of six new research centres for artificial intelligence - Department of Geosciences

- **KI-Norge National Artificial Intelligence Platform:** KI-Norge (Norwegian Artificial Intelligence) was established as a national platform aimed at promoting the responsible use of artificial intelligence in education and other sectors. This initiative includes the establishment of an "AI Sandbox" to test systems in a safe environment, supporting innovation and compliance with European standards.[20]

Curriculum Development

A new government committee has been formed to oversee the integration of artificial intelligence into higher education. The committee works to provide guidance to educational institutions on how to incorporate artificial intelligence into curricula and to ensure the responsible use of technology by students.[21]

Training Programs and Educational Initiatives

A. Use of Artificial Intelligence in Primary and Secondary Education

Norway is working to integrate artificial intelligence into primary and secondary education by developing smart educational tools that help personalize learning and provide individualized support for students. This aims to improve the quality of education and ensure equal access to educational opportunities.

B. Challenges and Opportunities

Despite the progress achieved, Norway faces challenges in ensuring equal access to artificial intelligence technologies, particularly in rural areas. Nevertheless, government initiatives and educational programs offer opportunities to enhance digital competence and develop the skills necessary to keep pace with technological advancements.

[20] AI in Norway: Innovation, KI-Norge, and Compliance in 2025, op cit,

[21] Wasson and Færstad join the government's AI committee for higher education, Wasson and Færstad join the government's AI committee for higher education | News | UiB

Doctoral Projects in the Public Sector

As part of its support for research and development, Norway has allocated funding amounting to NOK 62 million to support doctoral projects in the public sector, with a focus on artificial intelligence applications. This initiative aims to strengthen cooperation between universities and government institutions to develop innovative solutions in fields such as healthcare, public administration, and energy.[22]

Conclusion

The paper affirms that artificial intelligence offers immense opportunities for societal development, while at the same time posing serious threats to digital privacy. The principal challenge lies in striking a balance between technological innovation and safeguarding individuals' digital rights. Accordingly, cooperation among legislators, companies, and civil society remains an urgent necessity to ensure a safer and more equitable digital space.

Therefore, fully harnessing artificial intelligence in Iraq requires creating a delicate balance between innovation and privacy protection. This necessitates establishing a clear legal framework, providing effective technical tools, and building strong institutional and societal capacities. Moreover, the systematic and gradual implementation of these solutions is capable of transforming potential risks into tangible economic and social opportunities.

References:

- Nadhim Hassan and Mayy Ablahad, Auditing Bias in Artificial Intelligence in Light of the Institute of Internal Auditors' Artificial Intelligence Audit Framework: A Theoretical Analytical Study, Journal of Contemporary Business and Economic Studies, Vol. 6, No. 1, 2023.

[22] The Artificial Intelligence Initiative, op cit,

- 10 Under-the-Radar AI Companies to Watch in 2026, https://www.eweek.com/news/under-the-radar-ai-companies-2026/

- AI in Norway: Innovation, KI-Norge, and Compliance in 2025, Norway AI 2025: KI Norge & Responsible Compliance | Nemko Digital.

- Anvendelse av kunstig intelligens (KI) i Norge i norsk offentlig sektor 2024, [2412.19273] Anvendelse av kunstig intelligens (KI) i Norge i norsk offentlig sektor 2024.

- Anvendelse av kunstig intelligens (KI) i Norge i norsk offentlig sektor 2024, [2412.19273] Anvendelse av kunstig intelligens (KI) i Norge i norsk offentlig sektor 2024.

- Artificial Intelligence 2025, Artificial Intelligence 2025 – Norway | Global Practice Guides | Chambers and Partners.

- Data Protection Laws in Norway, Data Protection Laws in Norway – Data Protection Laws of the World.

- Data Protection Laws in Norway, Data Protection Laws in Norway – Data Protection Laws of the World.

- Data Protection in Iraq: Limitations of Existing Laws Amid the Tech Wave, TWEJER Journal, Vol. 8, Issue 4, Nov. 2025, pp. 468–469. https://journals.soran.edu.iq/index.php/Twejer/article/view/2066/1081

- Dutch Regulator Slaps Clearview AI with $33 Million Fine and Threatens Executive Liability, The Verge.

- EU Hits Elon Musk's X with 120 Million Euro Fine for Breaching Bloc's Social Media Law, https://apnews.com/article/x-elon-musk-twitter-european-union-regulations-0a135601e050518d5aa0a0155f973177

- Key Data & Cybersecurity Laws, Norway | Global Data and Cyber Handbook | Baker McKenzie Resource Hub.

- Meta Pulls Plug on Release of Advanced AI Model in EU, The Guardian.

- Norway's Digital Priorities, Norway's Digital Priorities.

- Røkkes Datasenter Kan Bli Natos Nye AI-Våpen, E24.

- The Artificial Intelligence Initiative, The Artificial Intelligence Initiative.

- The National Strategy for Artificial Intelligence, The National Strategy for Artificial Intelligence – regjeringen.no.

- TRUST Is One of Six New Research Centres for Artificial Intelligence, Department of Geosciences.

- Wasson and Færstad Join the Government's AI Committee for Higher Education, News | UiB.

For an Active state
and a participating society

www.bayancenter.org
info@bayancenter.org