International Journal of Law Research and Studies (IJLRS)
Vol. (5), No. (2)
IJLRS
February 2026
المجلة الدولية للبحوث والدراسات القانونية
الإصدار (5)، العدد (2)

Artificial Intelligence between Innovation Imperatives and Regulatory Controls: An Analytical Study in Digital Content Management

Mohammed Hassan Kahat
Dr., College of Law, University of Kerbala, Iraq
mohammed.h.kahat@uokerbala.edu.iq

Abstract

This research handles legal and regulatory challenges arising from artificial intelligence integration. The main problem is the tension between technological innovation and fundamental rights. The research objects to illustrate multidimensional implications, focusing on legislative gaps, algorithmic bias, and digital content management. It adopts a comparative analytical approach. The originality of this research lies in its highlight on the Iraqi and Arab realities as a model for developing countries facing the global digital divide. Whereas proposing accountability structures that cover the entire artificial intelligence system life cycle. The research proves that ensuring democratic control requires building effective legislative and regulatory frameworks.

Keywords: Artificial Intelligence, Human Rights, Digital Content Management, Algorithmic Bias, Generative Models, Digital Democracy.

1. Introduction

Democratic decision-making and social communication processes are now digital, taking place in electronic spaces governed by algorithmic rules and practices that follow privately owned platforms. In contrast to traditional public spaces, which are subject to laws established and enforced by states. Digital environments are essentially managed by private actors who define and implement communication rules via content control systems and formatting algorithms. These platforms are increasingly relying on artificial intelligence to automate their operations. Their impact on public discourse and democratic practices is increasing, and the integrity of information ecosystems is becoming hostage to the extent of transparency and accountability achieved in these systems (Pasquinelli, 2023, p. 46).

There is no single agreed definition of artificial intelligence. Still, modern definitions focus on the functional capabilities of systems based on machine learning algorithms without the claim of simulating human intelligence. The artificial intelligence law of the European Union (2024) defines artificial intelligence systems as machine-based systems, designed to operate with varying levels of autonomy. They can infer how to generate outputs such as predictions, content, or recommendations that may affect physical or virtual environments (Samoili et al., 2020, p. 7). Although the monopolistic nature of such systems often obscures their technical details. However, the use of the term "artificial intelligence" has become widespread in research, popular and official discourses alike.

Generative artificial intelligence in particular large language models has gained worldwide attention since the launch of ChatGPT in November 2022. Trained on large datasets, these models were able to synthesise content in multiple formats, including text, images, and videos. So that it is difficult to distinguish it from the content produced by humans (Bonfanti, 2020, p. 2). They are actually used in the production and supervision of content, as well as in the production of fake content of various kinds and in the dissemination and combating of disinformation, which poses both challenges and opportunities.

The reality is that with the increasing realism of deep fakes, however, the process of detecting them has become equally difficult. What threatens the safety of information circulating in public space? The integration of AI systems into information ecosystems has affected three fundamental levels: content production, curation and consumption. Legitimate concerns are being raised about the ability of these regimes to shape public discourse in ways that may adversely affect social cohesion and democratic resilience (De Gregorio, 2023, p. 7). Also, questions about the use of artificial intelligence cannot be resolved based on technical criteria alone. Broader legal and social issues need to be addressed, such as discrimination against certain groups, and reducing the diversity of information available to the public (Milmo, 2024).

As the capabilities of artificial intelligence continue to develop and the range of its uses expands, it is expected that algorithmic supervision and regulation

mechanisms will increasingly and rapidly integrate into everyday life (Katzenbach, 2021, p. 6). This raises fundamental questions about the rule of law and the protection of the fundamental rights of individuals. While the global north is facing the challenges of technological acceleration and its complexities. The majority of the world's population is struggling with various problems of poor internet access. In addition to unequal investment in digital safety and poor infrastructure, there are low levels of technical culture (De Gregorio & Stremlau, 2023, p. 874).

The International Telecommunication Union report indicates that 2.6 billion people are still out of the digital world, and thus out of the world of artificial intelligence (Vanoli, 2024). This deprives huge numbers of people of access to information and the use of artificial intelligence tools. However, this exclusion does not protect them from "AI gaps". In contrast, individuals continue to receive algorithmically produced and reformulated information by other means without providing effective protection mechanisms against the potential risks of these algorithms (Fendji, 2024).

Research Problem

The research revolves around the structural tension between the accelerated technical development of artificial intelligence, and the inability of traditional legal frameworks to protect fundamental rights. Specifically, the challenges threaten freedom of expression, privacy, and equality. Exacerbated by the absence of effective transparency and accountability mechanisms. These serious pressures stem from accelerated technological transformations and legal voids exploited to violate personal data. To be complicated by the absence of uniform international standards. Especially in regions such as the Middle East and North Africa, which suffer from legislative obsolescence and structural deficiencies in data protection. Consequently, the research addresses the central question: How to achieve a balance between investing in artificial intelligence capabilities in digital content governance and protecting fundamental rights? However, the study proceeds from the premise that the widening gap between the pace of technological development and regulatory capacity. Poses as a structural threat to the integrity of democratic processes; therefore, the research aims at analysing existing legislative gaps. By

examining the effects of algorithmic bias and addressing the challenges of generative models. To formulate practical recommendations for regulatory frameworks that balance the promotion of innovation and the protection of rights.

Methodology

The research adopts a composite approach that integrates theoretical analysis with a comparative approach. It is based on three procedural axes: the inductive approach to building a database, and the comparative analytical approach to examine international experiences. Finally, the descriptive-analytical approach to monitoring human rights, social and political repercussions. References to the Iraqi and Arab context to illuminate the challenges of developing countries, providing a balanced analysis, that combines theoretical depth and empirical richness.

The Research Gap

A review of the literature reveals a structural deficiency in Arab Knowledge Production on the legal and organisational dimensions of artificial intelligence. The majority of studies are often limited to technical or economic aspects, ignoring implications for fundamental rights and democratic structures. Especially, in contexts with fragile regulatory frameworks. There is an acute lack of research on generative AI models and their effects on political discourse and public space. With an absence of comparative studies for locally adaptable mechanisms. This research aims to address this gap through an in-depth analysis of generative artificial intelligence challenges taking into account regional contextual particularities.

2. Literature Review

The contemporary literature on AI and digital content governance has crystallised across two overlapping research tracks: Organisational Innovation Management, Regulatory and governance frameworks, and the legal status of machine-generated content.

2.1 Artificial Intelligence and Organisational Innovation:

From an innovation management perspective, artificial intelligence is framed as a multi-purpose digital technology that reshapes corporate capabilities. Gama and

Magistretti show that the adoption of artificial intelligence by companies has a dual effect: it calls for new competencies in data governance and algorithms (enabling innovation), transforms existing processes and reveals new business models (fostering innovation) (Gama & Magistretti, 2023, p. 78). Their triple classification ("substitution, reinforcement, disclosure") reveals how AI systems automate content production processes, enhance human creativity, or extract hidden patterns from user data.

From the point of view of knowledge management, Alfi and Mousavi argue that generative models restructure the institutional knowledge cycle (creation, storage, transfer, application), but generate risks of algorithmic bias, excessive dependence on automated outputs, and erosion of human implicit experience (Alavi & Mousavi, 2024, pp. 11-12). This research confirms the correlation of digital content governance with organisational learning and accountability issues.

At the sectoral level, Wang (2025: p.3-6) documents the transformations of media industries through automation and algorithmic personalisation, with new vulnerabilities emerging: misinformation, structural bias, and ambiguity of the intellectual property of machine-generated content. Morales parallels it by documenting the widespread adoption of AI tools in digital marketing to achieve efficiency, despite challenges related to authorship and originality (Morales, 2025, p. 1109).

2.2 Legal Challenges in the Governance of Digital Content and Platforms:

The specialised literature reveals multi-level legal dilemmas in the employment of artificial intelligence in business management and digital platforms. Divino (2024: 10-13) identifies five recurring problems in automated organisational processes: the accountability gap in algorithmic decisions, algorithmic discrimination, privacy violations, unfair results, and proposes detailed governance and compliance mechanisms (Divino, 2024, p. 9). Zhang et al. (2025: 7) expand the analytical scope to the economics of platforms that find appropriate solutions to algorithmic collusion and market distortions under economic law, while advocating enhanced transparency and competitive supervision (Zhang et al., 2025, p. 130).

In the field of content moderation, Dimitrova analyses European and national legislation for automated moderation. By focusing on the structural tensions between operational efficiency, freedom of expression and due process guarantees (Dimitrova, 2022, p. 6). Experimentally, Pano and Abrejo (2025) document the erosion of public trust in automated supervision systems, as users report arbitrary control practices, weak appeal mechanisms, and operational ambiguities (p. 86). Yang proposes a technical alternative via a blockchain-based framework to protect the identity of content creators, secure data and enable transparent supervision, explaining how to employ technical architecture to achieve legal compliance (Yang, F., et al, 2024, p. 1782).

This research reveals a fundamental dichotomy: artificial intelligence drives organisational innovation, while generating complex legal dilemmas related to liability, copyright, data protection, market fairness, and user rights. Current frameworks combine technical solutions (blockchain, interpretable models), internal governance (institutional and media self-regulation), and emerging legal systems (European Digital legislation and artificial intelligence laws). However, they show persistent gaps in the legal status of machine-generated content, accountability for algorithmic supervision, and calibrating regulation to balance innovation and protection.

3. Artificial Intelligence Systems and Human Rights:

This section examines the mechanisms of the realisation of human rights in digital environments, analysing the problems of equity resulting from algorithmic bias. The importance of freedom of expression and access to information, and the protection of privacy. In light of the significant and accelerating development of artificial intelligence systems. It also addresses the effects of AI-powered information manipulation on political and civic engagement.

3.1 Technological Development under Traditional Legal Systems:

In the era of accelerated technological transformations, the human rights system is facing a fundamental test of its ability to adapt. Without compromising its fundamental foundations. While this system is founded on inherent human dignity, the digital space imposes qualitative complexities that require a review

of existing protection mechanisms. The Vienna Declaration of Human Rights (1993) affirmed the universality, indivisibility and organic interdependence of rights. Therefore, that one right cannot be promoted without another. Whereas before the Universal Declaration of Human Rights (1948) laid the normative Foundation based on common dignity, as the basis of freedom, justice and peace (OHCHR, 2014). Accordingly, in the declaration, states committed themselves to promoting universal respect for fundamental rights, considering them the common goal of all peoples. Therefore, these rights remain valid and binding in the digital age, but the real challenge lies in preserving them in practice in an environment characterised, by accelerated technological transformation.

Michelle Bachelet, former High Commissioner for Human Rights (2019), concluded that technological development does not require new human rights instruments. However, rather than a recalibration of the mechanisms of existing institutions (Bachelet, 2019). Effective protection requires constant work to adjust these mechanisms and achieve the optimal combination of interventions. This situation raises a central problem: are the current human rights frameworks flexible enough, to accommodate the emerging challenges of artificial intelligence? Or does reality reveal legislative and executive gaps that require deeper radical treatment?

This obligation to respect human rights is not limited to states, but includes all social actors. Although the levels and nature of these obligations vary. Private digital platforms have specific responsibilities under Ruggie principles guidelines on Business and Human Rights. Which obliges private entities to protect and respect these rights and contribute to the Prevention of violations under general international supervision (Ruggie, 2011, p. 235). Also, International human rights law imposes three obligations on states: to respect, protect, and ensure the enjoyment of rights to everyone under their jurisdiction or control. However, in the absence of explicit legal regulation, these obligations are not necessarily binding or applied to the same extent across different actors.

Digital platforms adopt a rights discourse in presenting themselves, speaking of" giving people a voice "or" protecting freedom of expression". Jørgensen (2017) notes that academic research has focused unevenly on governments 'human rights

violations, ignoring how the business models of these platforms harm users' rights (p. 280). This disparity reflects a gap in understanding the emerging digital power dynamics. Large tech companies have an unprecedented ability to influence the individual rights and freedoms of citizens. As companies continue to hesitate to adhere to transparent and substantive standards. Therefore, regional and national approaches are emerging to apply human rights obligations directly on digital platforms and social media.

The EU Digital Strategy represents the first comprehensive regulatory model aimed at limiting the influence of digital giants. Through imposing obligations that limit the negative effects of electronic communication. It promotes the realisation of fundamental rights, as reflected in the law on digital services and content regulation rules. Therefore, the EU has emerged as an international normative actor in the digital environment through what is known as the "Brussels effect". To exceed its organisational standards and geographical limits. Modern legislation, including the Artificial Intelligence Law (2024). Includes various objective obligations, but its main weight revolves around strict requirements for transparency and compliance (Bradford, 2020, pp. 14-15).

At the international level, the United Nations initiatives, including the General Assembly resolution (March 2024) on artificial intelligence. Reflect a growing awareness of the role of technology in bringing about radical transformations and providing opportunities, for building bridges within countries. The resolution emphasises the need to strengthen reliable artificial intelligence systems. These contribute to achieving sustainable development globally. Consistent with existing human rights obligations. By September 2024, artificial intelligence systems were included among the frontier technologies in the UN Global Digital Compact (EC, 2024). As a tool to accelerate development, emphasizing the need for a comprehensive, balanced approach based on risk assessment in the governance of artificial intelligence. But a central question arises. Are these emerging regulatory frameworks, regionally and internationally, sufficient to ensure that human rights are actually respected in the face of the rising power of digital platforms? To what extent can these standards be applied in contexts that lack effective legislative and regulatory structures?

This requirement, a balance between technical innovation and regulatory controls requires an integrated approach based on key axes. First, to ensure the continuity of digital access, especially at critical times (Elections, protests) to protect freedom of expression, the flow of information and access to it by the public. Secondly, building clear and progressive legal frameworks that impose appropriate obligations on the extent of digital platforms and the nature of their services. In addition, companies based on the export of these technologies are required to undergo due diligence and submit periodic reports, on their effects on human rights. Thirdly, the imposition of transparency standards on the mechanisms of algorithms. Especially to counter technically generated algorithmic disinformation. By obliging platforms to tag artificial content and conduct independent assessments of its effects. Finally, investing in digital education and supporting independent media, to build communities capable of critical discrimination and identifying misinformation. Which is strengthens the community's immunity against the dangers of the contemporary digital environment.

3.2 Algorithmic Bias:

Algorithmic bias is defined as patterns that represent systematic errors in artificial intelligence systems, which lead to unfair results. Therefore, this prejudice is understood as unfairness, as an unjustified preference for one group at the expense of another. When these systems are used to make automated decisions that affect the rights of individuals or groups. In this case, they may produce unfair and non-transparent outputs. Sometimes they are aggravated by economic incentives that are biased in favour of corporate interests (Eubanks, 2018, p. 4).

For instance, in the field of employment, law enforcement, and credit granting, algorithmic decisions may negatively and disproportionately affect marginalised communities. Contributing to their exclusion from democratic participation or depriving them of the full enjoyment of their rights (Baecker et al., 2023, p. 7). Studies from the global North and South document how algorithmic bias leads to security decisions. That excessively punishes minority ethnic groups and immigrant communities. Belenguer (2022) identifies the factors of the emergence of biases: how the system is developed and who develops it. The institutional

environment underlying it, and in particular the nature of the training data used (p. 779). That is when the learning data imposed by AI applications is incomplete or saturated with preconceptions. Otherwise, the historical patterns of system reproduction are the same deviations in its research contexts and outputs.

It employs artificial intelligence algorithms to model the behavior of users, and then uses these models in ways biased in favor of platforms, by promoting the most interactive content even at the expense of the quality or reliability of information (Polissino & De Gregorio, 2022, P.15). In other words, algorithms are now power tools that mediate decision-making, as they can process data and make decisions that affect individuals independently of public interests, increasing the risks related to discrimination and lack of accountability (Mittelstadt et al., 2016, p. 1).

These results emerge from the large system language models work, which synthesises training data to produce a single output. Based on the most common statistical patterns, which reduces the variety of inputs to one specific answer. Moreover, such models may be trained on synthetic data simulating experimental observations, without direct matching to real-world realities. Despite the usefulness of the critical evaluation of this type of data. In protecting privacy and addressing some forms of bias, by their production, the artificial neural networks do not necessarily provide a clear explanation of the reasons for generating a specific output (Offenhuber, 2024, p. 2).

The concept of Algorithmic Justice refers to the quest to design and implement artificial intelligence systems. That do not discriminate between individuals or groups based on protected characteristics, such as race, gender, or ethnicity. Ferrara (2024) explains that fair algorithms are supposed to make their decisions without unjustified preference for one individual or group at the expense of another (p.4). However, the rapid progress in AI technologies, despite its benefits, has revealed serious risks related to algorithmic bias. Which is may perpetuate and even multiply existing patterns of inequality. It could lead to discrimination against marginalised groups and limit their access to basic services. This bias also contributes to the reproduction of gender stereotypes and discrimination based on skin (color, ethnicity, or physical appearance). Undermining societal trust in

these technologies and posing ethical problems related to accountability, justice, and human agency. Thus, ensuring the fairness of AI systems requires identifying and addressing sources of bias. In addition to, developing ethical and regulatory frameworks that promote the principles of fairness, transparency and accountability in the design and use of such systems.

- **Proposed Solutions To Counter Algorithmic Bias:**

  Current efforts are directed towards improving the quality of training data as a key input for reducing algorithmic bias. In this context, IBM has launched the Diversity in Faces dataset, to address some patterns of bias in facial recognition technologies (Smith, 2019). This collection includes a million photos of human faces, with various attributes attached, such as age, gender and skin colour. These are taken from different countries and cultures, providing a wider representation of human diversity. It helps to train systems that are less inclined to reproduce stereotypes. However, this approach assumes that increased diversity in the data will automatically reduce bias. However, this is an assumption that remains limited in contexts with a lack of diverse data.

  Equity challenges are multiplying as AI becomes increasingly integrated into processes that contribute to shaping social meaning, particularly in contexts where algorithms delegate decision-making tasks. This is clearly evident in the criminal justice sector; in 2016, ProPublica revealed the bias of the (COMPAS) algorithm used in the US judicial system. Classifying black defendants as more dangerous compared to whites in similar circumstances (Pfeiffer et al., 2023, p. 210). This example shows that discrimination is no longer the preserve of human decision-making, but is embedded in machine learning systems, that learn from biased historical data. As the use of these systems expands in multiple areas, the risks of systematic discrimination and its effects on individuals and society are increasing. By making Algorithmic Justice a prerequisite for reducing these deviations.

  Besides, the diversity of development teams is an important factor in exposing invisible biases within homogeneous teams. Microsoft has embraced this trend through its Inclusive Design initiative. Through involving people from diverse

backgrounds, including people with disabilities, in product design and testing (Microsoft, 2023, p. 15). However, some studies indicate that there is diversity of professional views. It plays a more influential role in bias reduction than morphological demographic diversity alone (Park, 2024).

3.3 Freedom of Expression and Right of Access to Information:

Freedom of expression is a pillar of democratic systems; it's guaranteed by Article 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights (ICCPR) (Khalid, 2019, p. 85). This freedom includes the adoption and expression of opinions. The transmission of information and the search for it and extends to the freedom of information in various media. In the digital environment, the exercise of freedom of expression has been reshaped by its intersection with other fundamental rights. The right to health requires access to and circulation of Health Information, and the right to education requires access to knowledge and educational resources via the internet.

Artificial intelligence systems, on which digital platforms rely to manage the flow of content and increase interaction (Gillespie, 2020, p.2), create a fundamental paradox. These applications facilitate access to communication spaces, while simultaneously controlling their content. However, this mechanism has produced a new algorithmic authority that generates a two-level effect on freedom of expression. The first level controls the possibility of publication and blocking. The second level controls presentation priorities, by highlighting particular discourses and marginalising others. This transformation is thus redefining the relationship between political power and the digital public sphere. As algorithms gradually replace traditional control mechanisms.

Information is a fundamental pillar of individual freedom, enabling individuals to make informed judgments. However, this ability is fundamentally challenged by the limited ability of citizens to evaluate content. Especially when faced with misleading or biased material. This challenge is even greater in the digital age, where the contradiction between the abundance of information and the scarcity of reliable sources makes abundance meaningless. The dilemma comes after the

alarming global decline in public confidence in the news, a decline fueled by the phenomenon of the spread of disinformation via the internet.

What we are facing today is the practice of "phishing" as a targeted subversive strategy. Which goes beyond random provocation to an effective mechanism for manipulating public opinion, by publishing provocative and misleading content. To attract the audience to sterile dialogues that drain their intellectual energy. The trolls play a pivotal role in amplifying virtual support for specific personalities or issues by artificially promoting the spread of fake content. The most dangerous thing is that this activity has turned into an industry, where political parties and companies finance teams of trolls to exploit these mechanisms. In election campaigns or for marketing gains, turning the interaction space into a planned arena for influence and disinformation (Samoilenko & Suvorova, 2023, p. 512). The focus on modifying content governance practices ignores the structural causes of social division and mistrust, that produce a sharp polarisation of public opinion. Splichal (2022) proposes to transfer attention from the imbalance of information to the concept of public merit of information. This reveals the problematic complex elements of the information sphere: visibility, accessibility, self-reflection, mediation, influence, and legitimacy of information (p.1903). By understanding the interaction of these elements in the formulation of new perceptions of the public and public space. Opens path for more vivid forms of democratic practice, it allows democracy to grow in more stable and confident information environments, away from narrow technical solutions that ignore broader political and social dynamics.

3.4 Protecting Digital Privacy:

Artificial intelligence systems pose serious challenges to privacy rights, which collect and analyse huge amounts of data to build multidimensional profiles, often without explicit consent (Forum on Information and Democracy, 2024, p. 107). For instance, Meta announced the expansion of public data collection to train its models, which prompted the authorities of the European Union and Brazil to restrict it. While the UK considered it a "legitimate interest". Data collection consents are also rarely informed, as users routinely consent without realising the implications (Abdulrauf & Dube, 2024, p. 45). It is funding

platforms from data provide an incentive to extract more, which threatens privacy. This can be countered by the strict application of data protection laws, supported by international standards such as Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights.

The training of large linguistic models (LLMs) integrates personal data into their transactions. Even if not directly memorised, enabling their inference via attacks such as model inversion or membership inference (Jagannatha, et al, 2021). However, it is based on the reflection of statistical probabilities from extensive data sets, with the added complexity of constant interaction with users. However, some Suggested solutions can deal with this matter:

Technically, differential privacy adds random noise to maintain general patterns without recognising individuals, as adopted by companies such as Apple's HomePod, Amazon Echo and Google (Zhao & Chen, 2022, p.2). Organizationally, strictly implement the GDPR, EU AI Act, and CCPA, while promoting transparency and individual control, despite their gaps (Lee, 2024, p. 132). Ethically, IEEE standards and the artificial intelligence alliance to promote human well-being (IEEE, 2019). It is clear to understand that data profiling exacerbates these risks by transforming everyday activities into AI surveillance data, requiring technical-organisational-ethical integration while promoting public awareness.

3.5 Digital Manipulation of Elections:

With the development of generative AI systems, the potential for abuse is increasing. Liu et al (2024) indicate that the "Sora" model of OpenAI and other generative systems are capable of producing high-realism video clips from short text inputs (p. 16). To increase the likelihood of producing misleading or propaganda visual materials that are difficult to distinguish from the truth. The use of artificial intelligence in political campaigns and elections raises serious concerns about transparency, accountability and the possibilities of manipulating citizens' decisions. These tools enable campaigns to target voters with unprecedented accuracy and provide the ability to spread false information. By

manipulating perceptions and amplifying divisive content. A study showed Bing Chat, which became part of "Microsoft Copilot", during the elections in Germany and Switzerland. A third of his answers to electoral questions contained factual errors: wrong dates, inaccurate candidates, or fabricated scandals (Helming, 2023).

The use of artificial intelligence to personalise content on social media platforms. It gives a great capacity to influence the choices of voters and create divisions in public opinion. What limits the skill of individuals to freely and consciously participate in public affairs? Advanced data analysis capabilities facilitate the expansion of accurate voter targeting. This may raise the levels of electoral interaction. Nevertheless, it exposes voters to hidden influence processes via overly personalised content. It may direct their opinions or dissuade them from voting (Michael, 2023).

These Challenges Require A Multidimensional Strategy:

- We must raise digital awareness and media education. This will enable citizens to assess the credibility of information and understand the mechanisms of digital manipulation.
- The development of technologies for detecting deep fakes and artificially generated content. Cross models specialise in distinguishing between original and modified content.
- Oblige digital platforms to adopt strict and transparent policies on AI-generated content. While providing effective mechanisms for reporting misleading content.
- Strengthen cooperation between governments, technology companies, research institutions and civil society organisations to protect the integrity of electoral processes.

The critical question remains: Will democracy withstand these mounting challenges, or will the increasing digital manipulation erode trust in electoral processes and undermine their political legitimacy?

4. Role of Artificial Intelligence in Content Management:

Against the backdrop of the increasing reliance on digital platforms as sources of information. Artificial intelligence systems are playing an essential role in

determining whether the content displayed to users is accurate or misleading. This section deals with two interrelated aspects: content generation and management via moderation policies (monitoring, deletion, restriction). In addition, the mechanisms governing content distribution and the limit of its spread play a significant role. Social media platforms have become focal arenas for public debate. The users draw their information, exchange thoughts and formulate political positions. Content governance systems directly influence these processes by determining the conditions for the appearance of content. Specifically, to whom it is offered and in what order, and who is excluded from the circle of vision.

4.1 Artificial Intelligence in Shaping Political Discourse:

Generative artificial intelligence models have radically transformed the production and distribution of political speech. This shift has revealed a paradox between the democratisation of access and the concentration of power. Models like ChatGPT and Midjourney have fundamentally altered the landscape of political and media content. Their ease of use has allowed political actors, election campaigns, and ordinary users to create professional-quality text, video, and audio content. This material can be published quickly and at low cost via digital platforms, thereby giving political speech an ostensibly "democratic" character. However, this superficial democracy hides a complex reality characterised by a huge concentration of power in the development centres of companies that produce AI models. The development of leading systems such as GPT-4 is based on a highly centralised structure. Consequently, OpenAI has only a few hundred employees, but it has attracted multibillion-dollar investments. The cost of one training course is estimated at about 100 million dollars. This focus is reminiscent of the concept of "technological exclusivity" (Allen & Weyl, 2024, p. 151).

It warns that the acceleration of technical progress may lead to the concentration of political and media power. In the hands of a technical elite or giant companies, undermining political pluralism and independence. The current landscape presents a paradox: on the one hand. These tools give political actors and citizens unprecedented abilities to produce and disseminate speech (democratisation of production). On the other hand, the basic infrastructures that enable this

production are concentrated in very few hands (uniqueness of control). The challenge lies in reconciling the empowerment of individuals and maintaining a fair distribution of power in the digital political sphere.

According to avoid a techno-authoritarian scenario that threatens political pluralism and democratic freedom. After the video industry was the preserve of those who possessed technical skills and expensive equipment, it became available to almost everyone. This shift has been clearly reflected in political campaigns globally, especially in the 2024 US presidential election. AI-generated content was widely used in advertising campaigns. By publishing photos and videos made to distort the image of competitors or promote specific political messages. For instance, India is the largest democracy in the world political parties have resorted in the 2024 elections to artificial intelligence technologies. This enables the production of election speeches in multiple local languages. By generating clips that demonstrate politicians addressing audiences in areas they haven't actually visited (Abdulkareem & Kareem, 2022, pp, 14-16).

Iraq and developing countries face fundamental challenges in the regulation of artificial intelligence and digital content management. As a result of weak regulatory frameworks and a lack of digital awareness, there is weakness in the technical infrastructure in most of the Arab countries. That turns digital environments into open spaces for the spread of misleading content without effective suppression. This phenomenon was evident in the recent Iraqi elections through the use of fabricated statements and altered images of mass crowds. However, this makes easy access to artificial intelligence tools possible for resource-limited campaigns to produce professional advertising content. This has reinforced polarising discourses and is fueling sectarian conflicts, through fabricated audio clips falsely attributed to officials and religious leaders (Farrugia, 2024). These problems are exacerbated by the absence of content verification mechanisms and the obsolescence of legislation on intellectual property that fails to address issues related to machine-generated content.

The danger is not limited to the ease of production, but extends to the hidden mechanisms of algorithms in the promotion and amplification of content. These systems are based on user behaviour to customise the displayed content. It is

difficult to distinguish between sincere and misleading political speeches. Moreover, these applications tend to promote more polarising attention-grabbing public content, which threatens individuals ' right to access reliable information. This dilemma is exacerbated by changing platform policies as ownership changes, as seen in X/Twitter after Elon Musk's acquisition. By reactivating blocked accounts and laying off trust and safety teams, and that keeps the final control, not society (York, 2022). These patterns are repeated internationally; for example, Brazil, Kenya, and Nigeria have seen the ease with which digital content is produced exploited to inflame political tensions and unrest to mislead voters.

These challenges require an integrated strategy through a radical modernisation of legal frameworks, to include a clear regulation of artificial intelligence applications. With the imposition of mechanisms governing the disclosure of automatically generated content and strict controls on privacy and intellectual property. By rehabilitating the capacities of regulatory bodies, establishing independent mechanisms to verify content and investing in local solutions that prioritise social justice. This approach involves the launch of comprehensive national digital literacy programmes (Bontridder & Poullet, 2021, p. 13). These programmers address the identification of algorithmic bias and the application of artificial intelligence in monitoring government behaviour. Accompanied by regional and international cooperation to formulate unified standards regulating the use of artificial intelligence in the public political sphere.

4.2 The Response of Digital Platforms to AI-generated Content:

In response to the accelerated spread of AI-generated content, major digital platforms have implemented divergent approaches to governance. While the gap between the announced policies and the actual implementation exists. However, this has revealed fundamental challenges in controlling the massive flow of manufactured content. Applications like Facebook, Twitter/X and YouTube have started to deal with the challenges posed by generative models. Yet in legal systems that do not impose clear obligations for risk assessment (Miguel & Krack, 2023). The internal rules of platforms are often blurry or applied with great unevenness. So, the main motivation for these rules ranges from fear of the

misleading effect of content to a compliance approach that focuses more on copyright and formal quality standards than on content.

The platforms' policies vary markedly; for instance, Meta (parent company of Facebook and Instagram) adopts a policy that requires tagging of digitally altered content in political contexts. While the X platform adopts a more lenient approach, it leaves the responsibility of disclosure to the users themselves (CBS News, 2023). In the same context, YouTube has imposed stricter obligations. This requires content creators to disclose the use of artificial intelligence in videos that address sensitive topics. The effectiveness of these policies remains limited, especially in developing countries, including Iraq, where platforms lack sufficient resources to monitor content in Arabic and its various dialects. They also rely on inaccurate automated algorithms or small review teams that lack the cultural and political context needed to understand local discourses.

This reality reveals a structural gap between the declared policies and the actual implementation. So that the regulatory frameworks of large platforms remain oriented towards western markets. Digital environments in developing countries are left vulnerable to the spread of misleading and politicised content without real control. This discrepancy not only reflects the limited technical and linguistic resources but also reveals the lack of political will among platforms to invest seriously in content governance outside the main markets. This dynamic both widens the digital divide and threatens access to reliable information in these regions. Thereby increasing the vulnerability of emerging democracies at risk of organised political manipulation via the digital space.

4.3 Artificial Intelligence and Political Disinformation:

International experience has revealed that the weak ability to distinguish AI-generated content from human content gives political actors ample space to exploit these technologies for disinformation and manipulation. It is increasingly important to raise awareness of artificial intelligence (AI literacy), alongside imposing explicit obligations to disclose automatically generated content or accounts managed by these systems. Especially among older and less educated groups, who show a clear limitation in distinguishing between real and

manufactured photos and videos.

In the Iraqi context, these problems are highlighted more sharply by the fragility of the digital infrastructure and the high rates of digital illiteracy. Therefore, social media is used as the main source of news and political information. The Iraqi voter, who often lacks content verification tools, becomes particularly vulnerable to disinformation campaigns designed, with artificial intelligence technologies. This was manifested in the 2025 parliamentary elections, where the disinformation spread on the platforms contributed to influencing the decisions of voters. By shaping their perceptions of candidates and political blocs (Shafaq News, 2025).

At the regional level, the Arab region suffers from a clear disparity in dealing with the challenges of artificial intelligence, in infrastructure, strategic visions and institutional capabilities. Jordan offers a model for a proactive approach via a national artificial intelligence strategy (2023-2027). It includes clear goals in raising community awareness, building skills, and developing a legislative and ethical framework (Ministry of Digital Economy and Entrepreneurship, 2022). Saudi Arabia is pursuing a more ambitious approach that combines the development of artificial intelligence and digital media education. By issuing strict legislation to Combat Information Crimes and misleading content. It seeks to strike a balance between encouraging innovation and protecting society from the risks of deep counterfeiting (Al Khawaldeh, 2025).

On the other hand, countries such as Iraq show an absence of announced strategies or clear operational plans. So, efforts remain sporadic and reactive, which weakens their ability to protect public space from digital manipulation. While Turkey is an intermediate case, the weakness of digital culture intersects with political polarisation and distrust of institutions. This creates a fertile environment for the spread of disinformation during election periods. But it is characterised by advanced research and professional discussions. Around the ethics of using artificial intelligence in the media, and by an active civil and academic community in monitoring and analysing the phenomenon (Çoban, 2025, p. 15). In many Arab countries, including Iraq, these discussions remain confined to narrow elites and do not turn to research or public policy priorities.

This extends the vulnerability of the public domain to artificial intelligence-powered disinformation tools.

Although the available evidence does not indicate widespread and systematic use of generative models. As the main tool for political disinformation campaigns globally. However, there is a clear tendency towards the intensification of such uses, which is evident. This prompted a number of technology companies to sign a voluntary agreement in early 2024 pledging to reduce the contribution of artificial intelligence to spoiling electoral processes. Although documented cases reveal that the usage of artificial intelligence in political disinformation takes multiple and evolving forms. For instance, in Russia, generative models were used to produce propaganda content in European languages, aimed at influencing public opinion in the EU countries on the war in Ukraine (Rehan, 2025). Additionally, in China, deepfake techniques have been used to produce clips showing foreign officials expressing support, for Chinese positions to modify international political discourse (Geng, 2023, p. 157).

In the Middle East, there have been cases of artificial intelligence recruitment in the context of regional conflicts. For example, in Yemen, fabricated clips of military leaders making statements they did not actually make have been published. To influence the morale of the combatants and distort the image of the parties to the conflict (AFP USA, 2023). In the same context, in Syria, altered images have been used to show unrealistic demonstrations or events to guide local and international public opinion (Khedr, 2025). In Iraq, the use of artificial intelligence in political disinformation has not reached the level of large-scale organized election campaigns.

Moreover, it is witnessing a gradual escalation in its presence and influence. There have been repeated cases of voice falsification attributed to officials or politicians. Including former prime minister Nouri al-Maliki. In the context of political crises or discussions of electoral entitlements that almost led to an armed clash. As well as modified images of mass rallies that exaggerate the volume of support for certain blocs or underestimate their competitors (Barakat, 2022). In a political environment characterised by intense competition and the willingness of some actors to exploit all available means. The risk of the development of these

sporadic uses of more complex organized campaigns increases. As the cost of technical tools decreases, effective regulatory frameworks continue to be absent.

The Iraqi copyright protection law No. 3 of 1971, as amended, does not address emerging issues related to digital content and artificial intelligence. It does not provide effective protection for journalists, writers and artists against the use of their works for model training or machine reproduction (Official Gazette of Iraq, 1971). While the United States and Europe are witnessing lawsuits against major artificial intelligence companies. Due to the use of protected materials in training without permission or compensation. In that case, Iraq remains out of this debate, leaving local journalistic and literary content vulnerable to exploitation, without protection or accountability.

Therefore, there is a weak awareness of artificial intelligence, the absence of coherent national strategies, and the willingness of some political actors to adopt advanced disinformation tools. As well as the fragility of legal frameworks for intellectual property. A dangerous system that exacerbates the vulnerability of public space in Arab countries to exploitation through generative artificial intelligence technologies. These factors make community awareness, good governance of technologies and reform of the legal framework. Inseparable interrelated conditions for protecting democratic participation from the wave of artificial intelligence-powered disinformation.

In this context, technical tools based on digital watermarks or cryptographic signatures should be accepted as means of proving the source of content and verifying its authenticity. It is also possible to take advantage of specialised technologies such as the Fake Catcher system developed by (Intel Company). Which is based on the analysis of microbial signals in videos to monitor manipulation and determine the degree of credibility of the presented material.

- Digital platforms should establish clear and transparent policies for dealing with AI-generated content, while imposing disclosure obligations on its use. Such policies should be effectively applicable in all regions, including developing countries.
- Cooperation between governments, technology companies, civil society and researchers should be strengthened to develop ethical principles and

international standards. Regarding the management of AI-generated digital content.

- Governments and institutions should invest in AI solutions that develop locally and prioritise social justice and equality.

5. Conclusion

This research revealed that generative AI systems have brought about structural transformations in the relationship between technology and the human rights system. As well as in the mechanisms of producing digital political discourse. However, AI is no longer a neutral technical tool; it has become an active force reforming the public space and defining its conditions. Furthermore, it is shaping political participation and the limits of fundamental freedoms. Nowadays, this technology has become a more complex binary that combines promising opportunities with fundamental threats to the human rights system and democratic practices. Rapid technological development has exceeded the capacity of legal systems to absorb it. Thereby creating a serious gap between technical innovation and the protection of human rights. Algorithmic bias reproduces historical discrimination patterns in more complex forms.

Fundamental questions are being asked about the balance between freedom of expression and the need to combat misleading content. Privacy violations associated with the collection and use of data in model training, therefore constitute an unprecedented challenge. However, the ability of these regimes to manipulate public opinion threatens the very essence of the democratic process. This causes citizens to shift from independent actors into passive consumers of content designed to guide their choices.

In the field of content management, generative models have made it possible to produce content for a wide range of segments of society. Nonetheless, they have opened the path to organised political disinformation and violations of intellectual property rights. The response of digital platforms has remained blurry and uneven in the absence of binding regulatory frameworks. This makes it urgent to raise awareness of artificial intelligence and to impose obligations to disclose machine-generated content.

In the Iraqi context, the research revealed a worrying reality characterised by weak regulatory frameworks, low digital awareness, and increasing political polarisation. The absence of a clear national strategy and the obsolescence of legislation reflect a noticeable lag behind countries in the region, such as Jordan and Saudi Arabia. This situation illustrates a deeper crisis in strategic planning and in the building of national consensus, alongside the absence of a culture of accountability.

This reality calls for a comprehensive response, by radically updating the laws to include clear regulation of artificial intelligence. In particular, with controls for privacy and intellectual property. Additionally, by building the capacities of regulatory bodies and establishing independent mechanisms for content verification. According to the promotion of comprehensive digital literacy programs and their integration into educational curricula, and strengthening regional and international cooperation to formulate unified standards.

In conclusion, the biggest challenge lies in balancing the potential of artificial intelligence with the protection of fundamental rights and the preservation of the democratic process. This, in turn, requires genuine political will and a national consensus that transcends divisions. Therefore, we are faced with a crucial choice: either to act now to lay the legal and institutional foundations. That ensures the responsible usage of artificial intelligence. Otherwise, to find ourselves hostage to a technology that deepens divisions and threatens the foundations of the social contract. Ultimately, a delay in meeting these challenges will only exacerbate the risks and erode the chances of building a just and sustainable digital future. Accordingly, this research emphasises the necessity for a reconsideration of artificial intelligence governance, positioning it not only as a technological challenge but also as a fundamental issue for shaping democratic resilience, social cohesion, and rights-based societal stability.

6. Recommendations

Based on the results of this research, the following recommendations stand out:

1. Governments should enact integrated national legislation to regulate artificial intelligence and data protection. By defining protected personal data and

controls on its collection and use. While requiring digital platforms to clearly mark AI-generated content in political and electoral contexts, data privacy laws, such as the General Data Protection Regulation (GDPR) in the European Union, make it more important to control AI (Sumartono et al., 2024, p. 104).

2. It should prohibit the use of artificial intelligence for mass surveillance, political manipulation, and systematic discrimination. Through facial and voice recognition models and predictive policing algorithms, technologies that harm vulnerable groups or violate the principles of justice (Anderljung et al., 2025, p. 3843).
3. The cross-border nature of AI technologies requires enhanced international cooperation to develop binding standards that comply with human rights principles. Including preventing the export of digital surveillance tools to authoritarian regimes, especially in Middle Eastern countries (Ala-Pietilä & Smuha, 2021, p. 24).
4. AI governance should be based on the principles of legality, proportionality, and accountability. This means that human rights impact assessment studies should be conducted before high-risk systems are implemented, and independent regulatory bodies should be established.
5. Large tech companies are obliged to apply international human rights standards in all their operations. They should take advantage of the ISO/IEC 42001 standard to manage AI risks and to balance innovation with responsibility (Dudley, 2024).
6. Addressing these challenges requires the launch of national programs aimed at raising digital awareness and integrating the ethics of artificial intelligence into educational curricula.
7. Finally, the study recommends the development of comprehensive national strategies based on the experiences of Jordan and Saudi Arabia. It also calls for strengthening regional cooperation to develop unified standards regulating AI-generated content in Arabic.

Bibliography

1. Pasquinelli, M. (2023). The Eye of the Master: A Social History of Artificial Intelligence. Verso Books. p, 46.
2. Samoili, S., Lopez, C. M., Gomez, G. E., De, P. G., Martinez-Plumed, F., & Delipetrev, B. (2020). AI WATCH. Defining Artificial Intelligence. European Commission, JRC EUR30117. P, 7.

3. Bonfanti, M. E. (2020). The Weaponisation of Synthetic Media: What Threat Does This Pose to National Security? Center for Security Studies (CSS) at Zürich, Elcano Royal Institute for International and Strategic Studies (Real Instituto Elcano). P, 2.
4. De Gregorio, G. (2023). The normative power of artificial intelligence. Indiana Journal of Global Legal Studies, 30(2), 55-80. https://ssrn.com/abstract=4436287.
5. Milmo, D. (2024). OpenAI putting 'shiny products' above safety, says departing researcher. The Observer, 28 May. www.theguardian.com/technology/article/2024/may/18/openai-putting-shiny-products-above-safety-says-departingresearcher.
6. Katzenbach, C. (2021). 'AI will fix this' – The technical, discursive, and political turn to AI in governing communication. Big Data & Society, 8(2), 1-8. https://doi.org/10.1177/20539517211046182. P. 6.
7. De Gregorio, G., & Stremlau, N. (2023). Inequalities and content moderation. Global Policy, 14(5), 870-879. https://doi.org/10.1111/1758-5899.13243.
8. Vanoli, C. (2024). Moving AI governance from principles to practice. ITU News, 19 April. www.itu.int/hub/2024/04/movingai-governance-from-principles-to-practice.
9. Fendji, J. L. K. E. (2024). From left behind to left out: Generative AI or the next pain of the unconnected. Harvard Data Science Review, 1-3. https://hdsr.mitpress.mit.edu/pub/jo4xfs0s/release/2.
10. Gama, F., & Magistretti, S. (2023). Artificial intelligence in innovation management: A review of innovation capabilities and a taxonomy of AI applications. Journal of Product Innovation Management. P, 78.
11. Alavi, M., Leidner, D., & Mousavi, R. (2024). Knowledge management perspective of generative artificial intelligence. Journal of the Association for Information Systems. Pp, 11-12.
12. Wang, R. (2025). Artificial intelligence and change in the media industry. Communications in Humanities Research. P, 3.
13. Morales, N. M. (2025). Adoption and usability of artificial intelligence in marketing content creation. Journal of Posthumanism. P, 1109.
14. Divino, S. (2024). Governance and compliance recommendations for artificial intelligence in business management. Nuevo Derecho. p, 9.
15. Zhang, W., an, K., Mei, H., Wu, B., & Fan, Y. (2025). Legal regulation and management innovation of artificial intelligence in the platform economy. Academic Journal of Management and Social Sciences. P, 130.
16. Dimitrova, R. (2022). Artificial intelligence in content moderation – legal challenges and EU legal framework. In 2022 10th International Scientific Conference on Computer Science (COMSCI). P, 6.
17. Bano, S., Baig, A., & Abrejo, S. (2025). Combating digital misinformation and deepfakes using artificial intelligence. Annual Methodological Archive Research Review. P, 86.
18. Yang, F., Abedin, M., Qiao, Y., & Ye, L. (2024). Toward trustworthy governance of AI-generated content. IEEE Transactions on Engineering Management. P, 1782.
19. OHCHR (Office of the United Nations High Commissioner for Human Rights). (2014). Factors that Impede Equal Political Participation and Steps to Overcome those Challenges.

www.ohchr.org/en/documents/thematic-reports/ahrc2729- factors-impede-equal-political-participation-and-steps-overcome.

20. Bachelet, M. (2019). Human rights in the digital age – Can they make a difference? OHCHR Keynote Speech. www.ohchr.org/en/speeches/2019/10/human-rights-digital-age.
21. Ruggie, J. G. (2011). Report of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises: Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework. United Nations General Assembly A/HRC/17/31. https://digitallibrary.un.org/record/705860?v=pdf. P.235.
22. Jørgensen, R. F. (2017). What platforms mean when they talk about human rights. Policy & Internet, 9(3), 280-296. https://doi.org/10.1002/poi3.152.
23. Bradford, A. (2020). The Brussels Effect: How the European Union Rules the World. Oxford University Press. pp, 14-15.
24. EC. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council 0f 13 June 2024 Laying Down Harmonised Rules on Artificial.
25. Eubanks, V. (2018). Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor. St Martin's Publishing Group. P.4
26. Baecker, C., Alabbadi, O., Yogiputra, G. P., & Tien Dung, N. (2023). Threats Provided by Artificial Intelligence that Could Disrupt the Democratic System. Scientific Paper, University of Applied Science, Brandenburg. P, 7.
27. Belenguer, L. (2022). AI bias: Exploring discriminatory algorithmic decision-making models and the application of possible machine-centric solutions adapted from the pharmaceutical industry. AI and Ethics, 2(4), 771-787. https://doi.org/10.1007/s43681-022-00138-8.
28. Pollicino, O., & De Gregorio, G. (2022). Constitutional democracy, platform powers and digital populism. Constitutional Studies, 8(1), 11-34. https://constitutionalstudies.wisc.edu/index.php/cs/article/view/87.
29. Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. Big Data & Society, 3(2). https://doi.org/10.1177/2053951716679679.
30. Offenhuber, D. (2024). Shapes and frictions of synthetic data. Big Data & Society, 11(2), 1-16. https://doi.org/10.1177/20539517241249390.
31. Ferrara, E. (2024). Fairness and bias in artificial intelligence: A brief survey of sources, impacts, and mitigation strategies. Sci, 6(1), 1-15. https://doi.org/10.3390/sci6010003.
32. Smith, J. R. (2019). IBM Research releases 'Diversity in Faces' dataset to advance study of fairness in facial recognition systems. Phys.org, 29 January. https://phys.org/news/2019-01-ibm-diversity-dataset-advance-fairness.html.
33. Pfeiffer, J., Gutschow, J., Haas, C., Möslein, F., et al. (2023). Algorithmic fairness in AI. Business & Information Systems Engineering, 65(2), 209-222. https://doi.org/10.1007/s12599-023-00787-x.
34. Microsoft. (2023). Diversity and Inclusion Report 2023: A Decade of Transparency, Commitment and Progress. P, 15.

35. Park, Y. J. (2024). Algorithmic bias, marketplaces, and diversity regulation. In Proceedings of the TPRC 2024 Conference, Washington DC. https://ssrn.com/abstract=4912448.
36. Khalid, H, H. Human Rights. Beirut: Al-Sanhuri Library, 2019. p. 85.
37. Gillespie, T. (2020). Content moderation, AI, and the question of scale. Big Data & Society, 7(2), 1-5. https://doi.org/10.1177/2053951720943234.
38. Samoilenko, S. A., & Suvorova, I. (2023). Artificial intelligence and deepfakes in strategic deception campaigns: The US and Russian experiences. In The Palgrave handbook of malicious use of AI and psychological security (pp. 507-529). Cham: Springer International Publishing.
39. Splichal, S. (2022). Datafication of Public Opinion and the Public Sphere: How Extraction Replaced Expression of Opinion. Anthem Press. P, 1903.
40. Forum on Information and Democracy. (2024). AI as a Public Good: Ensuring Democratic Control of AI in the Information Space. February. https://informationdemocracy.org/wp-content/uploads/2024/03/ID-AI-as-a-Public-Good-Feb-2024.pdf.
41. Abdulrauf, L. A., & Dube, H. (Eds) (2024). Data Privacy Law in Africa: Emerging Perspectives. Pretoria University Law Press. P, 45.
42. Jagannatha, A., Rawat, B. P. S., & Yu, H. (2021). Membership inference attack susceptibility of clinical language models. ArXiv. https://doi.org/10.48550/arXiv.2104.08305.
43. Zhao, Y., & Chen, J. (2022). A survey on differential privacy for unstructured data content. ACM Computing Surveys (CSUR), 54(10s), 1-28.
44. IEEE (Institute of Electrical and Electronics Engineers). (2019). Ethically Aligned Design: A Vision for Prioritizing Human Well-Being with Autonomous and Intelligent Systems. Version 2. https://ieeexplore.ieee.org/document/9398613.
45. Lee, J. (2024). CCPA/CPRA: Consumers bear the burden as companies bear the crown. Hastings International &Comparative Law Review, 47(2), p, 132.
46. IEEE (Institute of Electrical and Electronics Engineers). (2019). Ethically Aligned Design: A Vision for Prioritizing HumanWell-Being with Autonomous and Intelligent Systems. Version 2. https://ieeexplore.ieee.org/document/9398613.
47. Liu, Y., Zhang, K., Li, Y., Yan, Z., et al. (2024). Sora: A review on background, technology, limitations, and opportunities of large vision models. ArXiv. https://doi.org/10.48550/arXiv.2402.17177.
48. Helming, C. (2023). Microsoft's Bing Chat: A source of misinformation on elections. Algorithm Watch, 15 December. https://algorithmwatch.org/en/microsofts-bing-source-misinformation-elections.
49. Michael, A. (2023). Artificial intelligence, democracy and elections. European Parliament Briefing. www.europarl.europa.eu/RegData/etudes/BRIE/2023/751478/EPRS_BRI(2023)751478_EN.pdf.
50. Allen, D., & Weyl, E. G. (2024). The real dangers of generative AI. Journal of Democracy, 35(1), 147-162.

51. Abdulkareem, Y., & Kareem Ali, D. (2022). Fake news and disinformation in Iraqi social media platform: Representational and argumentation analysis. Journal of Education College for Women, (31). Pp, 14-16.
52. Farrugia, B. (2024, November 26). Brazil's electoral deepfake law tested as AI-generated content targeted local elections. Digital Forensic Research Lab (DFRLab). Retrieved January 6, 2026, from https://dfrlab.org/2024/11/26/brazil-election-ai-deepfakes/.
53. York, J. C. (29 October 2022). Elon Musk doesn't know what it takes to make a digital town square. MIT Technology Review, 29 October. www.technologyreview.com/2022/10/29/1062417/elon-musk-twitter-takeover-global-democracy-activists.
54. Bontridder, N., & Poullet, Y. (2021). The role of artificial intelligence in disinformation. Data & Policy, 3(e32), 1-21.
55. Miguel, R., & Krack, N. (2023). Platforms' policies on AI-manipulated and generated misinformation. EU DisinfoLab, 28 September. www.disinfo.eu/publications/platforms-policies-on-ai-manipulated-and-generated-misinformation. P, 3.
56. CBS News. (2023, November 8). To help 2024 voters, Meta to begin labeling political ads that use AI-generated imagery. CBS News. Retrieved January 6, 2026, from https://www.cbsnews.com/sanfrancisco/news/meta-label-political-ads-ai-generated-imagery-2024-election-facebook-instagram/.
57. Shafaq News. (2025, October 17). Iraq's digital battlefield: Social media shapes the 2025 elections. Retrieved January 6, 2026, from https://shafaq.com/en/Report/Iraq-s-digital-battlefield-Social-media-shapes-the-2025-elections.
58. Ministry of Digital Economy and Entrepreneurship. (2022). Jordanian Artificial Intelligence Strategy and Implementation Plan (2023–2027). Digital Watch Observatory. Retrieved January 6, 2026, from https://dig.watch/resource/jordanian-artificial-intelligence-strategy-and-implementation-plan-2023-2027.
59. Al Khawaldeh, K. (2025, October 10). Can Saudi Arabia outsmart AI deepfakes and set a global standard? Arab News. https://www.arabnews.com/node/2618372/amp.
60. Çoban, B. (2025). Use of Artificial Intelligence in Turkey's Alternative News Media. Interface-Journal of European Languages and Literatures, 26. p, 15.
61. Rehan, T. (2025, November 12). AI-driven disinformation campaigns on Twitter (X) in the Russia-Ukraine War. Irregular Warfare Initiative. Retrieved January 6, 2026, from https://irregularwarfare.org/uncategorized/ai-driven-disinformation-campaigns-on-twitter-x-in-the-russia-ukraine-war/.
62. Geng, Y. (2023). Comparing "Deepfake" Regulatory Regimes in the United States, the European Union, and China. Geo. L. Tech. Rev., 7, p, 157.
63. AFP USA. (2023, November 3). Posts falsely claim Yemen officially entered Israel-Hamas conflict. AFP Fact Check. Retrieved January 6, 2026, from https://factcheck.afp.com/doc.afp.com.33ZT7XN.
64. Khedr, F. (2025, March 11). Misinformation in Syria: Natural chaos or organised campaign? Al Jazeera Media Institute. Retrieved January 6, 2026, from https://institute.aljazeera.net/en/ajr/article/2983.

65. Barakat, B. (2022, July 20). Iraqi judiciary probes leaked audios attributed to ex-premier. Anadolu Agency. Retrieved January 6, 2026, from https://www.aa.com.tr/en/middle-east/iraqi-judiciary-probes-leaked-audios-attributed-to-ex-premier/2641200.
66. Official Gazette of Iraq. (1971). Copyright protection law with its amendments (Law No. 3 of 1971, Issue No. 1957, January 21, 1971; English translation, 2020). Ministry of Justice, Iraqi Official Gazette Department, Translation Division.
67. Sumartono, E., Harliyanto, R., Situmeang, S. M. T., Siagian, D. S., & Septaria, E. (2024). The legal implications of data privacy laws, cybersecurity regulations, and ai ethics in a digital society. The Journal of Academic Science, 1(2), 103-110.
68. Anderljung, M., Hazell, J., & von Knebel, M. (2025). Protecting society from AI misuse: When are restrictions on capabilities warranted? AI & SOCIETY, 40(5), 3841-3857.
69. Ala-Pietilä, P., & Smuha, N. A. (2021). A framework for global cooperation on artificial intelligence and its governance. In Reflections on artificial intelligence for humanity (pp. 237-265). Cham: Springer International Publishing.
70. Dudley, C (2024). The Rise of AI Governance: Unpacking ISO/IEC 42001. https://www.qualitymag.com/articles/98100-the-rise-of-ai-governance-unpacking-iso-iec-42001 [Retrieved February 4, 2026].