



كلية القانون
College of Law

Tikrit University Journal for Rights

Journal Homepage : <http://tujr.tu.edu.iq/index.php/t>

Freedom of Expression in Iraq's Digital Space: A Legal Analysis of Challenges in the Age of Artificial Intelligence

Dr. Mohammed Noori Ali

College of Law, University of Nineveh, Nineveh, Iraq.

mohammed.noori@uoninevah.edu.iq

Assist. Prof. Dr. Luqman O. Ahmed

College of Law, University of Mosul, Nineveh, Iraq

luqmanothman@uomosul.edu.iq

Article info.

Article history:

- Received 26 April 2026
- Accepted 25 May 2026
- Available online 1 June 2026

Keywords:

- Digital freedom of expression
- Artificial intelligence
- Algorithmic Regulation
- Privacy and Human Rights

Abstract: This study examines the issue of digital freedom of expression in Iraq and the potential transformations brought by the rise of artificial intelligence. AI has opened new horizons, offering exceptional opportunities to accelerate evolution and enhance the enjoyment of fundamental rights. Built upon core elements, machine learning, big data, and algorithms. Artificial intelligence has brought great benefits to humanity, but at the same time, it carries concerns that may threaten human dignity and privacy in exercising freedom of expression and opinion. It provides an explanation and analysis of how AI systems interact with the digital world and individuals' right to freedom of expression, while demonstrating that an appropriate legal framework would effectively reduce the potential risks of these interactions. After a thorough literature review, the study found that laws in Iraq could not clearly define an individual's right to freedom of expression and digital privacy. There are many gaps in the Iraqi legal framework. Many laws also enable the government to impose restrictions on the freedom of expression and digital privacy of individuals without adequate safeguards to protect them. Finally,

the study recommends that there should be a clear and well-defined regulatory framework for regulating AI systems, guaranteeing individuals their legal rights to benefit from the benefits of AI while protecting their digital rights in Iraq.

© 2023 TUJR, College of Law, Tikrit University

حرية التعبير في الفضاء الرقمي في العراق: تحليل قانوني للتحديات في عصر الذكاء الاصطناعي

م.د. محمد نوري علي

كلية القانون ، جامعة نينوى , نينوى , العراق

mohammed.noori@uoninevah.edu.iq

أ.م.د. لقمان عثمان أحمد

كلية الحقوق ، جامعة الموصل , نينوى , العراق

luqmanothman@uomosul.edu.iq

معلومات البحث :

تواريخ البحث:

- الاستلام : ٢٦ / نيسان / ٢٠٢٦

- القبول : ٢٥ / أيار / ٢٠٢٦

- النشر المباشر : ١ / حزيران / ٢٠٢٦

الكلمات المفتاحية :

- حرية التعبير الرقمية

-الذكاء الاصطناع

-التنظيم الخوارزمي

-الخصوصية والحقوق الإنسانية

الخلاصة: تبحث هذه الدراسة في إشكالية حرية التعبير الرقمية في العراق، وما قد يطرأ عليها من تحولات بفعل التطور المتسارع لتقنيات الذكاء الاصطناعي. لقد أتاح الذكاء الاصطناعي آفاقاً واسعة لتعزيز ممارسة الحقوق الأساسية، من خلال أدواته الرئيسة المتمثلة في التعلم الآلي، والبيانات الضخمة، والخوارزميات. ورغم ما يقدمه من مزايا نوعية للبشرية، فإنه يثير في المقابل مخاوف جدية تتعلق بصون الكرامة الإنسانية وحماية الخصوصية عند ممارسة حرية الرأي والتعبير. وتعرض الدراسة تحليلاً معمقاً لآليات تفاعل أنظمة الذكاء الاصطناعي مع الفضاء الرقمي وحق الأفراد في التعبير، مؤكدة أن وجود إطار قانوني متماسك من شأنه أن يحد من المخاطر المحتملة لهذه التفاعلات.

وبعد مراجعة شاملة للأدبيات القانونية ذات الصلة، تبين أن التشريعات العراقية لا توفر تعريفاً دقيقاً لحق الفرد في حرية التعبير والخصوصية الرقمية، وأن هناك ثغرات واضحة في البنية القانونية القائمة. كما أن بعض النصوص القانونية تمنح السلطات صلاحيات واسعة لفرض قيود على حرية التعبير والخصوصية الرقمية دون ضمانات كافية لحماية الأفراد. وفي ضوء ذلك، توصي الدراسة بضرورة إرساء إطار تنظيمي واضح ومحدد لتنظيم عمل أنظمة الذكاء الاصطناعي، بما يكفل للأفراد حقوقهم القانونية في الاستفادة من مزايا هذه التقنيات، مع ضمان حماية حقوقهم الرقمية في العراق.

1. Introduction

The digital environment is undergoing profound transformations due to the widespread adoption of artificial intelligence technologies, which have ceased to be merely technical tools and have instead become a central force in regulating and managing the digital public sphere—particularly with respect to content governance, digital surveillance, and discourse generation. In recent years, artificial intelligence algorithms have evolved into the primary mechanism relied upon by social media platforms for classifying and removing content.¹ This situation has created legal issues about how far you can go in terms of how free someone can express himself or herself and if the advanced technologies that are being created and deployed will create forms of censorship or impose limitations on lawful speech or create a form of “chilling effect” that would lessen governmental participation by citizens through today’s electronic media and related technologies.²

AI has an impact on digital freedom of expression in Iraq, including changes in the way a person interacts with the government and digital platforms (like Facebook). Therefore, when looking at the current legal system, it is important to determine if it meets the needs of people who want to express themselves and have their rights protected by law. It is important to note that technology is no longer the only focus of regulations on freedom of expression; instead, AI is now a key player in determining what will be publicly said about whom via algorithmic systems and determining who has access to these audiences and what information they can receive, without any type of judicial checks or balance.³

Legal scholars today are examining many dimensions of the issue of Artificial Intelligence (AI) used to moderate content from both a freedom of expression perspective as well as from the threat to free expression posed by algorithmic bias and the lack of clarity in the operation of algorithms. Research in the area of algorithmic regulation reveals that, in many instances, algorithms are capable of producing unwarranted bans or deletions of suspected illegitimate speech that violate international standards for free expression which call for clarity regarding legal norms, and due process in regard to punitive action.⁴ Another strand of this research shows that over-reliance on AI filtering of content erodes human oversight and places the function of digital corporations as “*de facto regulators*” of their respective discourses; i.e. there is a total lack of accountability and democratic legitimacy in these regimes.⁵

Comparative studies show that laws regulating digital free expression (and limiting it) should be broad and not just based on vague criminal laws, but they should include safeguards related to substance and

¹ Nouri, Z., Walid Ben Salah, & AlOmran, N. (2024). *Artificial Intelligence and Administrative Justice: An Analysis of Predictive Justice in France*. **Hasanuddin Law Review**, 10(2), 119–143. DOI: <https://doi.org/10.20956/halrev.v10i2.5541>

² Abdullah Ahmed and Mudassar Nisar Khan, *AI and Content Moderation: Legal and Ethical Approaches to Protecting Free Speech and Privacy* (unpublished paper, 2024), on the risks to free speech posed by algorithmic moderation.

³ P.V.S. Sailaja et al., “Freedom of Speech in the Digital Age: Challenges of Algorithmic Censorship and AI Moderation,” *Lex Localis: Journal of Local Self-Government* 23, no. S6 (2025). <https://doi.org/10.52152/84jfy65>

⁴ Juan Felipe Gomez et al., “Algorithmic Arbitrariness in Content Moderation,” *arXiv* (2024), analyzing arbitrariness in machine learning content classification and implications for freedom of expression. <https://doi.org/10.48550/arXiv.2402.16979>

⁵ Mansour Malekpour Bahabadi et al., “Legal Challenges of Artificial Intelligence Tools in Regulating Freedom of Expression in Iran,” *Legal Studies in Digital Age* (2025), highlighting opacity and accountability issues in AI governance.

procedure that are compatible with International standards. These safeguards include that the restrictions should be "prescribed by law," "necessary" in order to protect a legitimate interest, and "proportionate" to the goal of the restriction. Furthermore, a large part of how this balance between limiting harmful content and enabling freedom of expression to be exercised in a democracy and by all citizens will depend on national laws.¹

The conflicting interests that exist in Iraq are seen in the way that a multitude of laws (criminal and constitutional) allow for very different levels of freedom of expression than do the laws that enable the state to react to violations of the constitutional prohibition on censorship. As such, the legislature must re-evaluate existing laws regarding freedom of expression and the relevant regulatory authorities for the purposes of determining their continued applicability in an age where artificial intelligence is a growing factor.

The scholarly contribution of this research is its combination of legal analysis to assess how AI will affect the digital environment, along with a review of various recent publications related to the regulation of algorithms, the challenges of transparency, and finding the proper balance between freedom and security. By clearly identifying the focus and purpose of this research, the author has developed a better understanding of the complexity of the problem and established an effective methodology to analyze the specific provisions of Iraqi law and their compliance with the standards established by international law to ensure the protection of citizens' basic rights in an ever-evolving technological environment with increasing regulatory and technological difficulties.

2. Method

This study adopts a dual approach: it uses doctrinal legal analysis (i.e., analysis of the law in light of existing statutory provisions) as well as a qualitative empirical approach. This will produce an analysis that holds both normative and contextual weight. In other words, this study will begin by assessing Iraq's constitutional and legislative frameworks, specifically Articles 38 and 46 of Iraq's 2005 Constitution and the Cyber Crimes Law Number 17 of 2012, as well as relevant provisions in Iraq's Penal Code. The authors believe that the text of Iraq's Constitution may clearly establish that right to use social media, but the differential interpretation of the Constitution (and enforcement thereof) often results in inconsistent enforcement due to political will and institutional competency. To bridge the gap between the law and reality, the study employs an empirical approach by using verified social media usage statistics, documented accounts of online discourse trends, and documented accounts of censorship as resources to provide evidence for the legal analysis of the above documents in relation to how users and officials experience the law and how they interpret it. Additionally, this study seeks to eliminate analytical blind spots by employing a variety of sources including the aforementioned documents and resources. The framework moves through three stages: a diagnostic stage that identifies the strengths and weaknesses of Iraq's legal framework in relation to social media, an impact assessment that evaluates how artificial intelligence is changing the scope of digital expression in the world's digital landscape and a normative recommendations stage that proposes legal guidelines for establishing equitable treatment of digital users in Iraq's legal framework.

3. AI in the Digital Space: Content, Surveillance, and Generation

¹ Gaikwad Sadhana, "The Study of Right to Freedom of Expression, Digital Media Laws and Demand for Innovation," *Law and World* (2025), on the need for clear legal standards in digital expression regulation.

Over the past two decades, artificial intelligence has become one of the most important legal and technological tools of our time that has fundamentally changed the path we comprehend, interact with, and utilize the digital world; ¹AI is now a crucial part of the process of content management via social networks and websites (including but not limited to) the surveillance of content and the creation of generative discourse.² As a tool for managing digital content on social networks and websites, intelligent algorithms have developed a method for monitoring and managing the presence of digital content on social networks and on web pages. As such, they allow for quick detection and removal of damaging or unlawful/dangerous content (i.e., hate speech, incitement to violence). This is intended to promote public safety, but it also raises questions about the limits of free expression, whether private companies may legitimately intervene in the regulating of public discourse and, if so, to what extent they must act under the principles of justice, transparency, and accountability.³

Artificial intelligence has increased the ability of states and other actors to monitor electronic activity and process large volumes of data through enhanced methods enabled by digital surveillance. These developments include new ways of utilizing machine learning and natural language processing technologies to watch how information is shared through electronic means and the behavior of users based on the tracking of their activities over time, including both private communications sent between individuals and items published publicly by those users. While these technologies have been used primarily for purposes of National Security (e.g., fighting terrorism and cybercrime), they raise considerable concerns about violations of digital privacy, government exceeding its authority under the principle of proportionality, and an impending threat of mass surveillance that could undermine the legitimacy of democratic government.⁴

Artificial intelligence has opened up a world of opportunities through generative discourse by allowing us access to unlimited text/images/sound/video production through advanced linguistic/generative modelling capabilities. This new ability to create new content has positive implications for education, media, and creativity in the arts; however, it has also raised a number of complex legal challenges regarding automated systems' responsibility for distributing false information or content that violates another party's intellectual property rights. Additionally, it has created a risk of manipulating public opinion via "synthetic content," which is becoming increasingly indistinguishable from normal human-created discourse.⁵

For these reasons, and as a consequence of the growing importance of AI and machine learning in numerous sectors, governments must develop balanced, comprehensive legal frameworks to ensure the protection of fundamental freedoms⁶ (e.g., freedom of Expression, right to Privacy) as well as provide the tools necessary for national governments to address threats to national security (e.g., cybercrime). Thus, comprehensive legal responses should be predicated on the principles of Transparency,

¹ Wordtune. "How AI Can Help Marketers with Personalization." Wordtune Blog. Accessed January 20, 2026. <https://www.wordtune.com/blog/ai-for-personalization>.

² Robert Gorwa, Reuben Binns, and Christian Katzenbach. "Algorithmic Content Moderation: Technical and Political Challenges in the Automation of Platform Governance." *Big Data & Society* 7, no. 1 (2020): 1–15. <https://doi.org/10.1177/2053951720923232>.

³ Tarleton Gillespie, "Content Moderation, AI, and the Question of Scale," *Social Media + Society* 6, no. 2 (2020): 1–5, <https://doi.org/10.1177/2056305120938614>.

⁴ David Lyon, "Surveillance, Big Data, and Democracy: The Paradoxes of Power," *International Journal of Communication* 8 (2014): 2061–2079.

⁵ Jan Kietzmann, Ian McCarthy, and Leyland Pitt, "Deepfakes: Trick or Treat?," *Business Horizons* 63, no. 2 (2020): 135–146, <https://doi.org/10.1016/j.bushor.2019.11.006>.

⁶ Rakesh, K. S., and S. Yadav, "To Analyze the Effectiveness of Mitigation Strategies Aimed Against Distributed Network Systems." *International Journal of Computing Programming and Database Management*, 2025. <https://doi.org/10.33545/27076636.2025.v6.i1a.107>.

Accountability, and Judicial Oversight, and the development of strong international partnerships to create a regulatory model for AI technologies in the Digital Sector. The regulation of AI technologies is not merely a technology issue; rather, it is about redefining the boundaries of public discourse in a world where Algorithms dictate how we interact with one another (vision, communication, participation).¹

4. Law, Technology, and Fundamental Rights in the Age of AI

Artificial Intelligence has become one of the most important representations of the intersection between laws and technologies in modern society. AI is not merely a tool of technology today; it has also evolved into a critical factor that can both help establish fundamental human rights and ensure that these rights are exercised or limited. Artificial intelligence contributes to the improvement of some fundamental rights (the right to receive information, the right to education, and the right to have access to health services) in the areas of providing and making available applications of big data and statistical analysis, early diagnosis of medical conditions, and creating advanced digital educational tools. These applications provide an extension of the law in a positive manner by protecting human beings and allowing them to exercise their rights in an efficient manner.²

However, there are serious legal implications to consider with AI. For example, People could violate your right to privacy if they were monitored or collected data from you without your consent on a large scale (mass surveillance). Also, censorship of free speech could be increased through content management systems or software built according to vague algorithmic processes retracting (removing or blocking) forms of digital speech created by users.³

This relationship between law and technology has to have a balanced regulatory system, based on the principles of accountability, transparency, responsibility, and judicial oversight to ensure that technological developments continue to adhere to human rights standards. Laws should be proactive in relation to advancements in technology while also creating novel methods for protecting against the misuse of these technologies within our society including, but not limited to, the protection of the fundamental principles of human rights and creating legitimacy in democratic governance through continued adherence to the rule of law.⁴

Artificial intelligence has thus presented what is probably a true test of the ability of legal systems to adapt to the rapidly changing digital environment. In addition to creating potential new pathways for providing legal justice, artificial intelligence presents difficult and complicated issues that require prudent and effective management in order to find an appropriate balance on the trilateral axis of civil liberties, public safety, and technological advancement.⁵

Freedom of expression is ensured by international instruments and national constitutions. The Universal Declaration of Human Rights states in Article 19 that "people have the right to freedom of opinion

¹ Karen Yeung, "A Study of the Implications of Advanced Digital Technologies (Including AI Systems) for the Concept of Responsibility within a Human Rights Framework," *Modern Law Review* 82, no. 2 (2019): 193–220, <https://doi.org/10.1111/1468-2230.12435>.

² Mireille Hildebrandt, "Law as Computation in the Era of Artificial Legal Intelligence: Speaking Law to the Power of Statistics," *University of Toronto Law Journal* 68, no. 1 (2018): 12–35, <https://doi.org/10.3138/utlj.2017-0044>.

³ Brent Mittelstadt et al., "The Ethics of Algorithms: Mapping the Debate," *Big Data & Society* 3, no. 2 (2016): 1–21, <https://doi.org/10.1177/2053951716679679>.

⁴ Sandra Wachter, Brent Mittelstadt, and Chris Russell, "Bias Preservation in Machine Learning: The Legality of Fairness Metrics under EU Non-Discrimination Law," *West Virginia Law Review* 123, no. 3 (2021): 735–768.

⁵ Karen Yeung, "Algorithmic Regulation: A Critical Interrogation," *Regulation & Governance* 12, no. 4 (2018): 505–523, <https://doi.org/10.1111/rego.12158>.

and expression." In the midst of the accelerating digital revolution and the emergence of artificial intelligence technologies, the digital sphere has become a principal arena for the exercise of this right, thereby imposing new legal and regulatory challenges upon states, including Iraq. ¹In the midst of the accelerating digital revolution and the emergence of artificial intelligence technologies, the digital sphere has become a principal arena for the exercise of this right, thereby imposing new legal and regulatory challenges upon states, including Iraq.

The challenges of regulating Iraq's freedom of expression in the digital world and AI raise the need to protect this basic human right while focusing on the necessity to protect against harmful information and ensure national security and protect cultural and religious values.² This is complicated further by the explosion of artificial intelligence devices that can create false or misleading content or alter information and can also violate people's privacy.³

5. Statistical Data on Social Media Users in Iraq and Digital Freedom of Expression

The Digital Media Centre's (DMC) (an organization that publishes and analyzes data related to Digital Media and their use) report dated March 3, 2025 indicates that Iraq has 34.3 million users on social media. These users represent 73.8% of Iraq's entire population. The total number of social media users in Iraq rose from 31.95 million to 34.3 million in one year (2015). This statistic comes from the reports of international organizations that track digital data usage and trends, including Meltwater and We Are Social, and highlights the rapid increase in the number of people using online platforms to participate in civic life.

The data provides evidence of considerable changes in how users engage with various social media channels. TikTok has seen remarkable growth and has attracted a significant audience as evidenced by its addition of 2.35 million new users which represents how popular TikTok is becoming with many types of audiences including but not limited to the youth, social media influencers, and content creators. In comparison, YouTube has had a slight decline in users therefore indicating a shift away from long-form content to more brief and interactive video formats. LinkedIn's growth was slightly less impressive than TikTok's but still impressive in the sense that their user growth has gone from 1.9 million to 2.3 million purely based on the growth in interest in using LinkedIn as a way to build relationships within one's professional field and find jobs via the Internet.

Various other platforms experienced a wide variety of trends. At the time of writing, the number of users using Facebook was approximately 20.1 million and 19 million for Instagram, and roughly 18.5 million for Snapchat. In contrast, the number of users using Facebook Messenger had decreased to 15 million, down from 15.7 million users, while the user count on X (formerly Twitter) reached approximately 2.65 million users. The numbers above indicate that Iraq's digital environment is in a state of flux and, as such, it has become the most extensive platform available for the expression of opinions and the exchange of information.

¹ Frank Pasquale, "A Rule of Persons, Not Machines: The Limits of Legal Automation," *George Washington Law Review* 87, no. 1 (2019): 1–40.

² Al-Hamdan, Sabbar Razzaq Sajit, and Elham Heydari. 2025. "The Legal Framework for Cybersecurity in Iraq: An Analytical Study Based on National Laws and International Standards." *Basra Studies Journal* 2, no. 62 (September 15): 89–114. <https://doi.org/10.XXXX/bsj.V2.62.347>.

³ David Kaye, "Speech Police: The Global Struggle to Govern the Internet," *International Journal of Communication* 13 (2019): 4221–4238.

So, it's an analytical base for following-up on the current level of digital expression and freedom within Iraq. Although, these statistics will not simply be a technical data-type figure — they will establish the legal foundation for evaluating where things stand today; in other words, these statistics will guide us in performing our evaluation of Iraq's right to reasonable digital expression.. They also provide a basis for measuring the need to develop specific legislation on digital rights and artificial intelligence, thereby achieving a balance between liberty and security, and reinforcing constitutional legitimacy within the digital environment.¹

6. The Constitutional and Legal Framework of Digital Freedom of Expression in Iraq

6.1. Constitutional Protection of Freedom of Expression

Iraq's new constitution that was adopted in 2005 establishes freedom of speech as a key pillar of democracy. However, limits on freedom of speech based upon maintaining public order and morality are part of the Constitution. This does not represent an exception to freedom of speech; it is the dialectical relationship between the ideals of a constitution and the need for control by the Iraqi government to maintain social stability and political safety. At one time, and in many respects, the Constitution states that individuals will have equal rights to exercise their freedom of speech through the lens of their culture and how it views a person's role in society. The Constitution acknowledges the existence of cultural variations in terms of how people think, act and speak about political matters but maintains an obligation on the part of citizens and the government to express opinions that are safe for society as a whole.²

The means of restricting rights must strictly conform with legislation in a manner that does not diminish what defines the core "essence" of that right. This represents a compromise between personal freedom and the rule of law. Precisely defining what represents the "essence" of any one right leaves room for a great deal of flexibility in interpreting such "essences" for both legislative and judiciary bodies. In reality, much flexibility will result in courts and legislatures from defining constitutional protections as contingent instead of existing as a constitutional right that is subject to political or social fluctuations.³

Based on a comparative analysis of constitutional frameworks in Iraq and elsewhere within a common regional context, the study observed a clear pattern emerging. The Egyptian Constitution (2014) protects the right to freedom of thought and expression; however, it allows for limitations based on "the national security" and "the public order."⁴ In a like manner, following its 2011 amendment, the Jordanian Constitution preserves freedoms of press and opinion while conditioning those freedoms on

¹ Digital Media Center (DMC), “34 Million Social Media Users in Iraq in 2025”, published on the Digital Media Center website, March 4, 2025, <https://dmc-iq.com/2025/03/04/٢٠٢٥-عام-العراق-الاجتماعي-في-الرقم-٣٤-مليون-مستخدم-لمواقع-التواصل-الاجتماعي-في-العراق>.

² Iraqi Constitution (2005), Art. 38

³ Iraqi Constitution (2005), Art. 46.

⁴ Constitution of Egypt (2014), Art. 65.

compliance with applicable statutes.¹ Tunisia's Constitution (2014)² is the most analogous to the textual structure of Iraq's; although it emphasizes the need for restrictions on the core right of Freedom of Thought and Expression, Tunisia's constitution provides for greater judicial oversight over how the courts or any other government entity can limit these rights, which indicates a relationship similar to Iraq's with regard to this constitutional standard (fragile balance). The current (2011) Constitution of Morocco guarantees free forms of expression; however, it subordinates that freedom to the country's cultural and normative values and presents yet another example of the way that legal and identity standards interact.³

The Constitutional framework analysed here highlights the tension that exists when applying principles of freedom of expression to the digital realm, and in particular, how that tension becomes heightened through the rapid growth of Artificial Intelligence. The Constitution of Iraq and those throughout the region contain provisions that grant and protect freedom of expression. However, these protections, being subject to "public order", "morals", and "rules of law", raise significant concerns about how these provisions will be interpreted in the realities of the Algorithmic Age. Digital Expressions facilitate the creation, dissemination and dialogue of ideas, thoughts, and opinions via various Media Channels. Digital expression also illustrates the dual capabilities offered by constitutional protections; AI provides expanded access to and amplification of information; however, AI also has a propensity to create invisible methods of control that may limit expression more broadly than traditional laws do. The challenge will be to create safeguards that embody constitutional protections and adequately reflect the current challenges we face as Technology continues to change the way we communicate, and to create the ability to think critically about the societal norms and processes that are embedded in AI systems that are/will be designed to influence the expression of ideas.

On the other hand, freedom of digital expression in Iraq has been enshrined in some decisions of the Federal Supreme Court, for instance. The decision of the Federal Supreme Court in Iraq clearly illustrates this problem, as it gave constitutional legitimacy to penal provisions restricting freedom of expression (articles 81 and 84 of the Iraqi Penal Code) by simply referring to the condition of not disturbing public order, without defining this condition or setting a standard for measuring it, which weakens effective constitutional control over the limits of freedom of expression in the digital space.⁴

In another decision of the Federal Supreme Court, when the Court enshrined this approach more deeply. She stressed that the concept of public order and public morals varies according to time and place, and that the judiciary decides it, which means in practice that the limits of freedom of expression in the digital space in Iraq are variable and unpredictable. There is no fixed objective criterion for knowing the limits of this freedom. In the age of artificial intelligence, the danger of this ambiguity is doubled, as algorithms make deletion and blocking decisions based on their own criteria, in the complete absence of any explicit legal definition of public order in the context of the digital space that restricts or controls these decisions⁵

The study observed that Article 38 of the Constitution of the Republic of Iraq of 2005 can be interpreted in a way that imposes an affirmative obligation on the state to protect in order to ensure that the artificial intelligence systems used in content management are in line with this constitutional guarantee. At the same time, this article suffers from a very important deficiency in dealing with freedom of expression in the digital space in terms of the lack of a precise and clear definition of the concept of "public order"

¹ Constitution of Jordan (1952, as amended 2011), Art. 15.

² Constitution of Tunisia (2014), Art. 31.

³ Constitution of Morocco (2011), Art. 25.

⁴ Iraq, Federal Supreme Court, Decision No. 46/2011 (August 22, 2011).

⁵ Iraq, Federal Supreme Court, Decision No. 63/2012 (October 11, 2012).

in the context of the digital space, which makes it open to algorithmic and executive interpretation. It does not explicitly require proof that any restriction on freedom of expression must be necessary and proportionate to the intended purpose, and this is contrary to the requirements of article 19 of the International Covenant on Civil and Political Rights (ICCPR), which Iraq has ratified. The legality of any restriction requires the existence of three criteria: legality, necessity and proportionality.

The study also found that Articles 38 and 46 of the Constitution of the Republic of Iraq of 2005 represent the constitutional framework regulating freedom of expression, as the former guarantees this right by all means, while the latter permits its restriction by law or based on a law, provided that this restriction does not affect the essence of this freedom. However, the area between the two articles represented by the limits of legitimate restriction constitutes one of the most prominent constitutional problems in the digital space. Especially with the escalating role of artificial intelligence and algorithms in curating and managing digital content. While not keeping pace with the rapid developments in this field, the development of clear digital constitutional controls to define precise criteria of necessity and proportionality commensurate with these developments in the digital space, as well as judicial oversight of digital restrictions. This widens the scope for interference with freedom of expression in a way that may in practice weaken the constitutional guarantee guaranteed by Article 38.

6.2. The Iraqi Cybercrime Draft Bill and Digital Rights

The Cybercrime Draft Bill for 2012 is arguably the most significant legislative attempt made by the Iraqi government to regulate cyberspace and prevent cybercrime from occurring—especially where technical intrusion occurs, digital fraud occurs, and/or damage occurs to national information systems. Nevertheless, although the primary purpose of the Cybercrime Draft Bill is to guarantee cybersecurity, it has been widely criticised on both legal and human rights grounds due to its vague wording which refers not only to technical illegalities but also to digital discourse and the right to free speech. For instance, Article 3 of the Cybercrime Draft Bill states that individuals who "create (a) website or (b) publish (a) piece of content...with the intent to undermine (of)(or) threaten (the) nation's internal/external security" could be punished for their act. There are no definitions for any of these outlined terms; therefore, there is much room for interpretation, and many interpretations can use this law to punish people who are exercising their right to express themselves as they feel necessary, which is particularly true in relation to expressing dissenting opinions politically or socially.¹

This legislative ambiguity stands in contradiction to the essence of digital rights, which represent a contemporary extension of fundamental rights and freedoms within the electronic environment—foremost among them freedom of expression, the right to privacy, and freedom of access to information. Digital rights aren't a new category of entitlements or invented in a vacuum without standard international and domestic regulations — they are simply an evolution of existing human rights.² Any restriction of digital rights must respect the following three principles: legality; necessity; and proportionality. According to the International Covenant on Civil and Political Rights (ICCPR),³ restrictions on freedom of expression are only lawful if they are expressly provided for in law, for a legitimate purpose, and if the restriction is necessary to achieve that purpose; thus, restrictions must be

¹ Human Rights Watch. Iraq's Cybercrime Law: Drafting Crimes and Cruel Penalties Undermine Due Process and Freedom of Expression. July 11, 2012. Accessed May 10, 2016. <https://www.hrw.org/ar/report/2012/07/11/256341>.

² Taghreed Abdulqader Ali, "Proportionality of Iraqi Draft IT Law with Constitutional Rights and Freedoms," Baghdad: House of Wisdom, Legal Studies Department, 2020, 191–216.

³ A. Kumar, "Using Courts to Enforce the Free Speech Provisions of the International Covenant on Civil and Political Rights," *Journal of International Law* 12, no. 3 (2006): 45–78.

closely aligned to the stated purpose and at the same time underpinned by a legitimate purpose.¹The UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression emphasises that blocking websites or placing limitations on digital content must only be done through an independent court decision and only to the absolute minimum extent necessary to accomplish the goal of blocking the site or limiting the content.²

Nevertheless, the Iraqi draft Cybercrime Law grants executive authorities broad powers of surveillance and blocking, and prescribes custodial penalties that may extend to lengthy prison terms. This produces a chilling effect that deters individuals from exercising their right to digital expression for fear of prosecution. International and Iraqi human rights organizations have warned that, in its current form, the law does not confine itself to combating technical crimes but rather transforms into a tool for controlling public discourse in the digital environment.³Thus, the problem does not lie in the principle of regulating cyberspace per se, but in the absence of balance between the requirements of digital security and the protection of fundamental rights.

Thus, integrating digital rights into Iraq's legal system means re-writing Iraqi law to follow the Iraqi constitution of 2005 and the standards of International Human rights. Therefore, it is necessary to define what criminal acts are being punished, limit the punishment to those technical acts that cause damage, and provide a legal system providing strict oversight of all limitations on Freedom of speech and privacy by the courts. Today, in the Age of Artificial Intelligence (AI), the law does not only cover the protection of information systems, but also provides protection for the Digital Public Sphere (i.e., where we exercise our citizenship, expression, and participation). Therefore, and to build upon constitutional legitimacy in the Digital World, it is imperative to reform and update the Cyber Laws (i.e., the laws related to computers and other digital media).

The Iraqi legislative authority must update and broaden traditional means of punishing offenders for new forms of criminal behaviour caused by rapid advances in technology used to communicate, in addition to the broadening of the way people interact with each other through cyberspace, which has expanded dramatically since the advent of the internet. Thus, to provide adequate protection to individuals in the virtual world, and to protect citizens of Iraq from this criminal behaviour, it will be necessary for the legislative authority to draft and incorporate provisions pertaining to electronic insult and defamation into a new form of cybercrime legislation.⁴

The Iraqi Penal Code No. 111 of 1969, as amended, does not contain specific provisions on electronic defamation and insult.⁵ Nevertheless, Articles (433) and (434) criminalize defamation and insult in general, and they have been interpreted in a manner that allows their application to content disseminated through electronic media, based on the broadening of the concept of publicity to include the digital sphere. The criminalization of defamation and insult constitutes one of the most significant forms of protection afforded by criminal law to personal liberty in its moral dimension; respect for human dignity

¹ International Covenant on Civil and Political Rights (ICCPR), adopted December 16, 1966, entered into force March 23, 1976, Art. 19.

² Frank La Rue, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, UN Doc. A/HRC/17/27 (2011), paras. 70–76.

³ Article 19 Organization, "Iraq: The draft cybercrime law threatens freedom of expression," London, 2021.

⁴ Nabaa Alwan Omran and Aziz Sami, "The Limits of Criminal Responsibility for Freedom of Expression," *Ashur Journal of Legal and Political Sciences* 2, no. 4 (2025): 82–88, <https://ashurjournal.com/index.php/AJLPS/about>.

⁵ Abdulrahman Abbas Al-Adain, "Contraindications to Punishment in the Iraqi Penal Code No. 111 of 1969 as Amended," *Journal of Education College Wasit University* 1, no. 47 (2022). <https://doi.org/10.31185/eduj.Vol47.Iss1.2863> (doi.org in Bing)

and reputation represents a natural extension of the right to personal freedom. Any infringement upon an individual's reputation or attack on his or her honor through words or electronic means is deemed a violation of human dignity, thereby justifying legislative intervention to deter such acts and protect society from moral decline.¹

6.3. Defamation and Insult in the Iraqi Legal Framework within the Digital Environment

An Iraqi lawmaker defined public defamation in Article (433/1), including such acts as attribution by public means to cause harm or contempt of another because they are false or inaccurate, which also has the potential of causing punishments to the defamed persons. Also of importance, if the defamation takes place through the media, whether by publication in newspapers, through printed materials or through other forms of publicity will constitute a greater factor in creating the defamation..² According to Article 434, an insult is any word directed towards someone that offends that person's reputation or honour, or that hurts someone's feelings, whether or not the word conveys an act committed by that person. An example of an aggravating circumstance would be if the insult was published in a newspaper, or other types of media (e.g., on the internet, via television, or through an advertisement). An insult could be in the form of direct statements, insinuations, or republishing of a rumour about someone; therefore, the definition of an insult includes many different forms of expression that could be criminally prohibited.³

The evolution of the digital world and the rise of social sites such as Facebook and Twitter (among others) means that actions that may have previously taken place only within the private sphere or through established channels of communication, are now being done in a communal/public setting. As a result, there is a greater ability to reach a larger audience. Therefore, this increases the risk to the individual's reputation. Thus, it poses a significant question regarding how to appropriately balance the potential for individual criminal actions with ensuring that individuals maintain their freedoms regarding the way they choose to express themselves digitally during this time of Artificial Intelligence. Individuals may not consciously wish to defame or do harm; they could simply be communicating information they have received from another party, or they may be sharing their viewpoint.⁴

6.3.1. Leading Case

A historic decision was recently made by the Judicial System of Iraq, by convicting an individual of committing acts of insulting (*Sabb*) and defaming (*Qadhf*) another via Facebook, this was the first time anyone in Iraq has been convicted for the offense of insulting and defaming that way using social media. The decision caused much discussion between media outlets and human rights organisations. The Appeals Committee of the Federal Appeals Court for Baghdad/Rusafa indicated that posting defamatory or insulting materials on Facebook was a type of serious crime, so that they included the criminal nature of it. They view Facebook as a media outlet under the Penal Code due to the nature of being able to disseminate information to a large public audience, and meeting the requirement of being public (*alaniyya*) which is needed to prove this offence.⁵

¹ Omran and Sami, "The Limits of Criminal Responsibility for Freedom of Expression." Pp.85-8.

² Fatima Makki Shaalan, "Crimes of Insult and Cursing in Iraqi Law: An Analytical Study," *Journal of Law and Political Science* 15, no. 2 (2025): 33–52.

³ Omran and Sami, "The Limits of Criminal Responsibility for Freedom of Expression." Pp.8 -85.

⁴ Sami Muhammad Al-Suqari, "Freedom of Expression between Permissibility and Criminalization in Criminal Law," *Al-Qanuniyya Journal*, Al-Nahrain University, 2021, 180.

⁵ Musfa Al-Obaidi, "The First Iraqi Convicted of Insult via Facebook," *Al-Quds Al-Arabi*, accessed December 18, 2025, available at: [الحكم على أول عراقي بتهمة السب عبر الفيسبوك](#)

Based upon that reasoning from the courts' ruling, the appellate found the defendant's actions on Facebook deserved criminal punishment due to the fact that he caused damage to the complainant's reputation socially and professionally. This ruling also has jurisprudential significance in that it broadened the meanings of existing doctrines regarding Defamation to include things like electronic media (i.e., Social Media) and, therefore, modern day methods of communications can now be included within the context of Criminal Liability.

The ruling establishes a new Judicial path under the Iraqi legal system by allowing digital expression of free speech to potentially become criminal under the rule of law when it goes outside its rightful constitutionally provided limits. The obiter dicta of the ruling implicitly raise normative questions regarding the compatibility of such judicial reasoning with constitutional guarantees of freedom of opinion and expression. In particular, the study argued that concerns arise that this interpretive trajectory may curtail journalistic freedom in reporting adverse social phenomena and may deter citizens from utilizing social media platforms as fora for public discourse.¹

From a comparative perspective, the decision invites scrutiny under international human rights jurisprudence, especially the balancing test between the protection of reputation and the safeguarding of free expression. The case thus exemplifies the tension between evolving judicial practice and constitutional text, and it underscores the necessity of a principled equilibrium between penal policy and democratic freedoms.

6.3.2. Defamation and the Dissemination of Misleading News

Defamation and false or misleading news is among the most severe abuses of free speech as it diminishes individual reputations, destroy public confidence and threaten social order. The issue has received attention in Iraq with regard to Article (179/1) of the Penal Code that prescribes punishment for any individual who willfully broadcasts false statements, reports or rumors; and/or who supports any type of provocative propaganda, when that action can reasonably be construed as likely to incite unrest, create alarm or promote chaos among citizens. The penalty for this violation is a maximum of ten years imprisonment.²

Therefore, the law has restricted defamation via social media platforms, and could impose legal penalties on those who commit this type of defamation because it is illegal for someone to defame someone else through social media or any other electronic medium. The legislator has stated that the dissemination of false or misleading News is a crime by establishing the principle of protecting the public order and the public interest. Given that the Law does not require evidence of actual damages; instead, it is sufficient for the purposes of defining the crime, that the act has the potential to create disorder or fear in society. The approach taken by the Legislator towards Defamation via Social Media shows a preference for Social Interest over Individual Freedom of Speech when that Freedom of Speech transcends the bounds of Legitimate Expression.³

6.4. Media and Communications Commission: Constitutional Independence and Organizational Problems

The Media and Communications Commission enjoys financial and administrative independence under the Constitution of the Republic of Iraq of 2005, and is linked to the House of Representatives,⁴ but the

¹ Al-Obaidi, "The First Iraqi Convicted of Insult via Facebook."

² Al-Suqari, "Freedom of Expression between Permissibility and Criminalization in Criminal Law."

³ Mohammad Hassan Mohammad Muharram, *The Substantive Criminal Protection of Freedom of Expression: A Comparative Study* (Alexandria: New University Publishing House, 2018), 102.

⁴ Iraqi Constitution (2005), Art. 103.

lack of a new law regulating its composition and independence, the mechanism for selecting the Board of Commissioners and the limits of its powers after the entry into force of the Constitution, kept its practical organization based on the Coalition Provisional Authority Order No. 65 of 2004. This has contributed to the emergence of problems related to the extent of its independence and its influence on the executive branch, in particular the mechanisms for the formation of the Board of Commissioners.¹ In addition, the Authority combines multiple regulatory powers, including granting operating licenses to digital platforms, monitoring content, and imposing blocking and restriction measures, which raises a problem related to the concentration of regulatory and supervisory functions in the hands of a single entity, so that the licensee is the same as the supervisory body.²

7. Iraq's International Obligations

Iraq has ratified the International Covenant on Civil and Political Rights of 1966. Article (19) of which provides for the protection of freedom of expression. Pursuant to Article (61) of the Iraqi Constitution, international treaties ratified by Iraq form part of the national legal system and prevail over domestic legislation in the event of conflict.³

As per Article-19 of the Covenant, all State Parties are obliged to provide their citizens with the right to Freedom of Expression. The right to Freedom of Expression includes, but is not limited to: The right to seek, receive, and exchange information and ideas through verbal (oral), written (printed), artistic expression (a form of language), or electronically in an Internet or other digital (fixed electronic) format and delivery method(s), anywhere in the world (irrespective of geographical borders). Accordingly, the Committee on Human Rights, in its General Comment No. 34 elaborates that the protection of an individual's Freedom of Expression includes (amongst other things) protection under the constraints of the Internet and other forms of electronic (Digital) Expression. In addition, Article-19(3)(c)(ii) of the Covenant defines that any limitation on an individual's Freedom of Expression is subject to limitations on the exercise of that right (i.e. whether it is fully exercised or is denied) being imposed: - by Legislation; - as necessary to respect someone else's rights and/or reputations (e.g. defamation); and/or - for the protection of national security, the public order, the public health and the public morals. Consequently, any limitation to an individual's Digital Freedom of Expression must be based on the previously listed conditions, or Iraq is in violation of its International Obligations.⁴

However, in reality, there exists a substantial difference between what Iraq's constitution and its commitments under international law stipulate, and what happens in practice. Reports from both local and international organisations involved in promoting human rights indicate that many people have been subject to abuses such as arbitrary detentions, unjust trials, intimidation, and physical violence, due to their use of social media.⁵

¹ Salah Abdullah, "Coalition Provisional Authority Order No. 65 of 2004 from a Legal Perspective," Iraqi Association for the Defense of Press Freedom, Publication date not given, accessed May 10, 2026, <https://pfaa-iq.com/?p=5046>

² Coalition Provisional Authority. Decree No. 65 of 2004 *on the Establishment of the Media and Communications Commission*. Baghdad: Official Gazette, 2004.

³ HRC (UN Human Rights Committee). *General Comment No. 34: Article 19: Freedoms of Opinion and Expression*. CCPR/C/GC/34, 21 July 2011.

⁴ O'Flaherty, Michael. "Freedom of Expression: Article 19 of the International Covenant on Civil and Political Rights and the Human Rights Committee's General Comment No. 34." *Journal of Human Rights Practice*, peer-reviewed, Scopus indexed.

⁵ Freedom House. *Freedom on the Net 2024: Iraq Country Report*. Freedom House.

8. Artificial Intelligence and Digital Freedom of Expression: Key Challenges

8.1. Misinformation and Fabricated Content

Modern-day artificial intelligence (AI) technologies have been used to create fake visual content (images, audiovisual materials). Moreover, fake textual products (written texts) have become a key source of counterfeit content, thereby raising major legal/security concerns. Generative adversarial networks (GANs), which enable users to produce images and videos that are extremely difficult to distinguish from real things, as they are designed to look so similar by AI technology, also belong to this category. In addition, a combination of natural language processing AIs, like GPT and BERT (both are very advanced natural language processors), used to create faux journalism-style text out of text, producing content that imitates the language of real journalists (and creating false news articles), has made it even more challenging to detect fake news/misinformation using these tools.¹

These models rely on vast datasets extracted from the Internet, with the capacity to be customized to produce targeted content as required. Typically, the first stage in developing fake videos and images is collecting video and audio samples of a person's voice or face, creating a training model using this information, generating a piece of content based on the training model, and improving the final product through Super Resolution-type enhancement.²

Misinformation does not only come in the form of visual or textual representation; it also includes the alteration of metadata, as well as the use of various textual patterns to evade filters and submit fraudulent (adversarial) inputs that can deceive automatic analytical programs. The lack of any official report on the establishment of advanced technologies in Iraq, both in terms of development and use, does mean that many users rely on Open Source Tools as their main means of accessing this capability. Additionally, social media platforms such as Facebook, Telegram and Twitter are widely used to circulate photos and videos that have been digitally altered in an unregulated manner. Furthermore, extremist groups (e.g. ISIS) use the same type of technology to recruit individuals and promote extremist ideologies, which adds complexity to this issue.³

In the face of this challenge, there have been many advances in technology to help with the detection of false content; examples are Deepware Scanner, InVID and Microsoft Video Authenticator. The use of artificial intelligence to assist with detecting false content is also an option through machine learning models that can identify variations and digital fingerprints in content.⁴ Iraq has many ongoing challenges to overcome, including having insufficient numbers of qualified personnel to deal with this type of problem, having limited digital infrastructure to support such efforts, not having the proper level of investment in cybersecurity efforts, not having adequate coordination between government entities, and lacking the necessary policies and legislation to provide a framework for these efforts.

¹ Romero-Moreno, Felipe. "Generative AI and Deepfakes: A Human Rights Approach to Tackling Harmful Content." *International Review of Law, Computers & Technology* 38, no. 3 (March 29, 2024): 297–326. <https://doi.org/10.1080/13600869.2024.2324540>.

² Hicks, Mar Hicks, James Humphries, and Joe Slater. "ChatGPT Is Bullshit." *Ethics and Information Technology* 26, no. 1 (2024): 1–8. <https://doi.org/10.1007/s10676-024-09775-5>.

³ Papernot, Nicolas, Patrick McDaniel, Arunesh Sinha, and Michael Wellman. "SoK: Security and Privacy in Machine Learning." *IEEE Security & Privacy* 16, no. 2 (2018): 58–69.

⁴ Verdoliva, Luisa. "Media Forensics and DeepFakes: An Overview." *IEEE Journal of Selected Topics in Signal Processing* 14, no. 5 (2020): 910–932.

Digital networks are susceptible to various types of security vulnerabilities that can be leveraged by extremist users to publish extremist content; many users of networks have turned to using Telegram to connect with other extremists and therefore there are numerous ways an extremist can take control of a user's account (or page) or otherwise use another's account (or page) for their needs.¹

In Iraq, a small number of technical initiatives have begun to be created in partnership with the international community through organizations like UNESCO and UNDP, but there needs to be a significant amount of growth and support for continued success and greater impact.² The emergence of new technologies, such as GPT-5 and Sora, will continue to blur the lines between real content and fake content that can be generated by extremist users; as such, it is likely that in the not-so-distant future we will see significant challenges such as identity theft, computer-generated content directed toward specific individuals, and other uses of technology to disrupt the democratic process.³

In light of these challenges, it becomes imperative to establish artificial intelligence systems that ensure the ethical use of technology. This requires clear legislation, ethical training of models, and independent oversight, thereby safeguarding society against the risks of misinformation and preserving the stability of the legal and political order.

8.2. Algorithmic Moderation and Automated Content Filtering

The objective of social media companies and digital services using artificial intelligence (AI) is to automatically filter online material through automated processes that flag any violations of their terms of service. AI-based filtering has been developed to eliminate harmful content including but not limited to hate speech, incitement of violence, and child sexual abuse material, however these systems don't operate perfectly and may incorrectly categorize some types of legitimate content as prohibited; therefore, they may trigger unintended deletions (due to a lack of precise criteria) of content that violates the company's terms of service.⁴ The biggest downside of moderation through AI is the lack of transparency. Although users may not realize it, AI does not come with instructions about how particular features of the software are utilized in classifying material, so they do not know exactly what criteria were used in selecting which pieces of material were flagged. Furthermore, AI has the potential to embed biases within its programming. Thus, certain minority groups (including individuals who are politically dissenting) may see a disproportionate amount of content deleted.⁵

Within the Iraqi context, it is clear that the risks associated with algorithmic moderation are heightened when a government attempts to pressure social media websites into removing content. When a government uses the algorithms of the social media companies to indirectly censor an individual's right

¹ Reza Montasari, The Impact of Technology on Radicalisation to Violent Extremism and Terrorism in the Contemporary Security Landscape, in *Cyberspace, Cyberterrorism and the International Security in the Fourth Industrial Revolution, Advanced Sciences and Technologies for Security Applications* (Cham: Springer, 2024), 109–133, https://doi.org/10.1007/978-3-031-51482-5_6.

² Alalag, Ahmed Shaker. 2025. "The Oxford Insights Government AI Readiness Index (GARI): An Analysis of its Data and Overcoming Obstacles, with a Case Study of Iraq." *ArXiv*. <https://arxiv.org/abs/2503.20833>.

³ Emilio Ferrara, "Charting the Landscape of Nefarious Uses of Generative Artificial Intelligence for Online Election Interference," *First Monday* 29, no. 6 (2024), <https://doi.org/10.5210/fm.v29i6.13443>.

⁴ Z. Chared et al., "AI-driven Detection of Hate Speech on Social Media: A Case Study in the French Language," *Cluster Computing* (Springer, 2025).

⁵ Gillespie, Tarleton. *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*. New Haven: Yale University Press, 2018.

to express themselves freely, there is no mechanism in place for the individual to appeal the decision to delete the content or to hold the social media website accountable for its actions.¹

8.3. Digital Surveillance and Privacy

AI presents advanced methods for monitoring online interactions, processing large amounts of information, and monitoring the online activities of users. Although there may be legitimate reasons to use these technologies for security purposes, the large scale of surveillance presents serious issues for freedom of expression by creating the “chilling” effect in which people are afraid to express their views because they fear of being monitored and prosecuted.²

In Iraq, there are no clear laws regulating digital surveillance or establishing the necessary safeguards and guarantees for the protection of privacy and freedom of expression. Reports have documented the use of surveillance technologies by Iraqi authorities to track activists and journalists, and the subsequent use of the information collected against them. Due to the lack of laws protecting people's personal data, citizens are in a vulnerable position when it comes to having their privacy violated in many ways. As individuals live in an environment where they are constantly under surveillance (due to the use of facial recognition technology in public and because digital communications are being monitored), they cannot express themselves freely or gather together peacefully without fear of being watched. This fundamentally undermines both freedom of expression and the right to peaceful assembly.³

8.4. Digital Discrimination and the Widening Information Gap

Artificial intelligence imposes an additional challenge in the form of an expanding digital divide. Access to AI technologies and the ability to use them effectively requires a certain level of education and resources. This means that particular segments of society such as the poor, residents of rural areas, and minorities may be excluded from full participation in the digital sphere.⁴

In Iraq, where vast regions suffer from weak Internet infrastructure and low rates of digital literacy, the risk of digital discrimination is even greater. As the exercise of freedom of expression increasingly depends on access to advanced digital technologies, those who lack such access are deprived of the full enjoyment of their rights. In addition, artificial intelligence systems can exacerbate already known inequalities. Algorithms developed based on existing levels of discrimination may be trained on biased input datasets, which may increase the level of bias in the algorithm's output. An example of this is the way some content moderation systems (for platforms) tend to discriminate against content created by individuals from some minority communities.⁵

¹ Imran, Naba' Alwan, “Limits of Freedom of Expression in the Digital Space.” *Ashur Journal for Legal and Political Sciences* 2, no. 4 (2025): 303–332. <https://doi.org/10.64184/ajlps.V2.I4.Y2025.P%25p.219>

² Tufekci, Zeynep. *Twitter and Tear Gas: The Power and Fragility of Networked Protest*. New Haven: Yale University Press, 2017.

³ Mahmood, Omar Muayad. “Legal Protection of Personal Data in Light of Modern Digital Legislation.” *Gateway Journal for Modern Studies and Research* (2025). DOI: <https://doi.org/10.61856/s3s84s80>

⁴ Bentley, Sarah V., Claire K. Naughtin, Melanie J. McGrath, Jessica L. Irons, and Patrick S. Cooper. “The Digital Divide in Action: How Experiences of Digital Technology Shape Future Relationships with Artificial Intelligence.” *AI and Ethics* 4 (2024): 901–915. <https://doi.org/10.1007/s43681-024-00452-3>.

⁵ Al-Ansari, Haider. “The Digital Divide and Its Implications for Iraqi Society in the Era of Artificial Intelligence.” *Baghdad Journal of Social Sciences* 15, no. 3 (2024): 45–68.

9. A balanced Legal Framework for Digital Freedom of Expression

9.1. Reforming Existing Legislation: Critique and Analysis

In order to protect digital freedom of expression in the era of AI, legal scholars have recommended a complete revamping of many current laws, not just surface-level changes. An example of this is Iraq's Cybercrime Law, which contains vague wording and subjective definitions that can be interpreted to restrict legitimate expression. A large part of this issue stems from the sections of the law that address "insulting the authorities" or "destroying national unity", as these sections are often used to prosecute journalists and activist instead of being used to protect public order.¹

Careful legislative safeguarding will maintain the balance between digital security and liberty. To protect the right of individual expression, judicial agency actions must have robust oversight. Additionally, judicial orders must be in writing, be limited in time, and allow an individual to appeal judicial action through clearly defined and disclosed means prior to their implementation.² Legislation governing personal data protection and digital privacy is a fundamental part of enabling individuals to exercise control of their personal information, and providing victims of violations with access to effective sanctions. Legislation should also regulate the use of digital surveillance, limit its use based on the principle of strict necessity, and provide for judicial review of the use of digital surveillance in order to create a proper balance between digital security and citizens' rights.³

9.2. Regulating Digital Content in the Age of Artificial Intelligence

The problem presented by AI requires a clear framework to regulate AI content. Digital platforms should be required to be transparent about how they use AI in content filtering and recommendation and provide clear information on the standards/algorithms used.⁴ Obligations should also be imposed on developers and users of these technologies to provide explicit labeling of AI-generated content, particularly where it is difficult to distinguish from human-produced material. This includes fabricated images and videos (deepfakes) as well as texts generated by large language models. The establishment of effective content verification mechanisms in partnership with independent media and civil society is an important part of fighting against misinformation. Any content removal or restriction must be based on unambiguous legal standards and provided with judicial oversight. With respect to the liability of social media platforms, a balanced approach is required. Platforms should not bear absolute responsibility for all content, which could incentivize excessive censorship. However, they must take appropriate action when notified of unlawful material.⁵

9.3. Capacity-Building and the Promotion of Digital Literacy

¹ Nabaa Alwan Omran, "The Limits of Freedom of Expression in Digital Space," *Ashur Journal of Legal and Political Sciences* 2, no. 4 (2025): 303–332.

² Al-Hamdan, Sajjad Sabbar Razzaq, and Elham Heydari. "The Legal Framework for Cybersecurity in Iraq: An Analytical Study Based on National Laws and International Standards." *Basra Studies Journal* 2, no. 62 (2025): 89–114.

³ Al-Hamdan, Sajjad Sabbar Razzaq, and Elham Heydari. "The Legal Framework for Cybersecurity in Iraq: An Analytical Study Based on National Laws and International Standards." *Basra Studies Journal* 2, no. 62 (2025): 89–114.

⁴ Florence, Lucie, and Richard Harvey. "Regulating AI-generated Content on Social Media Platforms: Challenges and Prospects." *Internet Policy Review* 11, no. 3 (2022): 1–23.

⁵ Gillespie, Tarleton. *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*. New Haven: Yale University Press, 2018.

Simply passing laws does not guarantee the success of those laws; in addition, it is critical to train and enhance the capacity of the judicial and executive branches of government. Judicial decision-making must be free and effective, which requires education for judges and all law enforcement personnel (including police officers) on issues related to the freedom of expression in accordance with the digital environment and ways that artificial intelligence can create new challenges for those who seek to exercise their right to express themselves.¹

Additionally, it is also extremely important that the population has digital literacy, which is the skill required to determine what is reliable and false or misleading. Digital literacy should be integrated into the current curriculum in schools, in addition to providing awareness campaigns and training programs for various social groups. Furthermore, encouragement for research and study of AI's effects on human rights is needed —both academic and professional. It is the role of civil society to track violations, defend rights, and put pressure on state governments to create a balanced legal system to address violations of these rights.²

9.4. International Cooperation and the Use of Comparative Experiences

Due to the cross-border characteristics of digital content, AI, and the international nature of the digital world, international cooperation will be essential from a strategic perspective. Through the use of the Digital Services Act and the General Data Protection Regulation, Iraq can learn from the European experience of balancing platform responsibilities with the protection of freedoms of expression and privacy rights.³

Engagement must occur at an international level through forums dealing with Internet governance/digital human rights/A.I., as well as creating partnerships between industry (the public sector), technology (the private sector), and citizens (the civil society) to create a comprehensive policy/legislation. The industry will provide expertise on technology; the civil society will be the voice of citizens, while the government will be the provider of legislation/regulation. Cooperation between these three entities forms the foundation for a balanced legal framework that protects freedom of expression while also responding to technological advancements.⁴

¹ Al-Ansari, Haider. "The Digital Divide and Its Implications for Iraqi Society in the Era of Artificial Intelligence." *Baghdad Journal of Social Sciences* 15, no. 3 (2024): 45–68.

² Tufekci, Zeynep. *Twitter and Tear Gas: The Power and Fragility of Networked Protest*. New Haven: Yale University Press, 2017.

³ European Commission. *Digital Services Act: Ensuring a Safe and Accountable Online Environment*. Brussels: European Union, 2022.

⁴ Bentley, Sarah V., et al. "The Digital Divide in Action: How Experiences of Digital Technology Shape Future Relationships with Artificial Intelligence." *AI and Ethics* 4 (2024): 901–915.

10. Conclusion

The adoption of Artificial Intelligence presents both opportunities and challenges for digital freedom of expression in Iraq. Modern technology has created new avenues for the expression of opinions, participation, and access to knowledge, while also creating a new set of risks (i.e., misinformation, algorithms that censor, invasion of privacy, and the continued growth of the digital divide). On the other hand, the constitutional problem does not lie in the adoption of the concepts of public order and public morals as reasons for restricting freedom of expression, but rather in the absence of precise constitutional and procedural standards that regulate the scope of their use, especially in the digital space that relies on artificial intelligence and automated content management systems, which expands the discretion of regulators and increases the likelihood of excessive restriction of freedom of expression in the digital space.

The use of broad terms and the imposition of disproportionate penalties also contribute to the expansion of the scope of restrictions on digital freedom of expression, which undermines the essence of the right and exceeds the constitutional limits set out in Article 46 of the Iraqi Constitution, in the absence of an explicit requirement of the criteria of necessity and proportionality in restricting rights and freedoms.

Recommendations

To address these challenges and risks, the study developed a set of recommendations that may contribute to the development of the existing legal system for the purpose of finding solutions:

1. The primary focus should be on keeping any limitations on free speech as the exception, instead of the norm; as such, restricting free speech needs to follow specific guidelines: it must be contained within the bounds of the laws, must serve a valid purpose, must not exceed what is needed in order to attain a desired result, and must have proper accountability through the judiciary.
2. Amend the constitution to include an explicit definition of digital expression in Article 38, and add procedural safeguards that restrict the power of restriction in the face of artificial intelligence.
3. The Law of the Media and Communications Commission should be enacted to establish its independence in accordance with the Constitution of the Republic of Iraq of 2005, separate the power of licensing from censorship, oblige the Commission to require judicial authorization reasoning for any blocking decision, as well as specify an appeal mechanism for the aggrieved party within 7 days.
4. A cybercrime law should be enacted and include precise definitions, require special criminal intent and actual harm, and exempt political criticism and the press from the scope of criminalization.

References

- Ahmed, Abdullah, and Mudassar Nisar Khan. *AI and Content Moderation: Legal and Ethical Approaches to Protecting Free Speech and Privacy*. Unpublished paper, 2024.
- Al Ansari, Haider. "The Digital Divide and Its Implications for Iraqi Society in the Era of Artificial Intelligence." *Baghdad Journal of Social Sciences* 15, no. 3 (2024): 45–68.
- Al Hamdan, Sajjad Sabbar Razzaq, and Elham Heydari. "The Legal Framework for Cybersecurity in Iraq: An Analytical Study Based on National Laws and International Standards." *Basra Studies Journal* 2, no. 62 (2025): 89–114.
- Al Obaidi, Musfa. "The First Iraqi Convicted of Insult via Facebook." *Al Quds Al Arabi*. Accessed December 18, 2025.
- Al Suqari, Sami Muhammad. "Freedom of Expression between Permissibility and Criminalization in Criminal Law." *Al Qanuniyya Journal*, Al Nahrain University, 2021, 180.
- Al-Adain, Abdulrahman Abbas. "Contraindications to Punishment in the Iraqi Penal Code No. 111 of 1969 as Amended." *Journal of Education College Wasit University* 1, no. 47 (2022). <https://doi.org/10.31185/eduj.Vol47.Iss1.2863>.
- Alalaq, Ahmed Shaker. "The Oxford Insights Government AI Readiness Index (GARI): An Analysis of its Data and Overcoming Obstacles, with a Case Study of Iraq." *arXiv* (2025). <https://arxiv.org/abs/2503.20833>.
- Al-Hamdan, Sabbar Razzaq Sajit, and Elham Heydari. "The Legal Framework for Cybersecurity in Iraq: An Analytical Study Based on National Laws and International Standards." *Basra Studies Journal* 2, no. 62 (September 15, 2025): 89–114. <https://doi.org/10.XXXX/bsj.V2.62.347>.
- Ali, T. A. (2020). Proportionality of Iraqi draft IT law with constitutional rights and freedoms. Baghdad: House of Wisdom, Legal Studies Department, pp. 191–216.
- Article 19 Organization. "Iraq: The Draft Cybercrime Law Threatens Freedom of Expression." London, 2021.
- Bahabadi, Mansour Malekpour, et al. "Legal Challenges of Artificial Intelligence Tools in Regulating Freedom of Expression in Iran." *Legal Studies in Digital Age* (2025).
- Bentley, Sarah V., Claire K. Naughtin, Melanie J. McGrath, Jessica L. Irons, and Patrick S. Cooper. "The Digital Divide in Action: How Experiences of Digital Technology Shape Future Relationships with Artificial Intelligence." *AI and Ethics* 4 (2024): 901–915. <https://doi.org/10.1007/s43681-024-00452-3>.
- Coalition Provisional Authority. Decree No. 65 of 2004 *on the Establishment of the Media and Communications Commission*. Baghdad: Official Gazette, 2004.
- Constitution of Egypt (2014), Art. 65.
- Constitution of Jordan (1952, as amended 2011), Art. 15.
- Constitution of Morocco (2011), Art. 25.
- Constitution of Tunisia (2014), Art. 31.

- Digital Media Center (DMC). "34 Million Social Media Users in Iraq in 2025." Published March 4, 2025. [https://dmc-iq.com/2025/03/04/-في-الاجتماعي-التواصل-المواقع-مستخدم-لمليون-٣٤-مركز-الاعلام-الرقمي-٢٠٢٥-عام-العراق-\(dmc-iq.com in Bing\)](https://dmc-iq.com/2025/03/04/-في-الاجتماعي-التواصل-المواقع-مستخدم-لمليون-٣٤-مركز-الاعلام-الرقمي-٢٠٢٥-عام-العراق-(dmc-iq.com%20in%20Bing)).
- European Commission. Digital Services Act: Ensuring a Safe and Accountable Online Environment. Brussels: European Union, 2022.
- Ferrara, Emilio. "Charting the Landscape of Nefarious Uses of Generative Artificial Intelligence for Online Election Interference." First Monday 29, no. 6 (2024). <https://doi.org/10.5210/fm.v29i6.13443>.
- Florence, Lucie, and Richard Harvey. "Regulating AI-generated Content on Social Media Platforms: Challenges and Prospects." Internet Policy Review 11, no. 3 (2022): 1–23.
- Freedom House. Freedom on the Net 2024: Iraq Country Report. Freedom House, 2024.
- Gillespie, Tarleton. "Content Moderation, AI, and the Question of Scale." *Social Media + Society* 6, no. 2 (2020): 1–5. <https://doi.org/10.1177/2056305120938614>.
- Gillespie, Tarleton. Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media. New Haven: Yale University Press, 2018.
- Gomez, Juan Felipe, et al. "Algorithmic Arbitrariness in Content Moderation." *arXiv* (2024). <https://doi.org/10.48550/arXiv.2402.16979>.
- Gorwa, Robert, Reuben Binns, and Christian Katzenbach. "Algorithmic Content Moderation: Technical and Political Challenges in the Automation of Platform Governance." *Big Data & Society* 7, no. 1 (2020): 1–15. <https://doi.org/10.1177/2053951720923232>.
- Hicks, Mar, James Humphries, and Joe Slater. "ChatGPT Is Bullshit." *Ethics and Information Technology* 26, no. 1 (2024): 1–8. <https://doi.org/10.1007/s10676-024-09775-5>.
- Hildebrandt, Mireille. "Law as Computation in the Era of Artificial Legal Intelligence: Speaking Law to the Power of Statistics." *University of Toronto Law Journal* 68, no. 1 (2018): 12–35. <https://doi.org/10.3138/utlj.2017-0044>.
- Human Rights Committee (HRC). General Comment No. 34: Article 19: Freedoms of Opinion and Expression. CCPR/C/GC/34, July 21, 2011.
- Human Rights Watch. *Iraq's Cybercrime Law: Drafting Crimes and Cruel Penalties Undermine Due Process and Freedom of Expression*. July 11, 2012. Accessed May 10, 2016. <https://www.hrw.org/ar/report/2012/07/11/256341>.
- International Covenant on Civil and Political Rights (ICCPR). Adopted December 16, 1966, entered into force March 23, 1976, Art. 19.
- Iraqi Constitution (2005), Art. 38.
- Iraqi Constitution (2005), Art. 46.
- Kaye, David. "Speech Police: The Global Struggle to Govern the Internet." *International Journal of Communication* 13 (2019): 4221–4238.
- Kietzmann, Jan, Ian McCarthy, and Leyland Pitt. "Deepfakes: Trick or Treat?" *Business Horizons* 63, no. 2 (2020): 135–146. <https://doi.org/10.1016/j.bushor.2019.11.006>.
- Kumar, A. "Using Courts to Enforce the Free Speech Provisions of the International Covenant on Civil and Political Rights." *Journal of International Law* 12, no. 3 (2006): 45–78.

- La Rue, Frank. Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression. UN Doc. A/HRC/17/27 (2011), paras. 70–76.
- Lyon, David. “Surveillance, Big Data, and Democracy: The Paradoxes of Power.” *International Journal of Communication* 8 (2014): 2061–2079.
- Mahmood, Omar Muayad. “Legal Protection of Personal Data in Light of Modern Digital Legislation.” *Gateway Journal for Modern Studies and Research* (2025). <https://doi.org/10.61856/s3s84s80>.
- Mittelstadt, Brent, et al. “The Ethics of Algorithms: Mapping the Debate.” *Big Data & Society* 3, no. 2 (2016): 1–21. <https://doi.org/10.1177/2053951716679679>.
- Montasari, Reza. “The Impact of Technology on Radicalisation to Violent Extremism and Terrorism in the Contemporary Security Landscape.” In *Cyberspace, Cyberterrorism and International Security in the Fourth Industrial Revolution, Advanced Sciences and Technologies for Security Applications*, 109–133. Cham: Springer, 2024. https://doi.org/10.1007/978-3-031-51482-5_6.
- Muharram, Mohammad Hassan Mohammad. *The Substantive Criminal Protection of Freedom of Expression: A Comparative Study*. Alexandria: New University Publishing House, 2018.
- Nouri, Z., Walid Ben Salah, & AlOmran, N. (2024). *Artificial Intelligence and Administrative Justice: An Analysis of Predictive Justice in France*. **Hasanuddin Law Review**, 10(2), 119–143. DOI: <https://doi.org/10.20956/halrev.v10i2.5541>
- O’Flaherty, Michael. “Freedom of Expression: Article 19 of the International Covenant on Civil and Political Rights and the Human Rights Committee’s General Comment No. 34.” *Journal of Human Rights Practice*.
- Omran, Nabaa Alwan, and Aziz Sami. “The Limits of Criminal Responsibility for Freedom of Expression.” *Ashur Journal of Legal and Political Sciences* 2, no. 4 (2025): 82–88. <https://ashurjournal.com/index.php/AJLPS/about>.
- Papernot, Nicolas, Patrick McDaniel, Arunesh Sinha, and Michael Wellman. “SoK: Security and Privacy in Machine Learning.” *IEEE Security & Privacy* 16, no. 2 (2018): 58–69.
- Pasquale, Frank. “A Rule of Persons, Not Machines: The Limits of Legal Automation.” *George Washington Law Review* 87, no. 1 (2019): 1–40.
- Rakesh, K. S., and S. Yadav. "To Analyze the Effectiveness of Mitigation Strategies Aimed Against Distributed Network Systems." *International Journal of Computing Programming and Database Management* (2025). <https://doi.org/10.33545/27076636.2025.v6.i1a.107>.
- Republic of Iraq. Cybercrime Draft Law No. (17) of 2012, Article 3.
- Romero-Moreno, Felipe. “Generative AI and Deepfakes: A Human Rights Approach to Tackling Harmful Content.” *International Review of Law, Computers & Technology* 38, no. 3 (2024): 297–326. <https://doi.org/10.1080/13600869.2024.2324540>.
- Sadhana, Gaikwad. “The Study of Right to Freedom of Expression, Digital Media Laws and Demand for Innovation.” *Law and World* (2025).
- Sailaja, P.V.S., et al. “Freedom of Speech in the Digital Age: Challenges of Algorithmic Censorship and AI Moderation.” *Lex Localis: Journal of Local Self-Government* 23, no. S6 (2025). <https://doi.org/10.52152/84jfy65>.
- Shaalán, Fatima Makki. “Crimes of Insult and Cursing in Iraqi Law: An Analytical Study.” *Journal of Law and Political Science* 15, no. 2 (2025): 33–52.

Tufekci, Zeynep. *Twitter and Tear Gas: The Power and Fragility of Networked Protest*. New Haven: Yale University Press, 2017.

Verdoliva, Luisa. "Media Forensics and DeepFakes: An Overview." *IEEE Journal of Selected Topics in Signal Processing* 14, no. 5 (2020): 910–932.

Wachter, Sandra, Brent Mittelstadt, and Chris Russell. "Bias Preservation in Machine Learning: The Legality of Fairness Metrics under EU Non-Discrimination Law." *West Virginia Law Review* 123, no. 3 (2021): 735–768.

Wordtune. "How AI Can Help Marketers with Personalization." *Wordtune Blog*. Accessed January 20, 2026. <https://www.wordtune.com/blog/ai-for-personalization>.

Yeung, Karen. "A Study of the Implications of Advanced Digital Technologies (Including AI Systems) for the Concept of Responsibility within a Human Rights Framework." *Modern Law Review* 82, no. 2 (2019): 193–220. <https://doi.org/10.1111/1468-2230.12435>.

Yeung, Karen. "Algorithmic Regulation: A Critical Interrogation." *Regulation & Governance* 12, no. 4 (2018): 505–523. <https://doi.org/10.1111/rego.12158>.

Z. Chared et al., "AI-driven Detection of Hate Speech on Social Media: A Case Study in the French Language," *Cluster Computing* (Springer, 2025).10.24018/ejpolitics.2025.4.1.165