Access to Justice in Eastern Europe
ISSN 2663-0575 (Print)
ISSN 2663-0583 (Online)
http://ajee-journal.com

RESEARCH ARTICLE

Research Article

DIGITAL RIGHTS, AI, AND THE LAW: INTERNATIONAL PERSPECTIVES ON SAUDI ARABIA'S LEGAL FRAMEWORK AND INTERNATIONAL EXPERIENCE

Soumaya Khammassi and Yusra AlShanqityi*

ABSTRACT

Background: *This research analyses the global evolution of digital rights and AI governance and examines the implications for Saudi Arabia's legal framework. As artificial intelligence becomes increasingly embedded in everyday life, there is an urgent need to assess its impact on fundamental human rights, particularly given the absence of a global consensus on the definition and scope of "digital human rights." The Kingdom of Saudi Arabia's (KSA) Vision 2030 initiative presents a unique opportunity to develop AI governance frameworks that align with international standards while reflecting local cultural values and Islamic ethical principles.*

Methods: *This study employs a qualitative analytical approach to examine Saudi Arabia's current legal framework governing AI and digital human rights. The methodology involves a comprehensive statutory analysis of Saudi Arabian legislation, particularly the Personal Data Protection Law (PDPL) and the Saudi Data and AI Authority (SDAIA) 's ethical guidelines, in comparison to international legal instruments, including*

DOI:
https://doi.org/10.33327/AJEE-18-8.S-a000154

Date of submission: 16 Apr 2025
Date of acceptance: 08 Sep 2025
Online First publication: 08 Dec 2025

Disclaimer:
The authors declare that their opinion and views expressed in this manuscript are free of any impact of any organizations.

UNESCO's AI Ethics Recommendation, the EU AI Act, and OECD guidelines. The research evaluates alignment with international standards and effectiveness in addressing emerging digital rights challenges in the AI era.

Results and conclusions: *The research reveals that while Saudi Arabia has made notable progress through the PDPL and SDAIA frameworks, significant regulatory gaps persist. The PDPL exhibits limitations in addressing contemporary AI challenges, including algorithmic accountability, bias mitigation, and comprehensive data protection in AI contexts. The study identifies critical deficiencies, including overly broad exceptions to consent requirements, insufficient provisions for algorithmic transparency, and fragmented regulatory oversight. Recommendations include establishing specialised oversight bodies, developing ethical frameworks tailored to the Saudi context, and increasing the involvement of experts in decisions related to AI governance. This paper contributes by offering a comparative evaluation of Saudi Arabia's digital rights framework against leading international instruments, highlighting reforms necessary for culturally grounded and globally aligned governance.*

1 INTRODUCTION

1.1. Research Context and Significance

Artificial intelligence is a trending issue transforming multiple sectors, including healthcare, education, governance, and societal systems. Researchers increasingly recognise both the positive and negative impacts AI can have on human rights, particularly digital human rights.[1] The implementation of AI raises significant ethical and legal issues regarding privacy, fairness, and transparency. As AI technologies advance, specific legislation becomes necessary to ensure they respect individual rights in the digital world.

At the core of the current technological evolution centred on AI's transformative potential, growing concerns exist about its effects on human rights. The legal debate primarily addresses three fundamental issues: how these new technologies violate existing rights, create conflicts among established rights, and introduce entirely new legal questions for which no established rights framework yet exists. This complex intersection of technology and rights requires thoughtful consideration of equity, transparency, and accountability in AI governance frameworks.[2]

The Kingdom faces a distinctive opportunity to contribute to the global discourse on digital rights by articulating an approach that harmonises international norms with

[1] Reema Bakheet Alzahrani, 'An Overview of AI Data Protection in the Context of Saudi Arabia' (2024) 3(3) International Journal for Scientific Research 199. doi:10.59992/IJSR.2024.v3n3p8 [in Arabic].

[2] Bart Custers, 'New Digital Rights: Imagining Additional Fundamental Rights for the Digital Era' (2022) 44 *Computer Law & Security Review* 105636. doi:10.1016/j.clsr.2021.105636.

Islamic ethical principles and local cultural values. Saudi Arabia's Vision 2030[3] initiative explicitly recognises the transformative potential of digital technologies, but this transformation necessitates careful consideration of how rights frameworks must evolve in parallel. Vision 2030 aims to diversify the economy, rebalance the country's dependence on oil revenues, and develop new technologies. This has led to setting strategic objectives for the digitalisation of several sectors, including the application of artificial intelligence and data technologies in health and other sectors.[4] However, as machine intelligence is increasingly implemented across governance activities and multiple aspects of life, there is a need to address human rights in the digital world. As a modernising country in the contemporary world, the KSA stands at the intersection of technology and human rights in the digital environment.

Unlike countries where digital rights discussions emerged gradually alongside technological development, K.S.A is engaging with these questions during an accelerated period of digital transformation, potentially allowing for more integrated approaches to rights protection within technological infrastructure.[5]

1.2. Research Problem and Gap

The governance of artificial intelligence at the international level has evolved rapidly, moving from early ethical principles to increasingly formalised regulatory approaches. The Asilomar AI Principles (2017)[6] and IEEE's "Ethically Aligned Design" initiative (2016-2019)[7] represented initial efforts from the research and engineering communities.[8] More comprehensive intergovernmental frameworks emerged with the OECD Principles on AI (2019)[9] and UNESCO's Recommendation on the Ethics of AI (2021),[10] adopted by 193 countries.

[3] *Saudi Vision 2030* (2025) <https://www.vision2030.gov.sa/en> accessed 10 April 2025.

[4] Custers (n 2).

[5] Mohammad Omar Mohammad Alhejaili, 'Integrating Smart Contracts into the Legal Framework of Saudi Arabia' (2025) 67(2) International Journal of Law and Management 230. doi:10.1108/IJLMA-03-2024-0086.

[6] Future of Life Institute, 'Asilomar AI Principles' (2017) <https://futureoflife.org/ai-principles/> accessed 10 April 2025.

[7] IEEE, *Ethically Aligned Design: A Vision for Prioritizing Human Well-Being with Autonomous and Intelligent Systems* (IEEE 2019); IEEE, 'The IEEE Global Initiative 2.0 on Ethics of Autonomous and Intelligent Systems' (*IEEE Standards Association (IEEE SA)*, 2025) <https://standards.ieee.org/content/ieee-standards/en/industry-connections/ec/autonomous-systems.html> accessed 10 April 2025.

[8] Alan FT Winfield and Marina Jirotka, 'Ethical Governance is Essential to Building Trust in Robotics and Artificial Intelligence Systems' (2018) 376(2133) Philosophical Transactions of the Royal Society A 20180085. doi:10.1098/rsta.2018.0085.

[9] OECD, 'Recommendation of the Council on Artificial Intelligence' (*OECD Legal Instruments*, 22 May 2019) <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449> accessed 10 April 2025.

[10] UNESCO, 'Recommendation on the Ethics of Artificial Intelligence' (*UNESCO Digital Library*, 2021) <https://unesdoc.unesco.org/ark:/48223/pf0000380455 > accessed 10 April 2025.

International frameworks exist along a spectrum from voluntary principles to legally enforceable regulations. The OECD Principles and UNESCO Recommendation function as "soft law," shaping behaviour through normative expectations rather than formal sanctions.[11] The EU AI Act[12] establishes legally binding obligations with significant penalties for non-compliance.[13] However, no universally accepted definition of digital human rights exists, and no binding treaty framework comprehensively addresses them.

Within this context, K.S.A presents a particularly compelling case: the Kingdom is undergoing accelerated digital transformation under Vision 2030 while integrating Islamic ethical principles into its legal system. Research examining how K.S.A's domestic framework aligns with, diverges from, or innovates upon international digital rights governance remains limited.

1.3. Research Objectives and Questions

This paper addresses the previously explained gap by critically examining K.S.A's evolving legal framework on digital rights and AI governance in light of international standards. It is guided by the following research questions:

1. To what extent are digital human rights conceptually established within international legal discourse and scholarly literature?
2. How has Saudi Arabia integrated global digital human rights frameworks and principles into its domestic legislative and regulatory infrastructure?
3. What distinctive challenges and strategic opportunities characterise Saudi Arabia's approach to digital rights protection within the context of accelerating technological advancement?

[11] Joel R Reidenberg, 'Lex Informatica: The Formulation of Information Policy Rules Through Technology' (1997) 76(3) Texas Law Review 553.

[12] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) [2024] OJ L 1689 <http://data.europa.eu/eli/reg/2024/1689/oi> accessed 10 April 2025.

[13] UK Department for Digital, Culture, Media and Sport, 'Establishing a Pro-Innovation Approach to Regulating AI: An Overview of the UK's Emerging Approach' (*UK Government*, 18 July 2022) <https://www.gov.uk/government/publications/establishing-a-pro-innovation-approach-to-regulating-ai> accessed 10 April 2025.

1.4. Contribution and Structure

By answering these questions, this paper contributes to the growing body of literature on digital rights. It employs a comparative doctrinal analysis, focusing on statutory analysis, soft law examination, and jurisdictional analysis of the digital rights framework.[14]

The comparative doctrinal approach allows for positioning Saudi Arabia's regulatory efforts within a broader international framework.

This paper is organised into five main sections. Section 2 develops the conceptual foundation by examining how digital human rights are defined in international scholarship and identifying five core categories: privacy, internet access, data protection, anonymity, and the right to be forgotten. Section 3 situates these concepts within the MENA regional context, examining how Islamic legal and ethical principles interact with emerging digital governance frameworks. Section 4 analyses international AI governance approaches, contrasting the EU's binding regulatory model with UNESCO and OECD soft-law frameworks to establish comparative benchmarks. Section 5 evaluates Saudi Arabia's legal framework—primarily the PDPL and Anti-Cybercrime Law—against these international standards, identifying both achievements and regulatory gaps. The paper concludes with targeted recommendations for legal reform that balance international alignment with cultural distinctiveness.

It highlights Saudi Arabia's progress in AI regulation through a systematic analysis of existing legal instruments, such as the Personal Data Protection Law (PDPL) and the Saudi Data and Artificial Intelligence Authority (SDAIA) Ethical Guidelines. It helps to analyse their compliance with international standards and their ability to respond to new digital human rights issues in the era of AI. More broadly, the study underscores how cultural and religious values, particularly Islamic ethical principles, can inform distinctive approaches to digital rights governance in non-Western contexts.

2 LITERATURE REVIEW AND CONCEPTUALIZING DIGITAL HUMAN RIGHTS

2.1. Overview and Rationale

This section reviews the evolving concept of digital human rights, surveys the main categories identified in the literature, and examines international and regional governance

[14] Royal Decree of the Kingdom of Saudi Arabia No M/19 of 09/02/1443 AH (16/09/2021 G) 'Personal Data Protection Law' (SDAIA 2023) <https://sdaia.gov.sa/en/SDAIA/about/Documents/Personal%20Data%20English%20V2-23April2023-%20Reviewed-.pdf> accessed 10 April 2025; Saudi Data and Artificial Intelligence Authority, *AI Ethics Principles* (SDAIA 2025) <https://sdaia.gov.sa/en/SDAIA/about/Documents/ai-principles.pdf> accessed 10 April 2025; Nayera Mohamed Hamed Ibrahim, 'Artificial Intelligence (AI) and Saudi Arabia's Governance' (2024) 40(4) Journal of Developing Societies 500. doi:10.1177/0169796X241288590.

approaches. The review highlights definitional debates, recurring principles, and regulatory models. It underscores the role of cultural and religious values, specifically Islamic ethical principles, in shaping non-Western approaches to digital rights governance.

2.2. Defining Digital Human Rights

The concept of digital human rights remains relatively new and emerging, unlike conventional human rights vested under International Human Rights frameworks such as the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR).[15] It was only during the early 2000s that international recognition of this category of rights began to emerge, with the World Summit on the Information Society (2003, 2005) marking a significant milestone in their institutional recognition.[16]

The digital human rights framework has evolved as an extension of traditional human rights frameworks, adapted to address the unique challenges posed by technological advancement. Digital rights are generally understood as human and legal rights that allow individuals to access, use, create, and publish digital content on devices such as computers and mobile phones, as well as in virtual spaces and communities.

The academic discussion reveals a significant question: do effective digital rights protections require entirely new frameworks, or can they be achieved by extending existing approaches? The answer to this issue remains challenging, since there is no agreement on a definition of digital human rights. While some scholars, such as Pangrazio and Sefton-Green,[17] define digital rights as merely a contextual expression of established rights, particularly freedom of expression and the right to privacy.[18] Others consider them a distinct category of rights,[19] particularly as new technologies like AI present issues not foreseen in traditional frameworks; thus, human rights are facing novel challenges that require new protection mechanisms.

[15] Universal Declaration of Human Rights (UDHR) (10 December 1948) <https://www.un.org/en/about-us/universal-declaration-of-human-rights> accessed 10 April 2025; International Covenant on Civil and Political Rights (ICCPR) (16 December 1966) <https://treaties.un.org/pages/viewdetails.aspx?chapter=4&clang=_en&mtdsg_no=iv-4&src=ind> accessed 10 April 2025.

[16] Rikke Frank Jørgensen, *Framing the Net: The Internet and Human Rights* (Edward Elgar 2013). doi:10.4337/9781782540809.

[17] Luci Pangrazio and Julian Sefton-Green, 'Digital Rights, Digital Citizenship and Digital Literacy: What's the Difference?' (2021) 10(1) *Journal of New Approaches in Educational Research* 15. doi:10.7821/naer.2021.1.616.

[18] Oleksandr M Kostenko and others, '"Legal Personality" of Artificial Intelligence: Methodological Problems of Scientific Reasoning by Ukrainian and EU Experts' (2023) 39(4) AI and Society 1683. doi:10.1007/s00146-023-01641-0.

[19] Mireille Hildebrandt, *Smart Technologies and the End(s) of Law* (Edward Elgar 2015).

The definitional ambiguity surrounding digital human rights, emphasised by AllahRakha,[20] Bendary and Rajadurai,[21] undermines consistent protection because jurisdictions adopt divergent interpretations of these rights. To address this, scholars propose different strategies. Cong advocates a "translation approach," arguing that existing human rights principles remain valid but must be carefully reinterpreted for digital contexts.[22] Similarly, Land and Aronson highlight the potential of adapting traditional human rights frameworks to guide the governance of new technologies, reinforcing the idea that established principles can provide a normative foundation.[23] By contrast, Hildebrandt[24] insists that computational technologies introduce fundamentally novel challenges that cannot be resolved through reinterpretation alone. She cautions that smart technologies may erode the very "ends of law", justice, accountability, and legal certainty, unless new forms of "legal protection by design" are embedded directly into technological infrastructures.

Adding to this debate, Custers goes further by exploring the possibility of articulating entirely new fundamental rights for the digital era, arguing that incremental reinterpretation may not be sufficient to protect individuals against AI-driven risks.[25] More recent scholarship in the non-Western context expands this conversation by emphasising the role of cultural and religious traditions. For example, Elmahjub[26] proposes a pluralist ethical benchmarking for AI governance that incorporates Islamic ethics, while Ali et al.[27] explicitly evaluate AI through the lens of *maqāṣid al-sharīʿa*, demonstrating how Islamic jurisprudential principles of dignity, justice, and privacy can enrich digital rights discourse.[28] These perspectives underline that the recognition and definition of digital human rights should not only deal with whether they are "translated" or "new" rights, but also consider how cultural and religious frameworks may inform distinctive and contextually legitimate approaches to governance.

[20] Naeem AllahRakha, 'UNESCO's AI Ethics Principles: Challenges and Opportunities' (2024) 2(9) *International Journal of Law and Policy* 24. doi:10.59022/ijlp.225.

[21] Mohamed G Bendary and Jegatheesan Rajadurai, 'Emerging Technologies and Public Innovation in the Saudi Public Sector: An Analysis of Adoption and Challenges Amidst Vision 2030' (2024) 29(1) The Innovation Journal: The Public Sector Innovation Journal 1.

[22] Wanshu Cong, 'Understanding Human Rights on the Internet: An Exercise of Translation?' (2017) 22(1-2) Tilburg Law Review 138. doi:10.1163/22112596-02201007.

[23] Molly K Land and Jay D Aronson (eds), *New Technologies for Human Rights Law and Practice* (CUP 2018) doi:10.1017/9781316838952.

[24] Hildebrandt (n 19).

[25] Custers (n 2).

[26] Ezieddin Elmahjub, 'Artificial Intelligence (AI) in Islamic Ethics: Towards Pluralist Ethical Benchmarking for AI' (2023) 36 Philosophy & Technology 73. doi:10.1007/s13347-023-00668-x.

[27] Fatima Ali and others, 'Islamic Ethics and AI: An Evaluation of Existing Approaches to AI using Trusteeship Ethics' (2025) 38(2) Philosophy & Technology 120. doi:10.1007/s13347-025-00922-4.

[28] Mohammad Omar Mohammad Alhejaili, 'Securing the Kingdom's e-Commerce Frontier: Evaluation of Saudi Arabia's Cybersecurity Legal Frameworks' (2024) 13(2) Journal of Governance & Regulation 275. doi:10.22495/jgrv13i2siart4.

Thus, digital rights are the rights individuals have in the digital realm. These rights are derived from conventional universal rights but are adapted to meet the demands and opportunities posed by the rapidly growing new technologies, including artificial intelligence. As digital environments increasingly shape humans' sociopolitical, economic, and personal existence, the scope of these rights has extended.

Ultimately, digital human rights represent a renewed paradigm, well-anchored in international human rights conventions, while suggesting an adaptive conceptual and normative approach.

2.3. Core Categories of Digital Human Rights

Comparative studies reveal both convergence and divergence across existing frameworks. Jobin et al., in their analysis of 84 ethics guidelines, identified documents transparency, justice, non-maleficence, responsibility, and privacy as recurring principles.[29] While the OECD emphasises inclusive growth and human-centred values, UNESCO places greater emphasis on cultural contexts and sustainability. The EU's AI Act adopts a more regulatory stance through its risk-based classification system.[30]

These frameworks address the issue of individuals' inherent rights in digital spaces with varying levels of specificity. Privacy protections are dominant in both ethical and legal discourse, though conceptualised differently across contexts. Non-discrimination principles appear consistently, but with varying approaches to bias mitigation. Transparency requirements have converged around key elements, including disclosure of AI use and appropriate explainability, though implementation guidance varies substantially.[31] Despite these variations, several consensus principles have emerged across frameworks. Fjeld et al. identified eight key themes with widespread support: privacy, accountability, safety and security, transparency and explainability, fairness and non-discrimination, human control of technology, professional responsibility, and promotion of human values.[32]

Taken together, these various frameworks show that digital rights discourse both continues established human rights traditions and introduces innovative protections. Building on this literature, the present research focuses on five essential digital rights: privacy, internet access, data protection, anonymity, and the right to be forgotten.

[29] Anna Jobin, Marcello Ienca and Effy Vayena, 'The Global Landscape of AI Ethics Guidelines' (2019) 1(9) Nature Machine Intelligence 389. doi:10.1038/s42256-019-0088-2.

[30] Michael Veale and Frederik Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act' (2021) 22(4) Computer Law Review International 97. doi:10.9785/cri-2021-220402.

[31] Stefan Larsson and Fredrik Heintz, 'Transparency in Artificial Intelligence' (2020) 9(2) Internet Policy Review. doi:10.14763/2020.2.1469.

[32] Gessfhk Fjeld and others, *Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI* (Berkman Klein Center for Internet & Society Research Publication Series no 2020-1, Harvard University 2020). doi:10.2139/ssrn.3518482.

2.3.1. Privacy Rights in Digital Contexts

Digital privacy right is, ultimately, an extension of the privacy right. The international legal framework has long recognised privacy as a fundamental right. According to the International Covenant on Civil and Political Rights, Article 17 protects individuals against "arbitrary or unlawful interference with their privacy, family, home, or correspondence."[33] Article 12 of the Universal Declaration of Human Rights similarly asserts the right to privacy and protection from arbitrary interference.[34]

The problem does not lie in recognising the normative value of this right nor in defining its limits within the traditional framework in which it was established, but rather in its rapid transposition to the digital context. In the physical world, it is relatively easy to define the scope of application of this right, limit the actions considered violations, and assign ongoing responsibility for them. However, in the virtual realm, parameters become increasingly blurred. The decentralised nature of digital environments has shifted the focus from protecting individuals from surveillance to empowering them, raising concerns about digital access, inclusion, and protection and giving rise to profound regulatory uncertainty.

The use of advanced technologies, such as facial recognition, big data, and AI-assisted surveillance, has been unparalleled in human history and has been carried out primarily without people's knowledge or permission, thereby altering this right. For instance, in *Glukhin v. Russia* (App. No 11519/20),[35] the European Court of Human Rights stressed that the use of facial recognition to identify to identify, locate, and subsequently arrest the applicant from photographs and video posted on social media constituted an interference with his right to respect for his private life and infringe Article 8 of the European Convention on Human Rights.

Custers[36] expressively affirms that AI surveillance impacts privacy rights, leading to their violation, and calls for greater attention to ensuring that artificial intelligence adheres to privacy-freedom governing principles.[37] Furthermore, research on algorithmic bias is especially concerning for diverse societies. Studies from the United States demonstrate that even the most advanced AI facial recognition tools exhibit significantly higher error rates when identifying black women compared to white men.[38]

[33] ICCPR (n 15) art 17; UN Human Rights Committee, 'CCPR General Comment No 16: Article 17 (Right to Privacy)' (8 April 1988) <https://www.refworld.org/legal/general/hrc/1988/en/27539> accessed 10 April 2025.

[34] UDHR (n 15) art 12.

[35] *Glukhin v Russia* App no 11519/20 (ECtHR, 4 July 2023) <https://hudoc.echr.coe.int/eng?i=001-225655> accessed 10 April 2025.

[36] Custers (n 2).

[37] Alzahrani (n 1).

[38] Adam Schwartz, 'Chicago's Video Surveillance Cameras: A Pervasive and Poorly Regulated Threat to Our Privacy' (2013) 11(2) Northwestern Journal of Technology and Intellectual Property 47.

2.3.2. Right to Internet Access

The concept of a "right" to internet access, or "digital connectivity," implies the ability of a person to connect to the internet to seek, receive and impart information.[39] Although, there is no binding international treaty that recognises the right to internet, the internet is growingly considered as an enabler of many human rights such as the right to freedom of speech and expression and the right to information as provided under Article 19 of the Universal Declaration of Human Rights, or the right to have equal access to public services (Article 21).[40] Recognising that internet access plays a facilitative role in the enjoyment of fundamental rights, the UNHRC (United Nations Human Rights Council) adopted Resolution 47/16 in 2021, calling on governments to close the gap in the availability and accessibility of affordable, stable Internet.[41]

Scholarly perspectives on this issue can be divided into three distinct groups for this research. Advocates for classifying internet access as a human right emphasise how digital connectivity has become essential for exercising numerous established rights in contemporary society, from freedom of expression to education.[42] According to the second group, represented by scholars such as Veale and Zuiderveen Borgesius,[43] internet access is only a means to the enjoyment of other rights; consequently, they contend that it lacks the fundamental quality required for recognition as a human right. For this group, internet access serves merely as a technological enabler of rights rather than constituting a right itself.[44]

Among these perspectives, the most compelling is the view that internet access can be conceptualised as an emerging human right.[45] This nuanced approach acknowledges the internet's crucial role in contemporary rights fulfilment while acknowledging that it does not carry the same foundational status as primary human rights, such as freedom from torture or the right to life. Yet, in a world where digital infrastructure has become indispensable for daily life, meaningful participation in society becomes severely limited without internet access.

The resulting legal discourse reflects both continuity and innovation: it builds upon existing treaty obligations while pressing towards recognition of a distinct digital entitlement in practice.

[39] Jonathon Penney, 'Open Connectivity, Open Data: Two Dimensions of the Freedom to Seek, Receive and Impart Information in the New Zealand Bill of Rights' (2012) 4 Victoria University of Wellington Law Review: Working Paper Series 1; Paul De Hert and Dariusz Kloza, 'Internet (access) as a New Fundamental Right: Inflating the Current Rights Framework?' (2012) 3(3) European Journal of Law and Technology 1.

[40] UDHR (n 15) arts 19, 21.

[41] Alhejaili (n 28).

[42] Stephen Tully, 'A Human Right to Access the Internet? Problems and Prospects' (2014) 14(2) Human Rights Law Review 175. doi:10.1093/hrlr/ngu011.

[43] Veale and Zuiderveen Borgesius (n 30).

[44] Vinton Cerf, 'Internet Access is Not a Human Right' *The New York Times* (New York, 4 January 2012) A25.

[45] Kay Mathiesen, 'The Human Right to Internet Access: A Philosophical Defense' (2012) 18 The International Review of Information Ethics 9. doi:10.29173/irie299.

2.3.3. Data Protection Rights

Data protection has become indispensable as AI systems process vast amounts of personal information, raising fundamental rights concerns. Traditionally, data protection has been governed by various legislations—such as the GDPR[46] in the EU—which grant individuals power and meaningful control over their information through rights of access, correction, and deletion.[47]

Data Protection right was firmly established in *Digital Rights Ireland Ltd v. Minister for Communications* (Joined Cases C-293/12 and C-594/12),[48] where the Court of Justice declared the Data Retention Directive invalid for exceeding the limits of proportionality under Articles 7, 8, and 52(1) of the Charter of Fundamental Rights. While acknowledging the Directive's legitimate objective of combating serious crime, the Court held that its general and indiscriminate retention of telecommunications data constituted a particularly serious interference with the rights to privacy and data protection. The judgment required any data retention regime to be strictly necessary, supported by clear and precise rules, and subject to independent supervision, thereby establishing the modern constitutional standard for data protection within the European Union.

However, the rise of AI places these standards under unprecedented pressure. The automated, predictive, and often opaque processing models that characterise AI challenge the very assumptions of informed consent, transparency, and proportionality that the Digital Rights Ireland judgment sought to safeguard. AI technologies rely on big data analytics and machine learning algorithms that often operate beyond conventional privacy safeguards. The "black box" nature of many AI systems—characterised by opaque decision-making processes lacking self-explainability—prevents individuals from understanding how their personal information is processed, analysed, and potentially shared.

This lack of transparency fundamentally weakens the principle of informed consent that underpins modern data protection regimes. As Vogel[49] argues, these obstacles can only be

[46] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

[47] Federica Paolucci, 'Enhancing Oversight and Addressing Gaps: Assessing the Impact of the AI Act on Biometric Identification Systems' in Natalia Menéndez González and Giuseppe Mobilio (eds), *Next Democratic Frontiers for Facial Recognition Technology (FRT): The Legal, Ethical and Democratic Implications of FRT* (Springer 2025) 71. doi.org/10.1007/978-3-031-89794-8_5.

[48] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* (CJEU (Grand Chamber), 8 April 2014) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0293> accessed 10 April 2025.

[49] Yannick Alexander Vogel, 'Stretching the Limit, The Functioning of the GDPR's Notion of Consent in the context of Data Intermediary Services' (2022) 8(2) European Data Protection Law Review 238. doi:10.21552/edpl/2022/2/10.

overcome through adaptive legal frameworks that ensure users maintain meaningful control over their data in increasingly complex AI environments. The rapid advancement of AI technologies necessitates specialised legislation that balances innovation with robust rights protection, addressing mounting concerns about fairness, transparency, and accountability in these rapidly evolving systems.

2.3.4. Right to Anonymity

The right to anonymity enables individuals to preserve their identity and personal integrity by preventing unwanted disclosure. This safeguard has become increasingly vital in digital environments where personal information can be exposed and circulated without consent.[50] Traditionally, this right has been understood as an extension of fundamental rights—most notably, the right to privacy[51] and the freedom of expression.[52]

In *Standard Verlagsgesellschaft MBH v. Austria (*App. No 21277/19*)*,[53] the European Court of Human Rights reinforced this principle within the context of online expression. The Court held that compelling the disclosure of anonymous commenters' identities violated Article 10 of the Convention, emphasising that anonymity shields individuals from retaliation and is essential to preserving free and uninhibited participation in democratic debate.

In today's digital age, anonymity has acquired renewed urgency. AI-driven technologies, such as facial recognition, predictive analytics, and pervasive data tracking, have profoundly altered the boundaries of private life. These systems continuously monitor user behaviour, eroding the ability to remain unidentifiable online. As Kettemann et al.[54] observe, anonymity now serves as a crucial safeguard against intrusive surveillance, reinforcing personal agency and autonomy in increasingly datafied societies.

With the proliferation of algorithmic profiling and biometric identification across everyday environments, protecting anonymity is no longer a matter of convenience but a condition for preserving individual freedom, diversity, and democratic discourse in the digital era. Ultimately, safeguarding anonymity is not only about concealing identity but about affirming each individual's right to define their digital presence and personal boundaries in a world of pervasive visibility.

[50] Samuel Samiai Andrews, 'Copyright Originality in the Digital Space: The Kingdom of Saudi Arabia's Creatives' in Indranath Gupta (ed), *Handbook on Originality in Copyright: Cases and Materials* (Springer 2023) 1. doi:10.1007/978-981-19-1144-6_9-1.

[51] UDHR (n 15) art 12; ICCPR (n 15) art 17.

[52] Council of Europe, *European Convention on Human Rights* (Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols) (ECHR 2013) art 10; ICCPR (n 15) art 19.

[53] *Standard Verlagsgesellschaft mbH v Austria (No 3)* App no 21277/19 (ECtHR, 7 December 2021) <https://hudoc.echr.coe.int/fre?i=001-213914> accessed 10 April 2025.

[54] Matthias C Kettemann and others, *UNESCO Recommendation on the Ethics of Artificial Intelligence: Conditions for the implementation in Germany* (German Commission for UNESCO 2023).

2.3.5. Right to Be Forgotten

The right to be forgotten reflects one of the most human aspirations in the digital age, the wish to move on from the past and regain control over one's own story. The legal recognition of this right has developed most clearly within the European Union, where it emerged from the long-standing commitment to privacy and data protection. The landmark *Google Spain SL and Google Inc. v. AEPD and Mario Costeja González* (Case C-131/12)[55] captured this idea in a remarkably personal way, when an ordinary citizen sought to erase outdated information that no longer accurately defined who he was. The Court of Justice ruled that individuals may ask search engines to delist links containing outdated or irrelevant personal data, provided this does not override the public's right to know. The decision transformed a private grievance into a principle of digital dignity, later codified in Article 17 of the General Data Protection Regulation (GDPR), which formally grants individuals the right to request the erasure of their personal data.[56]

Later cases, such as *Google LLC v. CNIL* (Case C-507/17),[57] further clarified the boundaries of the right to be forgotten. The Court of Justice affirmed that while individuals deserve the chance to outgrow their digital past, this right cannot extend without limit; it must be balanced with freedom of expression and the public interest. The result is not a promise of invisibility but a nuanced recognition that every person has the right to be more than the sum of their search results.[58]

Yet the challenges today go far beyond search engines. In an era dominated by big data and AI, personal information is not merely stored; it is constantly inferred, replicated, and reassembled by systems that learn from the digital traces individuals leave behind. AI models trained on personal data may reproduce information long after it has been deleted from public sources, raising new questions about whether technological forgetting is even possible.

Still, scholars such as Paolucci[59] emphasise that the right to be forgotten carries profound moral weight; it restores a sense of agency and redemption, allowing individuals to reclaim their narrative from the permanence of the digital archive. In this sense, the right is not only a legal tool but a deeply human one, anchored in dignity, mercy, and the universal need for renewal. It recognises that the digital world—like life itself—should allow space for growth, change, and new beginnings.

[55] Case C-131/12 *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (CJEU (Grand Chamber), 13 May 2014) <https://curia.europa.eu/juris/liste.jsf?num=C-131/12> accessed 10 April 2025.

[56] '*Google Spain SL v Agencia Española de Protección de Datos*: Comment Case C-131/12 (May 13, 2014)' (2014) 128(1) *Harvard Law Review* 282.

[57] Case C-507/17 *Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL)* (CJEU, 24 Septembe 2019) <https://curia.europa.eu/juris/liste.jsf?language=en&num=C-507/17> accessed 10 April 2025.

[58] Mary Samonte, 'Google v CNIL: The Territorial Scope of the Right to Be Forgotten Under EU Law' (2020) 4(3) European Papers 839. doi:10.15166/2499-8249/332.

[59] Paolucci (n 47).

These five digital rights—privacy, internet access, data protection, anonymity, and the right to be forgotten—provide the conceptual framework for evaluating national regulatory approaches. Across global contexts, three findings stand out. First, the *normative core* of human rights remains stable, but their *application* in digital environments varies depending on governance models and technological capabilities. Second, while the European Union leads with legally enforceable standards like the GDPR and AI Act, other regions, including MENA, still rely heavily on ethical or strategic frameworks. Third, the rise of artificial intelligence introduces new tensions between innovation and protection, as data-driven decision-making often exceeds traditional accountability mechanisms. These results highlight the importance of context-specific approaches to digital rights governance. In particular, the MENA region, characterised by rapid technological transformation, strong state involvement, and deeply rooted ethical traditions, offers a distinctive perspective on how universal digital rights are being adapted in practice.

3 DIGITAL RIGHTS AND AI IN THE MENA CONTEXT

3.1. Regional Regulatory Frameworks and Emerging AI Strategies

Building on the conceptual and legal foundation discussed earlier, this section examines how these universal principles translate into regional contexts, particularly in the Middle East and North Africa (MENA) region. Governance approaches to digital rights and AI in the MENA region reflect distinctive regional dynamics and priorities.

Ismail and Ahmad[60] observe that digital transformation across the region has progressed rapidly but unevenly, with Gulf Cooperation Council (GCC) countries generally establishing more advanced governance frameworks than other MENA nations. These differences stem from varying resource availability, institutional capacity, and prioritisation of digital development within national strategies. Several GCC countries have adopted comprehensive AI strategies that engage with both innovation and governance dimensions. The UAE's National Strategy for Artificial Intelligence (2017) was among the first in the region, establishing "responsible AI" as a core pillar alongside economic development goals.[61] Similarly, Qatar's National Artificial Intelligence Strategy emphasises ethical principles including fairness, transparency, and human-centred design.[62]

[60] Osama Ismail and Naim Ahmad, 'Ethical and Governance Frameworks for Artificial Intelligence: A Systematic Literature Review' (2025) 19(14) International Journal of Interactive Mobile Technologies121. doi:10.3991/ijim.v19i14.5698.

[61] UAE Government, *UAE Strategy for Artificial Intelligence (2017-2031)* (UAE Minister of State for Artificial Intelligence Office 2017) <https://ai.gov.ae/> accessed 10 April 2025.

[62] Qatar Ministry of Communications and Information Technology, *National Artificial Intelligence Strategy for Qatar* (MCIT 2019) <https://www.mcit.gov.qa/en/> accessed 10 April 2025.

Many MENA states draw significantly from international frameworks while adapting governance approaches to regionally specific cultural contexts. Qatar's Data Protection Law[63] incorporates GDPR-inspired provisions while reflecting local legal traditions. Similarly, Bahrain's Personal Data Protection Law[64] establishes rights and principles aligned with international standards while maintaining flexibility for national security considerations. The intersection of Islamic legal principles with digital rights frameworks represents a distinctive aspect of regional governance approaches.

Regional cooperation initiatives on digital governance have emerged through bodies including the Arab League and the Gulf Cooperation Council. The Arab Strategy for Information Security and Digital Technologies establish shared principles and cooperation mechanisms, though implementation remains primarily national.[65] As Fatafata and Samaro[66] note, regional initiatives have focused more on cybersecurity cooperation than on comprehensive digital rights frameworks.

Despite these developments, the academic literature on AI ethics and digital rights in the MENA region remains relatively limited compared to the European and North American context.[67] Significant gaps persist in region-specific research on algorithmic fairness, cultural adaptation of AI ethics principles, and implementation studies of digital rights frameworks. This underscores the need for expanded scholarship examining distinctive regional approaches and challenges rather than simply applying external frameworks.

3.2. The Role of Islamic Legal and Ethical Principles

A distinctive feature of AI and digital governance in the MENA context is the interaction between emerging digital rights frameworks and deep-rooted Islamic legal and ethical principles. Ethical foundations derived from *maqāṣid al-sharīʿah*, can enrich regional interpretations of privacy, dignity, justice, and trust as dynamic governance criteria (e.g. *hurmah al-insān*, *adl*, *amānah*). However, integrating these values into AI policy demands more than rhetorical invocation; it demands methodological translation, normative calibration, and institutional embedding.

[63] Law of the State of Qatar No 13 of 2016 'On Personal Data Privacy Protection', amended Law No 19 of 2021 <https://www.almeezan.qa/LawView.aspx?opt&LawID=7121&language=ar> accessed 10 April 2025.

[64] Law of the Kingdom of Bahrain No 30 of 2018 'On Personal Data Protection' <https://www.bahrain.bh/wps/wcm/connect/ab8b334e-8c6f-4ff9-90b6-94135da559ca/Law+No.+%2830%29+of+2018+DPL.pdf?MOD=AJPERES&CVID=oFapPNI > accessed 10 April 2025.

[65] ESCWA and League of Arab States, *Arab Digital Agenda 2023-2033: Arab States Action Programme on Advancing Digital Cooperation and Development* (edn 1.0, UN 2024) <https://www.unescwa.org/publications/arab-digital-agenda-2023-2033> accessed 10 April 2025.

[66] Marwa Fatafta and Dima Samaro, *Exposed and Exploited: Data Protection in the Middle East and North Africa* (Access Now 2021) <https://www.skeyesmedia.org/en/News/Reports/29-01-2021/9098> accessed 15 November 2025.

[67] Gulf Cooperation Council, *The Guiding Manual on the Ethics of Artificial Intelligence Use in Member States of the Gulf Cooperation Council (GCC)* (Version 1.0, GCC General Secretariat 2023).

Several scholars have explored how Islamic ethics might inform distinctive approaches to emerging challenges such as algorithmic decision-making, data ownership, and privacy by design. In recent research, Ali et al.[68] maintain that Islamic ethics can contribute as a pluralist benchmark for AI evaluation, combining textual sources (*Qur'an, Sunnah*) with *maslahah* (public benefit) and *maqāṣid* reasoning in a dynamic, context-sensitive manner. Elmahjub[69] argues that Islamic ethics should not be considered a static overlay, but rather a living tradition capable of negotiating tensions such as privacy versus utility or fairness versus efficiency through a purpose-based moral methodology.

Islamic jurisprudence provides a set of ethical imperatives that align closely with contemporary human rights standards. Principles such as *hurmah al-insan* (human dignity), *adl* (justice), and *amanah* (trust) resonate strongly with modern values of transparency, accountability, and respect for personal data. As AlKubaisi[70] argues, these principles can complement and reinforce digital rights protections when appropriately integrated into governance frameworks. Trust and responsibility, captured by the concept of *amānah*, are especially important when AI systems are involved in human affairs. From an Islamic perspective, ethical AI should hold developers and users responsible for handling sensitive data and decisions, using tools like audits, clear explanations, and ways to address problems. Western AI ethics are not entirely devoted to this more profound sense of moral accountability; in this regard, Islamic ideas of trusteeship (*amānah*) can offer new ways to embed responsibility into AI systems.

Islamic ethics can make AI governance more meaningful and humane; however, there are still challenges in translating Islamic ethical ideals into a clear regulatory system, especially without a clear, binding legal framework, independent Sharia-based ethical audits, or certified compliance programs. These ideals may not be put into practice.

4 THE INTERSECTION BETWEEN AI GOVERNANCE AND DIGITAL HUMAN RIGHTS IN INTERNATIONAL LEGAL FRAMEWORKS

The intersection between AI governance and digital human rights in international legal frameworks reveals significant variations in regulatory philosophy and implementation strategies. Different jurisdictions have struck varying balances between innovation and rights protection. The European approach generally applies what Jasanoff[71] terms a "precautionary principle," establishing substantial oversight before technologies enter the

[68] Ali and others (n 27).

[69] Elmahjub (n 26).

[70] Abdel Aziz Shaker Hamdan AlKubaisi, 'Ethics of Artificial Intelligence a Purposeful and Foundational Study in Light of the Sunnah of Prophet Muhammad' (2024) 15(11) Religions 1300. doi:10.3390/rel15111300.

[71] Sheila Jasanoff, *The Ethics of Invention: Technology and the Human Future* (WW Norton & Company 2016).

market. The American approach has historically emphasised innovation with more limited *ex-ante* restrictions, relying more heavily on market forces and ex-post remedies. Asian approaches often frame AI governance as "enabling innovation" through guidelines and certification rather than comprehensive restrictions.

Yet despite their differences, most jurisdictions face similar challenges when implementing digital rights frameworks. One challenge concerns the elastic nature of concepts such as "fairness" and "transparency," which are subject to varying interpretations, resulting in persistent definitional ambiguity. A second challenge arises from the technical verification difficulties that emerge when assessing complex socio-technical systems that cannot be fully predicted through traditional compliance mechanisms. A third challenge is the "expertise gap" between regulators and the regulated entities they oversee; regulatory bodies often lack the specialised technical capacity to effectively evaluate AI systems for compliance with abstract principles. These issues collectively explain why translating human rights norms into effective AI governance remains an unfinished global project.

4.1. The European AI Act: A Milestone in Human-Rights-Centred Regulation

Against this fragmented background, the European Union's AI Act, which was proposed in 2021 and entered into force on 1 August 2024, stands as the first comprehensive and binding legal framework allocated to managing the dangers and responsibilities of AI.[72] Its central aim is to reconcile technological innovation with the protection of human dignity and fundamental rights.

The Act classifies AI systems according to their potential risk—ranging from prohibited to high, limited, and minimal—with each category carrying corresponding duties relating to transparency, human oversight, and accountability (EU AI Act, Arts. 5–9).[73] For example, the Act prohibits the use of AI for social scoring or real-time biometric surveillance in public spaces, considering these practices incompatible with human dignity. Systems used in law enforcement, healthcare, employment, or education fall into the high-risk category and must undergo strict risk assessments, provide traceable documentation, and ensure that humans remain in control of key decisions.[74] By contrast, tools such as chatbots or emotion-recognition software—classified as limited-risk—are mainly required to inform users that they are interacting with AI, while minimal-risk systems such as spam filters face no additional regulation.[75]

[72] Regulation (EU) 2024/1689 (n 12).

[73] ibid, arts 5–9.

[74] ibid, arts 6(2), 9, 11, 14, 15; annex III (high-risk systems: law enforcement, healthcare, employment, education).

[75] ibid, art 50; recital 60 (transparency duties for limited-risk systems; no specific obligations for minimal-risk AI).

This system of categorisation, however, is not without limitations. Some technologies formally labelled as "low risk" may still raise deep ethical concerns, especially when their algorithms amplify bias, manipulate emotions, or operate in an opaque manner.

Despite its ambition, the Act has faced criticism for its ambiguous terminology, reliance on private standard-setting bodies, and limited enforcement pathways. Nevertheless, it remains a historic milestone, transforming abstract principles like privacy, fairness, and non-discrimination into enforceable obligations.

The widespread use of artificial intelligence systems has created a need to adopt mandatory legal measures to protect them, ensure their safety, and guarantee their accountability and adherence to human rights. The lack of binding legislative norms issued by international legislative bodies has left significant gaps in the central part. These gaps in the accountability system reflect a broader challenge of attributing criminal or moral responsibility when algorithmic systems contribute to harmful outcomes. As Abdelaziz[76] argues, the shift from physical to virtual life for human beings has blurred the traditional boundaries of liability, a shift that urgently requires comparative legal systems to rethink how intent, causation, and foreseeability apply to AI-mediated harm.

4.2. Soft-Law Approaches: UNESCO and OECD Frameworks

Beyond the European Union, many international organisations, such as the United Nations, have taken steps to develop ethical baselines for AI safe development and use of artificial intelligence and on the path of the leading world organisations, the Islamic World Educational, Scientific and Cultural Organisation (ICESCO) and the Saudi Data and Artificial Intelligence Authority launched in 2024 the Riyadh Charter for Artificial Intelligence in the Islamic World, which aims to establish an ethical framework for the development and use of artificial intelligence in line with the principles of Islamic moral traditions.

The UNESCO Recommendation on the Ethical Use of Artificial Intelligence, adopted by 193 member countries in November 2021, is particularly significant.[77] Unlike binding regulatory instruments, which rely on prohibitions and strict compliance measures, the Recommendation adopts a life-cycle approach that emphasises human dignity, the protection of individuals' privacy, and the inclusion of people in the development of AI. It challenges states to embed human rights into AI governance and seeks to ensure that technological innovation strengthens societies, respects liberty, and unites individuals. Its holistic approach sets out ten core principles—proportionality, safety and security, privacy and data protection, governance, inclusivity, responsibility and accountability, transparency and explainability, sustainability, human oversight, public AI literacy, and fairness and unbiased AI.

[76] Dalia Kadry Ahmed Abdelaziz, 'Incitement to Suicide in the Digital Age: A Comparative Legal Study of Criminal Liability' (2025) 5(6) Journal of Posthumanism 684. doi:10.63332/joph.v5i6.2105

[77] UNESCO (n 10).

Similarly, the OECD AI guidelines offer a set of recommendations with clear aims for the responsible stewardship of the development and use of AI that respects and protects human rights and includes democratic rights and core freedoms.[78] These principles were adopted by OECD member countries and remain a significant step towards the formation of an AI regulatory framework. The OECD AI Principles share significant similarities with UNESCO’s principles regarding inclusiveness, collaboration, openness, and responsibility.[79] The principles also provide that, to ensure fair and balanced rights for individuals, the AI systems used to process and reach decisions that affect people should be transparent and explainable to all stakeholders involved.

5 DIGITAL HUMAN RIGHTS WITHIN THE SAUDI ARABIA’S LEGAL FRAMEWORK: A PRELIMINARY ASSESSMENT

The Kingdom of Saudi Arabia has developed a multi-layered legal framework governing digital activities and data protection, comprising the Personal Data Protection Law (PDPL, 2021, amended 2023), the Anti-Cyber Crime Law (2007), and various sector-specific regulations. This framework operates within the broader context of Vision 2030, which explicitly prioritises digital transformation while recognising the need for rights protections.[80]

The regulatory architecture reflects a hybrid approach: comprehensive data protection provisions modelled on international standards[81] (particularly GDPR-inspired elements in the PDPL) coexist with cybersecurity legislation predating the AI era. The Saudi Data and Artificial Intelligence Authority (SDAIA) has issued AI Ethics Principles (2023), though these remain non-binding guidance rather than enforceable law. The Saudi Data and Privacy Protection Authority (SDPPA) serves as the primary enforcement body for data protection.[82]

This section evaluates Saudi Arabia's framework against the international benchmarks established in Section 3, examining both areas of alignment with global standards and regulatory gaps that limit comprehensive digital rights protection in AI-driven contexts. The analysis begins by assessing the achievements of the PDPL, before examining its limitations, and before turning to the contemporary relevance of the Anti-Cybercrime Law. The section concludes with a comparative assessment of the Kingdom's overall positioning within international governance models.

[78] OECD (n 9); ‘OECD AI Principles’ (*OECD*, 2025) <https://www.oecd.org/en/topics/ai-principles.html> accessed 6 October 2025.

[79] Nicholas Kluge Corrêa and others, ‘Worldwide AI Ethics: A Review of 200 Guidelines and Recommendations for AI Governance’ (2023) 4(10) Patterns 100857. doi:10.1016/j.patter.2023.100857.

[80] Mohammad Rashed Albous, Odeh Rashed Al-Jayyousi and Melodena Stephens, ‘AI Governance in the GCC States: A Comparative Analysis of National AI Strategies’ (2025) 82 Journal of Artificial Intelligence Research 2389. doi:10.1613/jair.1.17619.

[81] Bendary and Rajadurai (n 21).

[82] Ibrahim (n 14).

5.1. Personal Data Protection Law (PDPL)

The Personal Data Protection Law (PDPL), enacted on 16 September 2021 and amended on 27 March 2023,[83] constitutes Saudi Arabia's primary legal framework for data protection. Enforced by the Saudi Data and Privacy Protection Authority (SDPPA), the PDPL establishes comprehensive provisions governing the collection, processing, and storage of personal information, demonstrating the Kingdom's recognition of data privacy as an essential component of digital rights protection.

The PDPL reflects influence from established international frameworks, particularly the Council of Europe's Convention 108[84] and the EU's General Data Protection Regulation (GDPR).[85] The law incorporates several internationally recognised principles, including purpose limitation, data minimisation, and consent requirements for data processing. Article 5 mandates explicit consent for data processing, while Article 12 imposes transparency requirements for data use. Article 19 enforces data minimisation principles, requiring data collection to be limited to essential information.[86] These provisions constitute the foundational legal framework for digital human rights in Saudi Arabia, particularly regarding the right to informational self-determination that enables individuals to exercise control over their personal information.[87]

The Kingdom has successfully implemented additional protective measures that mirror global best practices. Article 24 requires data breach notification to both authorities and affected individuals without undue delay—a provision consistent with leading international data protection regulations. Article 32 mandates the appointment of Data Protection Officers within organisations that process personal data, and establishes an internal compliance mechanism.[88] The establishment of the SDPPA as a dedicated regulatory body reflects international trends toward specialised data protection oversight, providing institutional capacity for enforcement and guidance. The law grants individuals specific rights regarding their personal data, including access, correction, and deletion rights, demonstrating the Kingdom's commitment to empowering citizens with meaningful

[83] Royal Decree of the Kingdom of Saudi Arabia No M/19 of 09/02/1443 AH (n 14).

[84] Council of Europe, *Convention 108 + : Convention for the Protection of Individuals with Regard to the Processing of Personal Data* (CoE 2018) <https://www.coe.int/en/web/data-protection/convention108-and-protocol> accessed 6 October 2025.

[85] Regulation (EU) 2016/679 (n 46).

[86] Mutaz Abdulaziz Alkhedhairy, 'Balancing Privacy and Risk: A Critical Analysis of Personal Data Use as Governed by Saudi Insurance Law' (2025) 14(4) Laws 47. doi:10.3390/laws14040047.

[87] Nick O'Connell, 'An overview of Saudi Arabia's new Personal Data Protection Law' (*Al Tamimi & Co*, September 2021) <https://www.tamimi.com/law-update-articles/an-overview-of-saudi-arabias-new-personal-data-protection-law/> accessed 15 November 2025.

[88] Marianne Rahme, 'Data Protection in Saudi Arabia: Comparative Analysis General Data Protection Regulation Kingdom of Saudi Arabia KSA' (*SMEX*, 10 February 2022) <https://smex.org/data-protection-in-saudi-arabia-comparative-analysis/> accessed 15 November 2025.

control over their personal information. Substantial penalties for non-compliance—potentially reaching 5 million Saudi Riyals (approximately 1.3 million USD) for serious violations—signal strong enforcement commitment.[89]

Despite these achievements, several areas reveal divergence from international best practices and warrant additional attention to address contemporary technological challenges. Article 16 delineates multiple circumstances that permit the waiver of consent requirements, including public interest, vital interests protection, national security considerations, credit referencing, and research purposes. These exceptions, though providing operational flexibility, create broader latitude than comparable provisions in the GDPR, which may weaken the foundational principle of informed consent that underpins modern data protection regimes.

The current legal framework provides limited algorithmic accountability provisions, creating gaps in oversight of AI decision-making systems that increasingly affect citizens' lives across sectors, from employment to public services. The law currently lacks specific provisions addressing emerging technological applications. Spatiotemporal data and AI-generated information receive limited attention despite their widespread use across healthcare, transportation, and smart city initiatives. Post-mortem data processing, particularly regarding facial recognition and predictive analytics, lacks clear regulatory guidelines. Additionally, the framework does not explicitly address bias mitigation in automated systems or transparency requirements for AI decision-making processes, creating a significant regulatory gap, as the Kingdom lacks unified legislation that addresses the full spectrum of AI-related rights and risks.[90]

These gaps create challenges for comprehensive digital rights protection as artificial intelligence and machine learning technologies expand throughout Saudi society. Developing provisions for algorithmic transparency and accountability would strengthen the framework's capacity to address automated decision-making in employment, judicial processes, and public services. As the Kingdom advances its digital transformation agenda under Vision 2030, evolving the PDPL to encompass these emerging areas would enhance alignment with international best practices while supporting technological innovation objectives.

[89] 'Penalties for Non-Compliance with PDPL' (*Standard Touch*, 2025) <https://standardtouch.com/pdpl-penalties-saudi-arabia/> accessed 6 October 2025.

[90] Adamantia Rachovitsa, 'Engineering and Lawyering Privacy by Design: Understanding Online Privacy Both as a Technical and An International Human Rights Issue' (2016) 24(4) *International Journal of Law and Information Technology* 374. doi:10.1093/ijlit/eaw012.

5.2. 2007 Anti-Cybercrime Law and Digital Rights Implications

The 2007 Anti-Cybercrime Law[91] complements the PDPL but predates both contemporary data protection standards and the proliferation of AI technologies. Article 3(1) prohibits unauthorised data interception through information networks. Article 3(4) addresses privacy invasion through mobile devices and similar technologies.[92] These provisions establish baseline privacy protections but do not explicitly address AI-powered surveillance technologies such as facial recognition systems or predictive analytics.[93]

Article 6(1) regulates content production and transmission that impinges on public order, religious values, or privacy. Article 7(2) addresses unauthorised system access that may result in the obtaining of data relevant to national security or economic interests. These provisions provide flexibility for addressing evolving threats but lack specific guidance on algorithmic content moderation or AI-driven security measures. Such systems currently operate throughout the Kingdom, including biometric identification at border entry points, the ABSHER digital government services platform,[94] and AI-powered urban management technologies deployed in NEOM smart city initiatives.[95]

Article 14 designates the Communications and Information Technology Commission to provide technical support to security agencies during investigations. The law does not address algorithmic bias in automated enforcement systems, transparency requirements for AI-powered investigative tools, or citizens' rights to challenge automated decisions.[96] International courts have increasingly recognised these gaps as human rights concerns. The European Court of Human Rights found that mass surveillance systems lacking adequate safeguards violate privacy rights in *Big Brother Watch and Others v. United Kingdom* (Apps. Nos 58170/13, 62322/14 and 24960/15).[97] The Court of Justice of the European Union invalidated data transfer mechanisms where surveillance frameworks

[91] Royal Decree of the Kingdom of Saudi Arabia No M/17 of 8 Rabi'I 1428H 'Anti-Cyber Crime Law' (26 March 2007) <https://www.wipo.int/wipolex/en/legislation/details/14570> accessed 10 April 2025.

[92] Selma Dilek, Hüseyin Çakır and Mustafa Aydın, 'Applications of Artificial Intelligence Techniques to Combating Cybercrimes: A Review' (*arXiv preprint,* 12 February 2015) arXiv:1502.03552. doi:10.48550/arXiv.1502.03552.

[93] Thomas C King and others, 'Artificial Intelligence Crime: An Interdisciplinary Analysis for Foreseeable Threats and Solutions' (2020) 26 Science and Engineering Ethics 89. doi:10.1007/s11948-018-00081-0.

[94] Ministry of Interior of the Kingdom of Saudi Arabia, *Absher Platform* (2025) <https://www.absher.sa/portal/landing.html> accessed 6 October 2025.

[95] NEOM, 'Technology and Digital' (*NEOM Official Website*, 2025) <https://www.neom.com> acsessed 6 October 2025.

[96] Cristos Velasco, 'Cybercrime and Artificial Intelligence. An Overview of the Work of International Organization on Criminal Justice and the International Applicable Instruments' (2022) 23 ERA Forum 109. doi:10.1007/s12027-022-00702-z.

[97] *Big Brother Watch and Others v United Kingdom* Apps nos 58170/13, 62322/14 and 24960/15 (ECtHR, 25 May 2021) <https://hudoc.echr.coe.int/fre?i=001-210077> accessed 6 October 2025.

provided insufficient individual protections.[98] The CJEU also recognised individuals' rights to request deletion of inadequate or outdated personal data, a principle not yet incorporated into Saudi legislation.[99]

The 17-year gap between the law's enactment and current AI capabilities underscores the need for updated provisions that address algorithmic accountability and transparency. Developing such provisions would strengthen the Kingdom's framework capacity to balance security objectives with digital rights protections as AI technologies expand throughout Saudi society.

6 CONCLUSION AND RECOMMENDATIONS

K.S.A has established foundational digital governance structures that demonstrate general alignment with international standards, particularly through the Personal Data Protection Law (2021, amended 2023) and the creation of specialised regulatory institutions. The PDPL incorporates core data protection principles, including purpose limitation, data minimisation, consent requirements, and breach notification, while granting individuals meaningful rights over their personal information. These achievements position the Kingdom comparably to other jurisdictions pursuing digital transformation under comprehensive data protection regimes.

However, the accelerating deployment of AI systems across governance, healthcare, education, and smart city infrastructure has outpaced the legal framework's capacity to address algorithmic decision-making. Three critical gaps persist: the PDPL does not recognise data protection as a fundamental human right; neither the PDPL nor the 2007 Anti-Cybercrime Law adequately addresses AI-specific challenges, including algorithmic accountability, bias mitigation, and transparency requirements; and fragmented regulatory oversight leaves individuals without clear mechanisms to challenge automated decisions affecting their interests.

The path forward requires targeted legal reforms. Amending the PDPL to explicitly recognise data protection as a fundamental right would strengthen its constitutional foundation. Comprehensive AI governance legislation that consolidates SDAIA's ethical guidelines into binding requirements would establish clear obligations for high-risk applications, mandatory transparency standards, and enforceable bias-prevention measures. Expanding the PDPL's scope to explicitly cover AI-generated data, biometric information, and spatiotemporal analytics would address technological developments since

[98] Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* (CJEU (Grand Chamber), 16 July 2020) <https://curia.europa.eu/juris/liste.jsf?num=C-311/18> accessed 6 October 2025.

[99] Case C-131/12 *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (n 55).

the law's enactment. Strengthening enforcement mechanisms—including accessible complaint procedures, rights to explanation for automated decisions, and meaningful remedies for violations—would transform abstract protections into actionable rights.

KSA's distinctive position presents both challenge and opportunity. The Kingdom is undergoing accelerated digital transformation while simultaneously integrating Islamic ethical principles into its legal system. Operationalising concepts of human dignity (*hurmah al-insan*), justice (*adl*), and trust (*amanah*) within technical standards and compliance frameworks would position the KSA model for governance approaches that harmonise international norms with cultural values. Rather than viewing Vision 2030's technological ambitions and robust rights protections as competing imperatives, the Kingdom can demonstrate their mutual reinforcement—innovation flourishes most sustainably within frameworks that safeguard human dignity and accountability.

By addressing these regulatory gaps through comprehensive legal reform, Saudi Arabia can establish itself as a regional leader in rights-based AI governance, demonstrating that rapid technological advancement and fundamental rights protection are not opposing forces but complementary pillars of sustainable digital transformation.

REFERENCES

1. Abdelaziz DKA, 'Incitement to Suicide in the Digital Age: A Comparative Legal Study of Criminal Liability' (2025) 5(6) Journal of Posthumanism 684. doi:10.63332/joph.v5i6.2105
2. Albous MR, Al-Jayyousi OR and Stephens M, 'AI Governance in the GCC States: A Comparative Analysis of National AI Strategies' (2025) 82 Journal of Artificial Intelligence Research 2389. doi:10.1613/jair.1.17619
3. Alhejaili MOM, 'Integrating Smart Contracts into the Legal Framework of Saudi Arabia' (2025) 67(2) International Journal of Law and Management 230. doi:10.1108/IJLMA-03-2024-0086
4. Alhejaili MOM, 'Securing the Kingdom's e-Commerce Frontier: Evaluation of Saudi Arabia's Cybersecurity Legal Frameworks' (2024) 13(2) Journal of Governance & Regulation 275. doi:10.22495/jgrv13i2siart4
5. Ali F and others, 'Islamic Ethics and AI: An Evaluation of Existing Approaches to AI using Trusteeship Ethics' (2025) 38(2) Philosophy & Technology 120. doi:10.1007/s13347-025-00922-4
6. Alkhedhairy MA, 'Balancing Privacy and Risk: A Critical Analysis of Personal Data Use as Governed by Saudi Insurance Law' (2025) 14(4) Laws 47. doi:10.3390/laws14040047
7. AlKubaisi AASH, 'Ethics of Artificial Intelligence a Purposeful and Foundational Study in Light of the Sunnah of Prophet Muhammad' (2024) 15(11) Religions 1300. doi:10.3390/rel15111300

8. AllahRakha N, ‘UNESCO's AI Ethics Principles: Challenges and Opportunities’ (2024) 2(9) *International Journal of Law and Policy* 24. doi:10.59022/ijlp.225
9. Alzahrani RB, ‘An Overview of AI Data Protection in the Context of Saudi Arabia’ (2024) 3(3) International Journal for Scientific Research 199. doi:10.59992/IJSR.2024.v3n3p8 [in Arabic]
10. Andrews SS, ‘Copyright Originality in the Digital Space: The Kingdom of Saudi Arabia’s Creatives’ in Gupta I (ed), *Handbook on Originality in Copyright: Cases and Materials* (Springer 2023) 1. doi:10.1007/978-981-19-1144-6_9-1
11. Bendary MG and Rajadurai J, ‘Emerging Technologies and Public Innovation in the Saudi Public Sector: An Analysis of Adoption and Challenges Amidst Vision 2030’ (2024) 29(1) The Innovation Journal: The Public Sector Innovation Journal 1
12. Cerf V, ‘Internet Access is Not a Human Right’ *The New York Times* (New York, 4 January 2012) A25
13. Cong W, ‘Understanding Human Rights on the Internet: An Exercise of Translation?’ (2017) 22(1-2) Tilburg Law Review 138. doi:10.1163/22112596-02201007
14. Custers B, ‘New Digital Rights: Imagining Additional Fundamental Rights for the Digital Era’ (2022) 44 *Computer Law & Security Review* 105636. doi:10.1016/j.clsr.2021.105636
15. De Hert P and Kloza D, ‘Internet (access) as a New Fundamental Right: Inflating the Current Rights Framework?’ (2012) 3(3) European Journal of Law and Technology 1
16. Dilek S, Çakır H and Aydın M, ‘Applications of artificial intelligence techniques to combating cybercrimes: A review’ (*arXiv preprint,* 12 February 2015) arXiv:1502.03552. doi:10.48550/arXiv.1502.03552
17. Elmahjub E, ‘Artificial Intelligence (AI) in Islamic Ethics: Towards Pluralist Ethical Benchmarking for AI’ (2023) 36(4) Philosophy & Technology 73. doi:10.1007/s13347-023-00668-x
18. Fatafta M and Samaro D, *Exposed and Exploited: Data Protection in the Middle East and North Africa* (Access Now 2021)
19. Fjeld G and others, *Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI* (Berkman Klein Center for Internet & Society Research Publication Series no 2020-1, Harvard University 2020). doi:10.2139/ssrn.3518482
20. Hildebrandt M, *Smart Technologies and the End(s) of Law* (Edward Elgar 2015)
21. Ibrahim NMH, ‘Artificial Intelligence (AI) and Saudi Arabia’s Governance’ (2024) 40(4) Journal of Developing Societies 500. doi:10.1177/0169796X241288590

22. Ismail O and Ahmad N, 'Ethical and Governance Frameworks for Artificial Intelligence: A Systematic Literature Review' (2025) 19(14) International Journal of Interactive Mobile Technologies121. doi:10.3991/ijim.v19i14.5698

23. Jasanoff S, *The Ethics of Invention: Technology and the Human Future* (WW Norton & Company 2016)

24. Jobin A, Ienca M and Vayena E, 'The Global Landscape of AI Ethics Guidelines' (2019) 1(9) Nature Machine Intelligence 389. doi:10.1038/s42256-019-0088-2

25. Jørgensen RF, *Framing the Net: The Internet and Human Rights* (Edward Elgar 2013). doi:10.4337/9781782540809

26. Kettemann MC and others, *UNESCO Recommendation on the Ethics of Artificial Intelligence: Conditions for the implementation in Germany* (German Commission for UNESCO 2023)

27. King TC and others, 'Artificial Intelligence Crime: An Interdisciplinary Analysis for Foreseeable Threats and Solutions' (2020) 26 Science and Engineering Ethics 89. doi:10.1007/s11948-018-00081-0

28. Kluge Corrêa N and others, 'Worldwide AI Ethics: A Review of 200 Guidelines and Recommendations for AI Governance' (2023) 4(10) Patterns 100857. doi:10.1016/j.patter.2023.100857

29. Kostenko OM and others, '"Legal Personality" of Artificial Intelligence: Methodological Problems of Scientific Reasoning by Ukrainian and EU Experts' (2023) 39(4) AI and Society 1683. doi:10.1007/s00146-023-01641-0

30. Land MK and Aronson JD (eds), *New Technologies for Human Rights Law and Practice* (CUP 2018) doi:10.1017/9781316838952

31. Larsson S and Heintz F, 'Transparency in Artificial Intelligence' (2020) 9(2) Internet Policy Review. doi:10.14763/2020.2.1469

32. Mathiesen K, 'The Human Right to Internet Access: A Philosophical Defense' (2012) 18 The International Review of Information Ethics 9. doi:10.29173/irie299

33. O'Connell N, 'An overview of Saudi Arabia's new Personal Data Protection Law' (*Al Tamimi & Co*, September 2021) <https://www.tamimi.com/law-update-articles/an-overview-of-saudi-arabias-new-personal-data-protection-law/> accessed 15 November 2025.

34. Pangrazio L and Sefton-Green J, 'Digital Rights, Digital Citizenship and Digital Literacy: What's the Difference?' (2021) 10(1) *Journal of New Approaches in Educational Research* 15. doi:10.7821/naer.2021.1.616

35. Paolucci F, 'Enhancing Oversight and Addressing Gaps: Assessing the Impact of the AI Act on Biometric Identification Systems' in Menéndez González N and Mobilio G (eds), *Next Democratic Frontiers for Facial Recognition Technology (FRT): The Legal, Ethical and Democratic Implications of FRT* (Springer 2025) 71. doi:10.1007/978-3-031-89794-8_5

36. Penney J, 'Open Connectivity, Open Data: Two Dimensions of the Freedom to Seek, Receive and Impart Information in the New Zealand Bill of Rights' (2012) 4 Victoria University of Wellington Law Review: Working Paper Series 1

37. Rachovitsa A, 'Engineering and Lawyering Privacy by Design: Understanding Online Privacy Both as a Technical and An International Human Rights Issue' (2016) 24(4) *International Journal of Law and Information Technology* 374. doi:10.1093/ijlit/eaw012

38. Rahme M, 'Data Protection in Saudi Arabia: Comparative Analysis General Data Protection Regulation Kingdom of Saudi Arabia KSA' (*SMEX*, 10 February 2022) <https://smex.org/data-protection-in-saudi-arabia-comparative-analysis/> accessed 15 November 2025.

39. Reidenberg JR, 'Lex Informatica: The Formulation of Information Policy Rules Through Technology' (1997) 76(3) Texas Law Review 553

40. Samonte M, 'Google v CNIL: The Territorial Scope of the Right to Be Forgotten Under EU Law' (2020) 4(3) European Papers 839. doi:10.15166/2499-8249/332

41. Schwartz A, 'Chicago's Video Surveillance Cameras: A Pervasive and Poorly Regulated Threat to Our Privacy' (2013) 11(2) Northwestern Journal of Technology and Intellectual Property 47.

42. Tully S, 'A Human Right to Access the Internet? Problems and Prospects' (2014) 14(2) Human Rights Law Review 175. doi:10.1093/hrlr/ngu011

43. Veale M and Zuiderveen Borgesius F, 'Demystifying the Draft EU Artificial Intelligence Act' (2021) 22(4) Computer Law Review International 97. doi:10.9785/cri-2021-220402

44. Velasco C, 'Cybercrime and Artificial Intelligence. An Overview of the Work of International Organization on Criminal Justice and the International Applicable Instruments' (2022) 23 ERA Forum 109. doi:10.1007/s12027-022-00702-z

45. Vogel YA, 'Stretching the Limit, The Functioning of the GDPR's Notion of Consent in the context of Data Intermediary Services' (2022) 8(2) European Data Protection Law Review 238. doi:10.21552/edpl/2022/2/10

46. Winfield AFT and Jirotka M, 'Ethical Governance is Essential to Building Trust in Robotics and Artificial Intelligence Systems' (2018) 376(2133) Philosophical Transactions of the Royal Society A 20180085. doi:10.1098/rsta.2018.0085

AUTHORS INFORMATION

Soumaya Khammassi
PhD (Law), Assistant Professor, College of Law, Prince Sultan University, Riyadh, Saudia Arabia
skhammassi@psu.edu.sa
https://orcid.org/0009-0008-7810-0032

Co-author, responsible for conceptualization, methodology, investigation, writing – original draft and writing – review & editing.

Yusra AlShanqityi*
PhD (Law), Assistant Professor, College of Law, Prince Sultan University, Riyadh, Saudia Arabia
yshanqityi@psu.edu.sa
https://orcid.org/0009-0004-9275-2046

Corresponding author, responsible for conceptualization, methodology, investigation and writing – review & editing.

Competing interests: No competing interests were disclosed. Any potential conflict of interest must be disclosed by authors.

Disclaimer: The authors declare that their opinion and views expressed in this manuscript are free of any impact of any organizations.

RIGHTS AND PERMISSIONS

ADDITIONAL INFORMATION

The authors are thankful to the Governance and Policy Design Research Lab (GPDRL) and to Prince Sultan University for their academic support and for providing APC for this publication.

EDITORS

Managing Editor – Mag. Yuliia Hartman. **English Editor** – Julie Bold.
Ukrainian language Editor – Mag. Liliia Hartman.

ABOUT THIS ARTICLE

Cite this article

Khammassi S and AlShanqityi Y, 'Digital Rights, AI, and the Law: International Perspectives on Saudi Arabia's Legal Framework and International Experience' (2025) 8(Spec) Access to Justice in Eastern Europe 1-32 <https://doi.org/10.33327/AJEE-18-8.S-a000154> Published Online 08 Dec 2025

DOI: https://doi.org/10.33327/AJEE-18-8.S-a000154

Keywords: *digital rights, artificial intelligence, human rights, legislation, data protection, cybersecurity, privacy, e-government, Vision 2030.*

DETAILS FOR PUBLICATION

Date of submission: 16 Apr 2025
Date of acceptance: 08 Sep 2025
Online First publication: 08 Dec 2025
Last date of publication: December 2025
Whether the manuscript was fast tracked? - No
Number of reviewer report submitted in first round: 3 reports
Number of revision rounds: 1 round with conditionally acceptance

Technical tools were used in the editorial process:
Plagiarism checks - Turnitin from iThenticate https://www.turnitin.com/products/ithenticate/
Scholastica for Peer Review https://scholasticahq.com/law-reviews

AI DISCLOSURE STATEMENT

The corresponding author confirmed that the manuscript was written by the authors. AI tools (Claude and Grammarly) were used for spelling, grammar, stylistic refinement, and citation format verification. No generative AI was used to create original content, research ideas, or legal analyses.

АНОТАЦІЯ УКРАЇНСЬКОЮ МОВОЮ

Дослідницька стаття

ЦИФРОВІ ПРАВА, ШТУЧНИЙ ІНТЕЛЕКТ ТА ЗАКОНОДАВСТВО: МІЖНАРОДНІ ПЕРСПЕКТИВИ ЩОДО ПРАВОВОЇ СИСТЕМИ САУДІВСЬКОЇ АРАВІЇ Т А МІЖНАРОДНИЙ ДОСВІД

Сумая Хаммассі та Юсра Аль-Шанкіті*

АНОТАЦІЯ

Вступ. *У цьому дослідженні аналізується глобальна еволюція цифрових прав та управління штучним інтелектом, а також розглядаються наслідки для правової системи Саудівської Аравії. Оскільки штучний інтелект все більше впроваджується в повсякденне життя, існує нагальна потреба оцінити його вплив на основоположні права людини, особливо з огляду на відсутність глобального консенсусу щодо визначення та сфери застосування «цифрових прав людини». Ініціатива Королівства Саудівської Аравії (КСА) «Vision 2030» надає унікальну можливість розробити рамки управління ШІ, які відповідатимуть міжнародним стандартам і водночас відображатимуть місцеві культурні цінності та ісламські етичні принципи.*

Методи. *У цьому дослідженні використовується якісний аналітичний підхід для вивчення чинної правової бази Саудівської Аравії, яка регулює ШІ та цифрові права людини. Методологія передбачає комплексний аналіз законодавства Саудівської Аравії, зокрема Закону про захист персональних даних (PDPL) та етичних принципів Управління з питань даних та штучного інтелекту Саудівської Аравії (SDAIA), у порівнянні з міжнародними правовими інструментами, включно з Рекомендаціями ЮНЕСКО щодо етики штучного інтелекту, Законом ЄС про штучний інтелект та Принципами ОЕСР з питань штучного інтелекту. У статті оцінюється відповідність міжнародним стандартам та ефективність у вирішенні нових проблем, що стосуються цифрових прав в епоху ШІ.*

Результати та висновки. *Дослідження показує, що хоча Саудівська Аравія досягла прогресу завдяки структурам PDPL та SDAIA, все ж значні нормативні прогалини* *залишаються. PDPL має обмеження у вирішенні сучасних проблем у сфері штучного інтелекту, зокрема алгоритмічну підзвітність, зменшення упередженості та комплексний захист даних у контексті штучного інтелекту. У результаті дослідження було виявлено критичні недоліки, зокрема занадто широкі винятки щодо вимог стосовно згоди, недостатньо чіткі положення щодо прозорості алгоритмів і фрагментований регулятивний нагляд. Рекомендації передбачають створення спеціалізованих органів нагляду, розробку етичних рамок, адаптованих до контексту Саудівської Аравії, і більшого залучення експертів до ухвалення рішень, пов'язаних з управлінням ШІ. Ця стаття робить свій внесок, пропонуючи порівняльну оцінку системи цифрових прав Саудівської Аравії з провідними міжнародними інструментами, висвітлюючи реформи, необхідні для управління, заснованого на культурних традиціях та узгодженого на глобальному рівні.*

Ключові слова: *цифрові права, штучний інтелект, права людини, законодавство, захист даних, кібербезпека, конфіденційність, електронне урядування, «Vision 2030».*

ABSTRACT IN ARABIC

مقال بحثي

الحقوق الرقمية والذكاء الاصطناعي والقانون: منظور دولي لإطار السعودية القانونيوالخبرة الدولية

سمية الخماسي ويسرى الشنقيطي*

الملخص

الخلفية: *يقدّم هذا البحث تحليلًا للتطوّر العالمي للحقوق الرقمية وحوكمة الذكاء الاصطناعي، ويبحث في انعكاساته على الإطار القانوني في المملكة العربية السعودية. ومع تزايد حضور الذكاء الاصطناعي في مختلف جوانب الحياة اليومية، تبرز الحاجة الملحّة إلى تقييم أثره على حقوق الإنسان الأساسية، خصوصًا في ظل غياب توافق دولي حول تعريف ومجال «الحقوق الرقمية للإنسان». وتقدّم مبادرة رؤية المملكة 2030 فرصة فريدة لتطوير أطر حوكمة للذكاء الاصطناعي تتماشى مع المعايير الدولية، مع مراعاة القيم الثقافية المحلية والمبادئ الأخلاقية الإسلامية.*

المنهجية: *يعتمد هذا البحث مقاربة تحليلية نوعية لفحص الإطار القانوني الحالي في المملكة العربية السعودية المنظّم للذكاء الاصطناعي والحقوق الرقمية للإنسان. وتشمل المنهجية تحليلًا تشريعيًا شاملًا*

للأنظمة السعودية، وعلى وجه الخصوص نظام حماية البيانات الشخصية (PDPL) وإرشادات الأخلاقيات الصادرة عن الهيئة السعودية للبيانات والذكاء الاصطناعي (SDAIA)، مع مقارنتها بالأدوات القانونية الدولية، بما في ذلك توصية اليونسكو لأخلاقيات الذكاء الاصطناعي، وقانون الاتحاد الأوروبي للذكاء الاصطناعي، وإرشادات منظمة التعاون الاقتصادي والتنمية (OECD). ويقيّم البحث مدى الاتساق مع المعايير الدولية وفعالية هذه الأطر في معالجة تحديات الحقوق الرقمية في عصر الذكاء الاصطناعي.

النتائج والاستنتاجات: *يكشف البحث أنه على الرغم من أن المملكة العربية السعودية حققت تقدمًا ملحوظًا من خلال نظام حماية البيانات الشخصية وأطر إرشادات الأخلاقيات الصادرة عن الهيئة السعودية للبيانات والذكاء الاصطناعي، فإن فجوات تنظيمية كبيرة ما تزال قائمة. ويُظهر نظام حماية البيانات الشخصية جوانب قصور في التعامل مع تحديات الذكاء الاصطناعي المعاصرة، بما في ذلك مساءلة الخوارزميات، والحد من التحيّز، والحماية الشاملة للبيانات في سياقات الذكاء الاصطناعي. كما يحدّد البحث أوجه قصور أساسية، منها الاستثناءات الواسعة لمتطلبات الموافقة، وضعف الأحكام المتعلقة بشفافية الخوارزميات، وتشتّت الجهات الرقابية. وتشمل التوصيات إنشاء هيئات رقابية متخصصة، وتطوير أطر أخلاقية تراعي السياق السعودي، وزيادة إشراك الخبراء في القرارات المتعلقة بحوكمة الذكاء الاصطناعي. وتُسهم هذه الورقة في تقديم تقييم مقارن لإطار الحقوق الرقمية في المملكة العربية السعودية مقابل أبرز الأدوات الدولية، مع تسليط الضوء على الإصلاحات اللازمة لضمان حوكمة متجذّرة ثقافيًا ومتوافقة عالميًا.*