Justicia Islamica: Jurnal Kajian Hukum dan Sosial
Vol.22, No.2, December 2025

The Right to Digital Tranquillity: A Comparative Analysis of AI Governance in Oman and Jordan from an Islamic Legal Perspective

Murtada Abdalla Kheiri,[1*] Racem Gassara,[2] Nizar Qashta,[3]
Mohammed Elsadig Abdallah Mohammed Zain[4]
[1 2 3] Faculty of Law, A'Sharqiyah University, Oman
[4] Faculty of Law, King Faisal University, Kingdom of Saudi Arabia
Email : [1]murtadha.kheiri@asu.edu.om, [2]gassara.racem@gmail.com
[3]nizar.qasta@gmail.com, [4]melsadig@kfu.edu.sa

**Corresponding Author*

DOI: 10.21154/justicia.v22i2.11259

Received: June 18, 2025	*Revised: Oct 30, 2025*	*Approved: Nov 29, 2025*

Abstract: The development of artificial intelligence (AI) and digital technology in the Middle East has raised new challenges to the right to privacy and tranquillity of individuals in cyberspace. This article examines the concept of the right to digital tranquillity through a comparative analysis of legal policies in the Sultanate of Oman and the Hashemite Kingdom of Jordan. This study uses a qualitative legal approach that combines normative and comparative analysis to assess the country's ability to regulate the collection and processing of personal data, as well as respond to digital violations arising from the use of AI. The results show that Oman implements a preventive approach based on *al-siyāsah al-shar'iyyah* values with a focus on explicit user consent as stipulated in Personal Data Protection Law No. 6 of 2022. In contrast, Jordan adopts a repressive and law enforcement approach through Cybercrime Law No. 17 of 2023 and Data Protection Law No. 24 of 2023, which emphasise the need for accountability and balance between digital freedom and national security. From an Islamic legal perspective, the right to digital tranquillity represents the implementation of *maqāṣid al-shariah*, specifically *ḥifẓ al-'ird* (protection of honour) and *ḥifẓ al-nafs* (protection of life). Principles such as *karāmah al-insān, dar' al-mafsadah, maslahah mursalah*, and *lā ḍarar wa lā ḍirār* form the moral basis for fair and humane AI governance. This article concludes that strengthening the right to digital peace requires an ethical, participatory AI governance model that aligns with Islamic legal values, ensuring that technological progress does not compromise human dignity in the digital age.
Keywords: artificial intelligence; digital serenity; internet privacy; rights.

Abstrak: Perkembangan kecerdasan buatan (AI) dan teknologi digital di kawasan Timur Tengah telah memunculkan tantangan baru terhadap hak atas privasi dan ketenangan individu di ruang siber. Artikel ini menelaah konsep hak atas ketenangan digital (the right to digital tranquility) melalui analisis komparatif terhadap kebijakan

hukum di Kesultanan Oman dan Kerajaan Hashemite Yordania. Penelitian ini menggunakan pendekatan hukum kualitatif yang menggabungkan analisis normatif dan komparatif untuk menilai sejauh mana kedua negara mengatur pengumpulan dan pemrosesan data pribadi, serta menanggapi pelanggaran digital yang timbul akibat penggunaan AI. Hasil penelitian menunjukkan bahwa Oman menerapkan pendekatan preventif berbasis nilai-nilai *al-siyāsah al-shar'iyyah* dengan fokus pada persetujuan eksplisit pengguna sebagaimana diatur dalam Personal Data Protection Law No. 6 Tahun 2022. Sebaliknya, Yordania menempuh pendekatan represif dan penegakan hukum melalui Cybercrime Law No. 17 Tahun 2023 dan Data Protection Law No. 24 Tahun 2023 yang menekankan akuntabilitas dan keseimbangan antara kebebasan digital dan keamanan nasional. Dalam perspektif hukum Islam, hak atas ketenangan digital merepresentasikan pelaksanaan *maqāṣid al-syarī'ah*, khususnya *ḥifẓ al-'ird* (perlindungan kehormatan) dan *ḥifẓ al-nafs* (perlindungan jiwa). Prinsip-prinsip seperti *karāmah al-insān, dar' al-mafsadah, maslahah mursalah*, dan *lā ḍarar wa lā ḍirār* menjadi dasar moral bagi tata kelola AI yang berkeadilan dan manusiawi. Artikel ini menyimpulkan bahwa penguatan hak atas ketenangan digital menuntut model tata kelola AI yang etis, partisipatif, dan selaras dengan nilai-nilai hukum Islam agar kemajuan teknologi tidak mengorbankan martabat manusia di era digital.
Kata Kunci: Kecerdasan buatan, kedamaian digital, privasi internet, hak.

Introduction

Social facts reveal an alarming increase in digital privacy violations worldwide, driven by the ability of artificial intelligence and machine learning tools to collect personal data.[1] This development raises concerns about data collection without explicit consent.[2] This privacy issue is exacerbated by practices such as data scraping, which involves extracting large amounts of data from the internet, often including personal data. It supports AI tools like facial recognition and generative AI.[3] AI companies are usually not transparent about their operations and data handling, raising concerns about data privacy and security.[4]

---

1 Lu Cheng et al., "Socially Responsible AI Algorithms: Issues, Purposes, and Challenges," *arXiv (Cornell University)*, ahead of print, Cornell University, January 2021, https://doi.org/10.48550/arXiv.2101.02032; José Ramón Saura et al., "Is AI-Based Digital Marketing Ethical? Assessing a New Data Privacy Paradox," *Journal of Innovation & Knowledge* 9, no. 4 (2024): 100597–100597, https://doi.org/10.1016/j.jik.2024.100597.

2 Cheng et al., "Socially Responsible AI Algorithms: Issues, Purposes, and Challenges."

3 Daniel J. Solove and Woodrow Hartzog, "The Great Scrape: The Clash Between Scraping and Privacy," *SSRN Electronic Journal*, ahead of print, RELX Group (Netherlands), January 2024, https://doi.org/10.2139/ssrn.4884485.

4 Nestor Maslej et al., "Artificial Intelligence Index Report 2024," *arXiv (Cornell University)*, ahead of print, Cornell University, May 2024, https://doi.org/10.48550/arxiv.2405.19522.

Arab countries, including the Sultanate of Oman and the Hashemite Kingdom of Jordan, face growing challenges in regulating AI and protecting digital privacy.[5] This is particularly relevant in the midst of the development of digital surveillance technology and the use of innovative applications that collect users' personal information on a large scale.[6] Reports indicate a debate surrounding emerging ethical threats and violations associated with unregulated AI applications, underscoring the need for effective AI governance models in Oman and Jordan to address these issues.[7]

The Sultanate of Oman is facing new social dynamics amid the widespread use of digital technology and innovative applications that collect citizens' personal data. The implementation of the Personal Data Protection Law, as outlined in Royal Decree No. 6 of 2022, which took effect on February 13, 2023, demonstrates the country's efforts to establish a legal framework for personal data protection. However, high digital penetration, with more than 8.13 million mobile users and 1.55 million Internet of Things (IoT) connections as of May 2025, increases the potential for large-scale data collection, which is often not accompanied by adequate public awareness of digital privacy.[8] Regional surveys also show growing concerns among Omani citizens about data security on social media and online services, particularly due to the large number of innovative applications that access users' location, biometrics, and contact data without explicit permission.[9]

Meanwhile, the Hashemite Kingdom of Jordan faces more complex social challenges due to its direct involvement with issues of digital surveillance and threats to citizens' privacy. Although the country passed Personal Data Protection Law No. 24 of 2023 in September 2023, reports from Access Now and Citizen Lab reveal that at least 35 activists, journalists, and lawyers were targeted by Pegasus spyware attacks between 2019 and 2023. This situation is worsened by the enactment

---

5 Hana Trigui et al., "Exploring AI Governance in the Middle East and North Africa (MENA) Region: Gaps, Efforts, and Initiatives," *Data & Policy* 6 (January 2024), https://doi.org/10.1017/dap.2024.85.

6 Mohammad Rashed Albous et al., "AI Governance in the GCC States: A Comparative Analysis of National AI Strategies," *Journal of Artificial Intelligence Research* 82 (April 2025): 2389–422, https://doi.org/10.1613/jair.1.17619; Barry Solaiman et al., "Regulating AI in Health in the Middle East: Case Studies from Qatar, Saudi Arabia and the United Arab Emirates," in *Edward Elgar Publishing eBooks* (Edward Elgar Publishing, 2024), https://doi.org/10.4337/9781802205657.00028.

7 Halah Al Zadjali, *Building the Right AI Governance Model in Oman*, September 2020, 116–19, https://doi.org/10.1145/3428502.3428516.

8 "Oman's Telecom Sector Powers Ahead with Surge in IoT, Mobile Connections | Arab News," accessed October 25, 2025, https://www.arabnews.com/node/2608769/business-economy.

9 Ali Farooq et al., "Exploring Social Media Privacy Concerns: A Comprehensive Survey Study Across 16 Middle Eastern and North African Countries," *IEEE Access* 12 (2024): 147087–105, https://doi.org/10.1109/ACCESS.2024.3463869.

of the 2023 Cybercrime Law, which, according to Freedom House, is believed to strengthen the state's digital surveillance practices and suppresses freedom of expression in the online space. This phenomenon highlights the gap between the legal norms pursued by the government and the social reality of a society that still faces threats to privacy and ethical use of AI-based technology in the public sphere.[10]

Normatively, the governance of artificial intelligence and digital privacy protection in Arab countries, including Oman and Jordan, should be based on the principles of ethical AI governance, as affirmed by the OECD Principles on Artificial Intelligence and the UNESCO Recommendation on the Ethics of Artificial Intelligence.[11] These principles include transparency, accountability, fairness, and respect for human rights. From an Islamic legal perspective, the concepts of maslahah, mursalah, and *hifz al-'ird* (protection of individual honour and privacy) also provide a moral basis for the use of technology to be directed towards the public interest without causing mafsadat, such as the misuse of personal data.[12] Privacy in Islam is a fundamental value which deeply rooted in shariah principles, which emphasise individual dignity, personal boundaries, and moral behaviour. Adapting an AI ethical framework that takes into account cultural and religious values, such as Islamic principles, is essential to ensure that technological innovation and advancement align with national ethical standards and community needs.[13]

Therefore, theoretically, the state should develop a multi-level governance model for AI, in which the government, private sector, and civil society jointly establish regulatory, ethical, and educational mechanisms to ensure that the use of

---

[10] "Jordan: Freedom on the Net 2024 Country Report," Freedom House, accessed October 25, 2025, https://freedomhouse.org/country/jordan/freedom-net/2024.

[11] Fabio Morandín-Ahuerma, *Ten UNESCO Recommendations on the Ethics of Artificial Intelligence*, September 2023, https://doi.org/10.31219/osf.io/csyux; Andy Nguyen et al., "Ethical Principles for Artificial Intelligence in Education," *Education and Information Technologies* 28, no. 4 (October 2022): 4221–41, https://doi.org/10.1007/s10639-022-11316-w; OECD, "State of Implementation of the OECD AI Principles," *OECD Digital Economy Papers*, ahead of print, June 2021, https://doi.org/10.1787/1cd40c44-en; Andreas Reis et al., "ethics and governance of artificial inTELligence for health : who guidance," in *Research Portal Denmark* (Technical University of Denmark, 2021), 150, https://local.forskningsportal.dk/local/.

[12] Bakhrudin Bakhrudin et al., "Islamic Perspectives on Cybersecurity and Data Privacy: Legal and Ethical Implications," *West Science Law and Human Rights* 1, no. 4 (October 2023): 166–72, https://doi.org/10.58812/wslhr.v1i04.323; Ella Gorian and Noor Dzuhaidah Osman, "digital ethics of artificial inTELligence (ai) in saudi arabia and united arab emirates," *Malaysian Journal of Syariah and Law* 12, no. 3 (December 2024): 583–97, https://doi.org/10.33102/mjsl.vol12no3.798.

[13] Ella Gorian and Noor Dzuhaidah Osman, "Digital Ethics of Artificial Intelligence (AI) In Saudi Arabia And United Arab Emirates," *Malaysian Journal of Syariah and Law* 12, no. 3 (2024): 583–97, https://doi.org/10.33102/mjsl.vol12no3.798; Muhammad Sibawaihi et al., "Islamic Legal Strategies in Indonesian Contexts to Combat Cybercrime and the Spread of Illegal Data Dissemination," *Justicia Islamica* 21, no. 2 (2024): 357–76, https://doi.org/10.21154/justicia.v21i2.9587.

AI and digital technology aligns with the values of social justice and citizens' rights to privacy.[14] Efforts to develop an appropriate AI governance model in Oman, for example, have been the focus of debate surrounding emerging ethical threats and violations associated with unregulated AI applications.[15] Policymakers need to establish a regulatory framework that strikes a balance between innovation, ethical considerations, economic development, and the well-being of communities in the MENA region.[16]

This literature review highlights the urgent need for an in-depth study of the concept of "the right to digital tranquillity" amid the increasing use of AI, as well as a legal evaluation of current protections in Oman and Jordan.[17] This is particularly important given the distinctive legal and social values that characterise Islamic societies.[18] This study examines whether current laws adequately protect this right and how Islamic principles can enhance AI regulation and safeguard individual digital rights.

A review of the literature reveals that, despite research on digital privacy rights, AI risks, and data collection, a significant research gap remains in the legal framework of the Middle East, particularly in the role of Islamic law. This gap includes a lack of focus on the Middle Eastern regional context, the application of Islamic principles to modern AI challenges,[19] and a lack of comparative analysis between Omani and Jordanian legislation in light of Islamic law and digital

---

14 Hyesun Choung et al., "A Multilevel Framework for AI Governance," *arXiv (Cornell University)*, ahead of print, Cornell University, January 2023, https://doi.org/10.48550/arxiv.2307.03198; Bernd Carsten Stahl et al., "Artificial Intelligence for Human Flourishing – Beyond Principles for Machine Learning," *Journal of Business Research* 124 (December 2020): 374–88, https://doi.org/10.1016/j.jbusres.2020.11.030.

15 Zadjali, *Building the Right AI Governance Model in Oman*.

16 Hana Trigui, "Exploring AI Governance in the MENA Region: Gaps, Efforts, and Initiatives," *SSRN Electronic Journal*, ahead of print, RELX Group (Netherlands), January 2024, https://doi.org/10.2139/ssrn.4796071.

17 Bart Custers, "New Digital Rights: Imagining Additional Fundamental Rights for the Digital Era," *Computer Law & Security Review* 44 (December 2021): 105636–105636, https://doi.org/10.1016/j.clsr.2021.105636; Thomas Ploug, "The Right Not to Be Subjected to AI Profiling Based on Publicly Available Data—Privacy and the Exceptionalism of AI Profiling," *Philosophy & Technology* 36, no. 1 (2023), https://doi.org/10.1007/s13347-023-00616-9.

18 Ezieddin Elmahjub, "Artificial Intelligence (AI) in Islamic Ethics: Towards Pluralist Ethical Benchmarking for AI," *Philosophy & Technology* 36, no. 4 (November 2023), https://doi.org/10.1007/s13347-023-00668-x; Gorian and Osman, "digital ethics of artificial inTELligence (AI) in saudi arabia and united arab emirates."

19 Gorian and Osman, "Digital Ethics of Artificial InTELLigence (AI) In Saudi Arabia And United Arab Emirates."

tranquillity.[20] Most studies also tend to be technical in nature without a comprehensive legal or cultural context.[21]

The novelty of this research lies in the combination of comparative legal analysis between Oman and Jordan, with a specific focus on their legislative responses to the impact of AI on digital privacy rights. This study applies Islamic legal and social values as a unique analytical lens, a perspective that is often overlooked. Additionally, this study addresses legislative gaps in the collection and processing of personal data by third parties, particularly through commercial platforms. It provides recommendations for legislative reform based on a relevant cultural and ethical framework.

The purpose of this study is to clarify the concept of "the right to digital tranquility" in its digital form, identify methods of collecting personal data that negatively impact this right, examine manifestations of violations of this right across various digital platforms, evaluate how the legal frameworks in Oman and Jordan address these violations, and explore the extent to which Islamic legal principles can serve as a strong foundation for enhancing the protection of digital tranquility in this context.[22]

This study uses a qualitative legal research design that combines analytical and comparative methods. The analytical method is used to analyse legal provisions related to the right to digital tranquillity. The comparative method involves comparing relevant legislation in Oman and Jordan, utilising the advantages of comparative analysis. This study primarily relies on secondary data sources, including legal texts, official reports, academic literature, and judicial opinions. Data collection was conducted through an extensive literature review and document analysis. The analysis was performed in several stages: a descriptive stage to describe the existing legal framework, an interpretative stage to explore its implications for protecting digital tranquillity, and a comparative stage to identify similarities, differences, and regulatory gaps between Oman and Jordan. This

---

20 Albous et al., "AI Governance in the GCC States: A Comparative Analysis of National AI Strategies"; Trigui et al., "Exploring AI Governance in the Middle East and North Africa (MENA) Region: Gaps, Efforts, and Initiatives."

21 Helena Machado et al., "Publics' Views on Ethical Challenges of Artificial Intelligence: A Scoping Review," in *AI and Ethics*, Springer Nature, December 2023, https://doi.org/10.1007/s43681-023-00387-1.

22 Hijrian Angga Prihantoro, "Examining Witness Interest: The Obstacles of Testimony in Islamic Jurisprudence and Positive Law," *Justicia Islamica* 21, no. 1 (2024): 1–22, https://doi.org/10.21154/justicia.v21i1.8653.

integrated approach ensures a comprehensive understanding of the legal landscape governing digital tranquillity in both jurisdictions.

Conceptual Framework of the Right to Digital Peace in Oman and Jordan Law

Public peace is one of the fundamental elements of public order in modern society. This right is crucial for human life as it relates to basic needs for security, peace, and tranquillity. Legally, the right to peace has been recognised by both divine law *(shariah)* and positive law as an inherent human right. Traditionally, public peace refers to protecting individuals from noise or sound pollution, as well as public comfort violations.

The protection of this right is regulated in the Basic Law of the State of Oman No. 6 of 2021, specifically Article 13, which stipulates that the state is obligated to establish an administrative system that guarantees justice, equality, and public order. Similarly, the Jordanian Constitution in Article 6 guarantees the security and welfare of citizens within the limits of the state's capabilities. Jordan's laws show efforts to safeguard digital privacy and bolster this constitutional right. Both countries' articles reveal that Oman and Jordan's lawmakers have ensured that public peace is a constitutional right.[23] Both articles indicate that legislators in Oman and Jordan have guaranteed the right to public peace as part of constitutional rights.

In addition, the Executive Regulations of the Omani Traffic Law also reinforce this protection,[24] for example, Article 84, which prohibits the use of vehicles for advertising with loudspeakers, and Article 86, which prohibits the installation of audio or visual devices resembling emergency vehicles (Royal Oman Police Regulation No. 28 of 2016). In Jordan, Traffic Law No. 49 of 2008 Article 31(e) also stipulates penalties for anyone who causes public noise through vehicle modifications. However, developments in information technology have changed the form of disturbance to public peace. Now, noise is not only a physical thing, but also a digital one, which presents itself through spam, automated advertising, data tracking, and the misuse of artificial intelligence algorithms. Violations of digital peace arise, for example, when individuals are bombarded by unsolicited promotional messages and advertisements that disturb the peace of internet use.

---

[23] Tareq Al-Billeh, "Legal Framework for Protecting the Right to Private Life in the Digital Space: The Extent to Which Jordanian Constitution and Legislation Takes into Account International Requirements," *Revista de Investigações Constitucionais* 11, no. 1 (2024): 258–258, https://doi.org/10.5380/rinc.v11i1.90631.

[24] Decision No. 98/23 issuing the executive regulations of the Omani Traffic Law issued based on the Police Law issued by Royal Decree No. 90/35 and the Traffic Law issued by Royal Decree No. 93/28. These regulations were published in the Official Gazette No. (620) issued on 4/1/1998.

This phenomenon, including disturbances caused by negative online feedback or unwanted digital communication, can have a significant psychological impact on individuals, affecting their well-being and mental activity.[25]

This type of violation is evident in the case of the "Ooredoo Spam Complaint," where several Omani citizens reported a telecommunications company for sending repeated promotional messages without their consent. The case sparked public debate until the Oman Telecommunications Authority issued Circular No. 3 of 2022, which requires operators to obtain explicit user consent before sending digital promotional content. The right to digital peace can be defined as the right of individuals to enjoy a peaceful digital space, to be free from algorithmic intervention, unwanted promotions, or privacy violations that can disrupt their psychological and social comfort when interacting in cyberspace. Algorithmic intervention and the use of AI in the context of warfare or data tracking have demonstrated a significant impact on existing legal systems, underscoring the need for a practical legal and ethical framework to support the sustainable development of AI.[26] Thus, the right to digital tranquillity extends traditional public tranquillity rights to include protection from tech-based digital disruptions. States must guarantee this right, just as they ensure public order in real life.

Furthermore, the collection of personal data is the starting point in the digital data processing process. According to the European Union's General Data Protection Regulation, the collection of personal data must be carried out with a legal basis, clear objectives, and explicit consent from the data owner (EU Regulation No. 2016/679). A similar principle is adopted by Oman's Personal Data Protection Law No. 6 of 2022, in Article 4, which states that collecting personal data without permission or for purposes other than those announced is a violation of the law. Many countries in the Middle East, including the United Arab Emirates and Saudi

---

[25] Semira Maria Evangelou et al., "Exploring the Impact of Negative Online Feedback on Well-Being: A Comprehensive Analysis Incorporating Big-Five Personality Traits and Physiological Responses," *Computers in Human Behavior Reports* 15 (July 2024): 100457–100457, https://doi.org/10.1016/j.chbr.2024.100457; Christopher Kelly and Tali Sharot, "Web-Browsing Patterns Reflect and Shape Mood and Mental Health," *Nature Human Behaviour*, ahead of print, Nature Portfolio, November 2024, https://doi.org/10.1038/s41562-024-02065-6; Francesca Stevens et al., "Cyber Stalking, Cyber Harassment, and Adult Mental Health: A Systematic Review," in *Cyberpsychology Behavior and Social Networking*, vol. 24, no. 6, Mary Ann Liebert, Inc., November 2020, https://doi.org/10.1089/cyber.2020.0253.

[26] J. Liu, "Artificial Intelligence and International Law: The Impact of Emerging Technologies on the Global Legal System," *Economics Law and Policy* 7, no. 2 (2024), https://doi.org/10.22158/elp.v7n2p73; Sylvia Lu, *Regulating Algorithmic Harms*, January 2024, https://doi.org/10.2139/ssrn.4949052.

Arabia, have adopted modernised data protection standards to align with international standards, such as the GDPR.[27]

One of the most common mechanisms used to collect data without permission is the use of cookies, which are small digital files that record user activity when visiting a website. Although cookies help improve the user experience, many companies use them to track users' digital behaviour and build commercial profiles without obtaining consent. Regulations such as the GDPR explicitly prohibit the processing of personal data, including website cookies, unless the data owner gives explicit permission.[28]

In Jordan, Cybercrime Law No. 17 of 2023 enhances the protection of personal data by criminalising all forms of unauthorised access and data collection.[29] Jordan's cyber laws have evolved since 2010, with amendments in 2015 and 2017 to expand protections, particularly for women.[30] Analysis shows that Jordanian laws, including cybercrime legislation, continue to evolve in an effort to address challenges in protecting personal life in the digital space and ensuring data privacy.[31] A notable example is the "Amman Data Harvesting Case," in which a digital marketing firm was penalised by the Data Protection Department for gathering and selling social media user data without their consent. The court decided that these actions infringed on individuals' rights to privacy and digital calm.

---

27 Latifa Adarmouch et al., "Perspectives Regarding Privacy in Clinical Research among Research Professionals from the Arab Region: An Exploratory Qualitative Study," *BMC Medical Ethics* 21, no. 1 (2020), https://doi.org/10.1186/s12910-020-0456-9; Ayman Shawqi Alhazmi and Anas Daghistani, "Privacy Practices of Popular Websites in Saudi Arabia," *Deleted Journal*, ahead of print, December 2024, https://doi.org/10.1007/s43995-024-00085-x; Lori Baker and Julie Beeton, "Dubai International Financial Centre's Updated Data Protection Law - Part 1: Developing a Modern, Global Law in a UAE Financial Free Zone," *Journal of Data Protection & Privacy*. 3, no. 2 (2020): 161–161, https://doi.org/10.69554/kcjb7880; Laroussi Chemlali et al., "A Reflection on the UAE's New Data Protection Law: A Comparative Approach with GDPR," *Journal of Data Protection & Privacy*. 6, no. 1 (2023): 24–24, https://doi.org/10.69554/opeg2767; Radwan Eskhita and Evert Stamhuis, "The Influence of the Brussels Effect on the Interpretation of Data Protection Laws in the Gulf," *Global Journal of Comparative Law* 13, no. 2 (2024): 261–78, https://doi.org/10.1163/2211906x-13020007.

28 Alhazmi and Daghistani, "Privacy Practices of Popular Websites in Saudi Arabia."

29 Ahmad Al-Amawi and Hashim Balas, "Digital Character Assassination in the Jordanian Law," *Multidisciplinary Reviews* 7, no. 11 (2024): 2024273–2024273, https://doi.org/10.31893/multirev.2024273.

30 Rula Odeh Alsawalqa, "Evaluating Female Experiences of Electronic Dating Violence in Jordan: Motivations, Consequences, and Coping Strategies," *Frontiers in Psychology* 12 (November 2021), https://doi.org/10.3389/fpsyg.2021.719702.

31 Sanaa Maaytah and Hiba Kobarie, "The Extent of the Impact of Cybersecurity Rules on Electronic Civil Transactions in Jordanian Law," *International Journal of Religion* 5, no. 10 (August 2024): 5191–98, https://doi.org/10.61707/ad442p10; Nabeel Zaid Suliman Magableh, "the adequacy of the laws regulating electronic business in jordan," *public administration and law review*, March 2024, 66–77, https://doi.org/10.36690/2674-5216-2024-1-66.

The danger of illegal data collection lies in its potential to interfere with individuals' rights to use the Internet peacefully. For example, when personal data such as names, addresses, phone numbers, or shopping interests is collected through cookies and AI algorithms, users often receive unwanted promotional emails, advertising notifications, and repetitive content.[32] This phenomenon causes constant digital disruption, destroying users' sense of peace in cyberspace. Exposure to negative information online, as well as experiences of cyberstalking and cyberbullying, can have a significant negative impact on mental health, which causes depression, anxiety, and even suicidal ideation.[33]

In addition to cookies, other technologies such as data fusion, clickstream tracking, Radio Frequency Identification, and social media scraping are also used to collect personal data. With the emergence of artificial intelligence, data collection has become increasingly complex as algorithmic systems can recognise and connect information from different databases. AI systems demonstrate an extraordinary ability to access digital data, which poses a serious threat to individuals' right to privacy.[34] For example, two accounts with different names can be identified as belonging to the same individual based on a phone number or similar digital behaviour patterns, which clearly constitutes a serious violation of the right to digital tranquillity.

Thus, it can be concluded that the collection of personal data in violation of the law directly threatens digital privacy rights, which causes technical issues such as spam and ads, as well as psychological impacts from feeling constantly monitored.[35] Therefore, both Oman and Jordan need to strengthen their legal frameworks for digital privacy by enforcing laws against personal data violations more strictly, while also adapting national laws to technological developments and international digital privacy principles.

---

[32] Marvin Iroegbu et al., "Investigating the Psychological Impact of Cyber-Sexual Harassment," *Journal of Interpersonal Violence* 39 (February 2024): 3424–45, https://doi.org/10.1177/08862605241231615.

[33] Kelly and Sharot, "Web-Browsing Patterns Reflect and Shape Mood and Mental Health"; Stevens et al., "Cyber Stalking, Cyber Harassment, and Adult Mental Health: A Systematic Review."

[34] أحمد حسني علي الأشقر, "الخصوصية الرقمية في عصر الذكاء الاصطناعي:, قراءة في التشريعين الأردني والفلسطيني," *مجلة جامعة القدس المفتوحة للبحوث الإنسانية والاجتماعية*, January 2025, 32–32, https://doi.org/10.33977/0507-000-066-003.

[35] David Pagliaccio et al., "Probing the Digital Exposome: Associations of Social Media Use Patterns with Youth Mental Health," *NPP—Digital Psychiatry and Neuroscience* 2, no. 1 (2024), https://doi.org/10.1038/s44277-024-00006-9.

Manifestations of Violations of the Right to Digital Peace

The right to digital tranquillity is a component of the right to privacy, safeguarding individuals from digital interference, data misuse, and cyberattacks. In modern life, this right is crucial as social, economic, and political activities rely on Information Technology. However, technological advancements such as AI, ad algorithms, and big data analytics have created opportunities for violations. The implications of AI in cross-border relationships also raise significant issues related to data privacy, jurisdiction, regulatory consistency, and accountability.[36] Manifestations of these violations are evident on websites, in emails, and on social media platforms.

A website is a digital space where information is provided on the internet through a specific address (domain). Omani legislators define a website in Article 2 of the Information Technology Crimes Law No. 12 of 2011 as "a place where electronic information is provided on an information network through a specific address." A similar definition is also adopted in Article 2 of Jordan's Electronic Crimes Law No. 17 of 2023. In practice, websites have become a significant channel for digital tranquillity rights violations, often through unauthorised collection of users' personal data.[37] For example, many global e-commerce sites, such as Amazon and Alibaba, use tracking technologies (cookies and web beacons) to record user activities, including products viewed, geographic location, and access time. The data is then analysed to display advertisements that are adjusted to user behaviour. Advertising and analytics companies widely collect, aggregate, process, and trade large amounts of users' personal data for targeted advertising purposes.[38] Although this practice is considered legitimate in the context of digital marketing, it is often done without the explicit consent of users, thereby violating the principle of consent in personal data protection.[39] Targeted advertising mechanisms that reveal interests are considered "privacy-exposing" rather than "privacy-preserving," even with new technologies such as Google's Topics API.[40]

---

36 Gorian and Osman, "digital ethics of artificial inTELligence (AI) in saudi arabia and united arab emirates."

37 Zahra Pooranian et al., "Online Advertising Security: Issues, Taxonomy, and Future Directions," *IEEE Communications Surveys & Tutorials* 23, no. 4 (2021): 2494–524, https://doi.org/10.1109/comst.2021.3118271.

38 Imdad Ullah et al., "Privacy in Targeted Advertising on Mobile Devices: A Survey," *International Journal of Information Security* 22, no. 3 (2022): 647–78, https://doi.org/10.1007/s10207-022-00655-x.

39 Manuel Batista et al., "Tensions between Privacy and Targeted Advertising," *Scientific Journal of Applied Social and Clinical Science* 3, no. 14 (2023): 2–7, https://doi.org/10.22533/at.ed.2163142316067.

40 Yohan Beugin and Patrick McDaniel, "Interest-Disclosing Mechanisms for Advertising Are Privacy-Exposing (Not Preserving)," *Proceedings on Privacy Enhancing Technologies* 2024, no. 1 (2023): 41–57, https://doi.org/10.56553/popets-2024-0004.

A similar thing happens on news sites or entertainment portals that display pop-up ads or tracking cookies, which automatically access user data. As a result, users often experience annoyances in the form of repeated ads that follow their online activities. This phenomenon, known as targeted advertising, can psychologically cause discomfort, anxiety, and a loss of digital peace of mind.[41] Studies reveal that users may view targeted ads as intrusive and have heightened privacy concerns, which can hinder product acceptance.[42] The dichotomy between the perception of personalised advertising as beneficial on the one hand and the intrusion on privacy on the other has been referred to as the personalisation-privacy paradox.

Laws in Oman and Jordan have attempted to address this issue. Articles 21 and 22 of Oman's Personal Data Protection Law No. 6 of 2022 require data controllers to maintain the confidentiality of personal information and obtain written consent from data owners before sending advertising material. In Jordan, Article 14(a) of Personal Data Protection Law No. 24 of 2023 also states that data transfers for marketing purposes may only be carried out with the consent of the data owner. However, Oman is more progressive since it mandates consent before sending promotional materials, unlike Jordan, where consent is sought after. Consumer protection in Oman for e-commerce transactions remains relatively new and limited, despite the existence of laws governing consumer protection, electronic transactions, and cybercrime.[43]

Violations of the right to digital tranquillity also occur frequently via email. The phenomenon of spam mail, or mass promotional messages, is a typical example.[44] For example, in 2023, Google reported that the Gmail system blocked over 15 billion spam emails daily, including unwanted promotional messages sent by global companies without the recipient's consent. Some spam is even sent to the official accounts of government or educational institutions, disrupting professional activities.[45] In addition, phishing, which involves sending fake emails that imitate

---

41 Pooranian et al., "Online Advertising Security: Issues, Taxonomy, and Future Directions."

42 Katharina Baum et al., "The Effects of Targeted Political Advertising on User Privacy Concerns and Digital Product Acceptance: A Preference-Based Approach," *Electronic Markets* 33, no. 1 (2023), https://doi.org/10.1007/s12525-023-00656-1.

43 Rakesh Belwal et al., "Consumer Protection and Electronic Commerce in the Sultanate of Oman," *Journal of Information Communication and Ethics in Society* 19, no. 1 (2020): 38–60, https://doi.org/10.1108/jices-09-2019-0110.

44 Francisco José Aranda Serna, "The Legal Regulation of Spam: An International Comparative Study," *Journal of Innovations in Digital Marketing* 3, no. 1 (2022): 1–11, https://doi.org/10.51300/jidm-2022-44.

45 SentinelOne, "What Is Spam? Types, Risks, and How to Protect Your Business," SentinelOne, July 17, 2025, https://www.sentinelone.com/cybersecurity-101/cybersecurity/what-is-spam/.

official institutions such as banks or government agencies, is also a serious violation of the right to digital tranquillity because it causes anxiety and insecurity in the online space. The "Ooredoo Spam Complaint" case, in which several Omani citizens reported a telecommunications company for sending repeated promotional messages without user consent, sparked public debate until the Oman Telecommunications Authority issued Circular No. 3 of 2022, which requires operators to obtain explicit user consent before sending digital promotional content. Thus, websites and emails are the primary channels for digital tranquillity rights violations, involving unauthorised collection, storage, and use of personal data, as well as intrusive digital ads that disrupt user comfort and privacy.

Furthermore, social media platforms such as *Facebook*, *Instagram*, *X, TikTok*, and *LinkedIn* are virtual spaces that enable social interaction without geographical boundaries. Jordanian legislators in the 2023 Electronic Crimes Law define social media as "any electronic space that allows users to publish, send, or receive images, videos, comments, writings, or audio recordings." However, the openness of this space has made social media one of the primary sources of violations of the right to digital tranquillity. These platforms often request users' personal data, such as name, date of birth, location, and personal interests, which are then used for commercial purposes. For example, the Cambridge Analytica scandal revealed how the personal data of approximately 87 million Facebook users was misused for political and marketing purposes without their consent. This case is clear evidence of how social media algorithms can be used to manipulate public behaviour and disrupt privacy and digital tranquillity. People have varying expectations of privacy, even for public data, creating "fuzzy boundaries" in social media privacy management.[46]

Additionally, location tracking features on platforms such as TikTok and Instagram enable advertisers to target users based on their precise location.[47] This causes users to receive unwanted local advertisements continuously. For example, when a user searches for restaurants in a city, they will continue to receive food advertisements from that area even after leaving the location. Although it seems trivial, this practice reveals a form of invasive digital surveillance of personal life.[48]

Another technique often used is social media phishing, where hackers create fake login pages that resemble official sites, such as Facebook or Instagram, to steal

---

[46] Anatoliy Gruzd et al., "Cybervetting and the Public Life of Social Media Data," *Social Media + Society* 6, no. 2 (2020), https://doi.org/10.1177/2056305120915618.

[47] Pooranian et al., "Online Advertising Security: Issues, Taxonomy, and Future Directions."

[48] Ullah et al., "Privacy in Targeted Advertising on Mobile Devices: A Survey."

user account data. Additionally, the widespread use of cookies by companies such as Meta Platforms Inc. enables them to track user activity across websites for digital advertising purposes. As a result, users lose control over their personal information, as they're bombarded with advertisements and promo messages in their digital space.[49] Jordan's cybercrime law has attempted to address these challenges by criminalising unauthorised access and protecting personal data. The "Amman Data Harvesting Case," in which the Data Protection Department fined a digital marketing company for collecting and selling user data from social media platforms without explicit consent, shows that the court ruled that such actions violate individuals' rights to privacy and digital tranquillity.[50]

This phenomenon reveals that violations of digital privacy rights on social media not only originate from other users but also from platform providers who systematically exploit personal data for economic gain. This exploitation highlights the digital power gap between tech giants and individual users. In fact, even a small amount of data accidentally disclosed on social media can reveal personal information that should not be made public.[51]

Table 1. Cases of Violations of the Right to Digital Peace through Websites, Email, and Social Media in Oman and Jordan

Country	Medium Violation	Case Example / Practice	Law / Provision Violated
Oman	Website/website cloning and email scam	Oman has reported a significant increase in cyber fraud, including fake websites that imitate official portals, phishing emails requesting personal data, and OTPs.[52]	1) Personal Data Protection Law No. 6/2022 ("PDPL"): Articles 21 & 22 stipulate that personal data may not be published without the owner's consent and that controllers must obtain written permission before sending

[49] Al-Amawi and Balas, "Digital Character Assassination in the Jordanian Law."

[50] Hamzeh Abu Issa et al., "Unauthorized Access Crime in Jordanian Law (Comparative Study)," *Digital Investigation* 28 (January 2019): 104–11, https://doi.org/10.1016/j.diin.2019.01.006.

[51] Stefan Kutschera, "Incidental Data: Observation of Privacy Compromising Data on Social Media Platforms," *International Cybersecurity Law Review* 4, no. 1 (2022): 91–114, https://doi.org/10.1365/s43439-022-00071-w.

[52] Tridwip, "Phishing, Crypto and Fake Job Scams up 35% in Q1 2025 in Oman," *Muscat Daily| Oman News |Business | Sports |Lifestyle*, May 26, 2025, https://www.muscatdaily.com/2025/05/26/35-rise-in-cyber-fraud-crimes-in-q1-2025-rop/.

			advertising/promotional material. 2) Cyber Crime Law 2011 (Oman): For example, Article 12 relates to data forgery using IT tools. 3) Anti-spam regulations in the process of being drafted: the draft "Anti-SPAM Regulations" by the Telecommunications Regulatory Authority (Oman) (TRA) stipulates that advertisers must obtain the consent of the recipient.
Oman	Unsolicited commercial emails/promotions & intrusive digital advertising.	The practice of sending advertising/promotional material via email/web without explicit permission (e.g., unsolicited online advertising) is contrary to the written consent requirements in the PDPL.	PDPL No. 6/2022, Article 22 (advertising/promotion only after written approval).
Oman	Social media/fake accounts or impersonation.	Oman has reported cases of fake social media accounts impersonating official institutions (e.g., fake social media accounts impersonating traffic authorities) that could disrupt digital peace.[53]	Cyber Crime Law 2011: Articles related to forgery/misuse of IT tools (Art. 12-13) that can be used for fake accounts.
Jordan	Social media/fake accounts & unauthorised content distribution.	In Jordan, for example, the creation of fake accounts/emails/websites is misused. The new	Cybercrime Law No. 17/2023 (Jordan): Article 5 (a), for example, regulates punishment for

[53] "Beware of Cyber Laws While Posting Messages Online - Times of Oman," accessed October 29, 2025, https://timesofoman.com/article/129537-beware-of-cyber-laws-while-posting-messages-online?utm_source.

		law imposes sanctions on anyone who creates fake social media accounts or impersonates institutions.[54]	"creating an email account, web page, or social media group and falsely associating it with an individual or legal entity."
Jordan	Websites/email/social media privacy violations, advertising/promotions without consent, and transfer of personal data.	The personal data protection law also states that transferring or marketing data without consent is a violation.[55]	Data Protection Law No. 24/2023 (Jordan): Article 7(w) and Article 14(a) stipulate that data processing must meet specific requirements and that data may not be transferred for the marketing of products/services unless consent has been obtained.

Source: Compiled by the author in 2025

Based on the table above, it can be concluded that both Oman and Jordan have fairly strict legal frameworks for prosecuting digital violations through social media, email, and websites, especially those related to the misuse of personal data, creation of fake accounts, and sending messages or advertisements without consent. In Oman, protection focuses on privacy and explicit permission, as outlined in the Personal Data Protection Law No. 6 of 2022 and the Cyber Crime Law of 2011. In contrast, Jordan emphasises accountability and cybersecurity through Cybercrime Law No. 17 of 2023 and Data Protection Law No. 24 of 2023. Both countries demonstrate serious efforts to protect citizens' rights to digital tranquillity, specifically in freedom from online harassment or abuse, by emphasising the importance of privacy regulations, data security, and social media ethics in the era of digital transformation.

[54] "Jordan: New Anti-Cybercrimes Law Enacted," web page, Library of Congress, Washington, D.C. 20540 USA, accessed October 29, 2025, https://www.loc.gov/item/global-legal-monitor/2023-09-27/jordan-new-anti-cybercrimes-law-enacted/.

[55] Library of Congress, Washington, D.C. 20540 USA, "Jordan."

Islamic Law Approaches to the Right to Digital Peace in Oman and Jordan: A Comparative Analysis

The right to digital tranquillity in Oman and Jordan demonstrates that both countries share a similar commitment to protecting the privacy of their citizens in the digital sphere. Oman affirms this through Personal Data Protection Law No. 6 of 2022 and the Cybercrime Law of 2011, while Jordan reinforces it through the Data Protection Law No. 24 of 2023 and the Cybercrime Law No. 17 of 2023. However, a fundamental difference can be observed in the orientation of the policies: Oman prioritises preventive protection based on Sharia principles, while Jordan prioritises law enforcement and strikes a balance between digital freedom and social security.[56]

The right to digital tranquillity upholds maqāṣid al-syarīʻah, protecting honour *(ḥifẓ al-ʻird)* and life *(ḥifẓ al-nafs)*, ensuring freedom from harassment, slander, and data exploitation. QS. Al-Isrā' [17]:70 emphasises the importance of respecting human dignity in the digital space.[57] Oman's preventive approach reflects the principle of *dar' al-mafsadah muqaddam 'ala jalb al-maṣlaḥah* (preventing harm takes precedence over seeking benefit). For example, Personal Data Protection Law No. 6 of 2022 Articles 21–22 require written consent before personal data is processed or used for commercial purposes.[58] Meanwhile, Jordan emphasises the principles of *taʻādul* (balance) and *lā ḍarar wa lā ḍirār* (no harm and no mutual harm), as affirmed in Cybercrime Law No. 17 of 2023, which prohibits the creation of fake accounts, digital fraud, and the dissemination of unauthorised content.[59]

---

56 Al-Billeh, "Legal Framework for Protecting the Right to Private Life in the Digital Space: The Extent to Which Jordanian Constitution and Legislation Takes into Account International Requirements."

57 Sherien Ghaleb et al., "Shari'ah Law and Courts," in *Encyclopedia of Forensic and Legal Medicine: Volume 1-4, Third Edition*, vol. 4 (Elsevier, 2024), https://doi.org/10.1016/B978-0-443-21441-7.00034-0.

58 Moufid El-Khoury and Saleh Albarashdi, "Navigating the Privacy Landscape of Healthcare-Driven AI in the Middle East: Case Studies from Oman, Qatar, and Saudi Arabia," *Social Sciences and Humanities Open* 11 (2025), https://doi.org/10.1016/j.ssaho.2025.101492.

59 Yousef Awad Al-Mashaqbeh, "Legislative Framework Regulating Digital Media In Jordan And Arab Countries: A Study On The Legal Dimensions," *Lex Localis - Journal of Local Self-Government* 23, no. 10 (August 2025): 1–20.

Table 2. Comparison of Islamic Values and Their Implementation in the Protection of the Right to Digital Tranquillity

Aspects of Islamic Legal Values	Implementation in Oman	Implementation in Jordan
***Karāmah al-insān* (human dignity)**	Placing digital privacy as part of the dignity of individuals that must be protected. PDPL No. 6 of 2022 regulates the obligation to maintain the confidentiality of personal data as a form of respect for human dignity.	Protecting social media users from slander and defamation, Cybercrime Law No. 17 of 2023 imposes sanctions for the dissemination of content that degrades the dignity of others.
***Dar' al-mafsadah* (damage prevention)**	Preventive approach: prohibition of data exploitation without consent, strict monitoring of digital activities.	Repressive approach: taking action against violations after the fact, for example, in cases of fake accounts and digital hoaxes.
***Maslahah mursalah* (public welfare)**	Promoting ethical technological innovation while maintaining a balance between digital progress and user privacy.	Balancing national security interests and digital civil liberties.
***Lā ḍarar wa lā ḍirār* (not mutually detrimental)**	Prohibition of spam, forced advertising, and the use of data for commercial purposes that disrupts users' digital peace.	Law enforcement against the dissemination of false content, online defamation, and cyber fraud as a form of protection from reciprocal harm.

Source: Author's Analysis Results, 2025

Based on the table above, it can be seen that Oman places more emphasis on preventive protection, as per the value of *al-siyāsah al-shar'iyyah*, specifically the role of the government in maintaining public welfare. Policies such as the requirement for written permission for data collection are concrete examples of the application of *sad al-dharā'i* (closing the path to harm). This demonstrates that Omani regulations align with the spirit of maqāṣid al-syarī'ah, which prioritises protection over harm. In contrast, Jordan adopts a reactive and law enforcement approach, focusing on sanctions for digital ethics violations. According to Al-Mashaqbeh, Jordan's legal system seeks to strike a balance between freedom of expression and respect for digital privacy through the principles of *ta'ādul* and *iqāmat al-'adl* (enforcement of

justice).[60] This approach is reinforced by Data Protection Law No. 24 of 2023, which explicitly prohibits the transfer of personal data for marketing purposes without the individual's consent.[61] Both countries apply the principle of *maṣlaḥah mursalah* to address ethical challenges in the era of artificial intelligence (AI). Islamic law serves as a moral and social counterbalance in digital governance, ensuring that technological progress does not compromise human dignity *(karāmah al-insān)* and the right to inner peace *(ḥifẓ al-nafs)*.[62]

Comparatively, Oman and Jordan exhibit two distinct approaches to applying Islamic law in a digital context: Oman prioritises prevention and caution *(iḥtiyāṭ)*, while Jordan focuses on justice and legal sanctions following violations. From an Islamic perspective, these two models are an ideal combination of the principles of *sad al-dharā'i* (prevention of harm) and *iqāmat al-'adl* (enforcement of justice). By integrating the values of *karāmah al-insān, dar' al-mafsadah, maṣlaḥah mursalah*, *and lā ḍarar wa lā ḍirār*, these two countries demonstrate that Islamic law remains relevant and applicable in protecting the right to digital peace in the era of artificial intelligence.

Conclusion

This article asserts that the right to digital tranquillity is a modern extension of the traditional right to public tranquillity, which now includes protection against technology-based disturbances, algorithmic surveillance, and misuse of personal data. Oman and Jordan prioritise digital privacy protection, but differ in their approaches: Oman focuses on prevention and Sharia ethics, while Jordan emphasises law enforcement and balances security with civil liberties. Within the framework of Islamic law, the protection of digital tranquillity is a manifestation of *the maqāṣid al-syarī'ah, which aims* to preserve human dignity and safety. The values of karāmah al-insān and dar' al-mafsadah are the foundation for building a legal system that not only upholds justice but also prevents social damage caused by technology. Thus, the protection of the right to digital tranquillity cannot be separated from Islamic ethical principles that demand moral responsibility in the use

---

60 Yousef Awad Al-Mashaqbeh, "Legislative Framework Regulating Digital Media In Jordan And Arab Countries: A Study On The Legal Dimensions," *Lex Localis - Journal of Local Self-Government* 23, no. 10 (2025): 1–20; Mashood A. Baderin, *International Human Rights and Islamic Law* (OUP Oxford, 2003).

61 "Personal Data Protection Law in Jordan," accessed October 30, 2025, https://www.dentons.com/en/insights/articles/2023/october/4/personal-data-protection-law-in-jordan.

62 Zulfa Amalia Firdaus and Nabila Luthvita Rahma, "The Reason For Childfree In Maqashid Sharia Perspective," *Ahkam: Jurnal Hukum Islam* 13, no. 1 (2025): 85–107, https://doi.org/10.21274/ahkam.2025.13.1.85-107.

of AI. Arab countries need to adopt a multi-level governance model for AI that involves the government, the private sector, and civil society to ensure a balance between digital innovation and human rights in the era of artificial intelligence.

References

Adarmouch, Latifa, Marwan Felaefel, Robert Wachbroit, and Henry Silverman. "Perspectives Regarding Privacy in Clinical Research among Research Professionals from the Arab Region: An Exploratory Qualitative Study." *BMC Medical Ethics* 21, no. 1 (2020). https://doi.org/10.1186/s12910-020-0456-9.

Al-Amawi, Ahmad, and Hashim Balas. "Digital Character Assassination in the Jordanian Law." *Multidisciplinary Reviews* 7, no. 11 (2024): 2024273–2024273. https://doi.org/10.31893/multirev.2024273.

Al-Billeh, Tareq. "Legal Framework for Protecting the Right to Private Life in the Digital Space: The Extent to Which Jordanian Constitution and Legislation Takes into Account International Requirements." *Revista de Investigações Constitucionais* 11, no. 1 (2024): 258–258. https://doi.org/10.5380/rinc.v11i1.90631.

Albous, Mohammad Rashed, Odeh Al-Jayyousi, and Melodena Stephens Balakrishnan. "AI Governance in the GCC States: A Comparative Analysis of National AI Strategies." *Journal of Artificial Intelligence Research* 82 (April 2025): 2389–422. https://doi.org/10.1613/jair.1.17619.

Alhazmi, Ayman Shawqi, and Anas Daghistani. "Privacy Practices of Popular Websites in Saudi Arabia." *Deleted Journal*, ahead of print, December 2024. https://doi.org/10.1007/s43995-024-00085-x.

Al-Mashaqbeh, Yousef Awad. "Legislative Framework Regulating Digital Media In Jordan And Arab Countries: A Study On The Legal Dimensions." *Lex Localis - Journal of Local Self-Government* 23, no. 10 (2025): 1–20.

Alsawalqa, Rula Odeh. "Evaluating Female Experiences of Electronic Dating Violence in Jordan: Motivations, Consequences, and Coping Strategies." *Frontiers in Psychology* 12 (November 2021). https://doi.org/10.3389/fpsyg.2021.719702.

Baderin, Mashood A. *International Human Rights and Islamic Law*. OUP Oxford, 2003.

Baker, Lori, and Julie Beeton. "Dubai International Financial Centre's Updated Data Protection Law - Part 1: Developing a Modern, Global Law in a UAE Financial Free Zone." *Journal of Data Protection & Privacy*. 3, no. 2 (2020): 161–161. https://doi.org/10.69554/kcjb7880.

Bakhrudin, Bakhrudin, Fahmi Ihsan Margolang, Eko Sudarmanto, and Sugiono Sugiono. "Islamic Perspectives on Cybersecurity and Data Privacy: Legal and

Ethical Implications." *West Science Law and Human Rights* 1, no. 4 (2023): 166–72. https://doi.org/10.58812/wslhr.v1i04.323.

Batista, Manuel, Adriana Lopes Fernandes, Lilian Ponzo Ribeiro, Bráulio Alturas, and Carla Pacheco Costa. "Tensions between Privacy and Targeted Advertising." *Scientific Journal of Applied Social and Clinical Science* 3, no. 14 (2023): 2–7. https://doi.org/10.22533/at.ed.2163142316067.

Baum, Katharina, Olga Abramova, Stefan Meißner, and Hanna Krasnova. "The Effects of Targeted Political Advertising on User Privacy Concerns and Digital Product Acceptance: A Preference-Based Approach." *Electronic Markets* 33, no. 1 (2023). https://doi.org/10.1007/s12525-023-00656-1.

Belwal, Rakesh, Rahima Al Shibli, and Shweta Belwal. "Consumer Protection and Electronic Commerce in the Sultanate of Oman." *Journal of Information Communication and Ethics in Society* 19, no. 1 (2020): 38–60. https://doi.org/10.1108/jices-09-2019-0110.

Beugin, Yohan, and Patrick McDaniel. "Interest-Disclosing Mechanisms for Advertising Are Privacy-Exposing (Not Preserving)." *Proceedings on Privacy Enhancing Technologies* 2024, no. 1 (2023): 41–57. https://doi.org/10.56553/popets-2024-0004.

"Beware of Cyber Laws While Posting Messages Online - Times of Oman." Accessed October 29, 2025. https://timesofoman.com/article/129537-beware-of-cyber-laws-while-posting-messages-online?utm_source.

Chemlali, Laroussi, Abdesselam Salmi, and Leila Benseddik. "A Reflection on the UAE's New Data Protection Law: A Comparative Approach with GDPR." *Journal of Data Protection & Privacy.* 6, no. 1 (2023): 24–24. https://doi.org/10.69554/opeg2767.

Cheng, Lu, Kush R. Varshney, and Huan Liu. "Socially Responsible AI Algorithms: Issues, Purposes, and Challenges." *arXiv (Cornell University)*, ahead of print, Cornell University, January 2021. https://doi.org/10.48550/arXiv.2101.02032.

Choung, Hyesun, Prabu David, and John S. Seberger. "A Multilevel Framework for AI Governance." *arXiv (Cornell University)*, ahead of print, Cornell University, January 2023. https://doi.org/10.48550/arxiv.2307.03198.

Custers, Bart. "New Digital Rights: Imagining Additional Fundamental Rights for the Digital Era." *Computer Law & Security Review* 44 (December 2021): 105636–105636. https://doi.org/10.1016/j.clsr.2021.105636.

El-Khoury, Moufid, and Saleh Albarashdi. "Navigating the Privacy Landscape of Healthcare-Driven AI in the Middle East: Case Studies from Oman, Qatar, and Saudi Arabia." *Social Sciences and Humanities Open* 11 (2025). https://doi.org/10.1016/j.ssaho.2025.101492.

Elmahjub, Ezieddin. "Artificial Intelligence (AI) in Islamic Ethics: Towards Pluralist Ethical Benchmarking for AI." *Philosophy & Technology* 36, no. 4 (2023). https://doi.org/10.1007/s13347-023-00668-x.

Eskhita, Radwan, and Evert Stamhuis. "The Influence of the Brussels Effect on the Interpretation of Data Protection Laws in the Gulf." *Global Journal of Comparative Law* 13, no. 2 (2024): 261–78. https://doi.org/10.1163/2211906x-13020007.

Evangelou, Semira Maria, Eleftheria Lito Michanetzi, and Michalis Xenos. "Exploring the Impact of Negative Online Feedback on Well-Being: A Comprehensive Analysis Incorporating Big-Five Personality Traits and Physiological Responses." *Computers in Human Behavior Reports* 15 (July 2024): 100457–100457. https://doi.org/10.1016/j.chbr.2024.100457.

Farooq, Ali, Joni Salminen, Justin D. Martin, Kholoud Aldous, Soon-Gyo Jung, and Bernard J. Jansen. "Exploring Social Media Privacy Concerns: A Comprehensive Survey Study Across 16 Middle Eastern and North African Countries." *IEEE Access* 12 (2024): 147087–105. https://doi.org/10.1109/ACCESS.2024.3463869.

Firdaus, Zulfa Amalia, and Nabila Luthvita Rahma. "The Reason For Childfree In Maqashid Sharia Perspective." *Ahkam: Jurnal Hukum Islam* 13, no. 1 (2025): 85–107. https://doi.org/10.21274/ahkam.2025.13.1.85-107.

Freedom House. "Jordan: Freedom on the Net 2024 Country Report." Accessed October 25, 2025. https://freedomhouse.org/country/jordan/freedom-net/2024.

Ghaleb, Sherien, Maram AlFaraedy, Ghada Al Shamsy, Abdulrahman Ali ALZahrani, and Magdy A. Kharoshah. "Shari'ah Law and Courts." In *Encyclopedia of Forensic and Legal Medicine: Volume 1-4, Third Edition*, vol. 4. Elsevier, 2024. https://doi.org/10.1016/B978-0-443-21441-7.00034-0.

Gorian, Ella, and Noor Dzuhaidah Osman. "Digital Ethics of Artificial Intelligence (AI) In Saudi Arabia and the United Arab Emirates." *Malaysian Journal of Syariah and Law* 12, no. 3 (2024): 583–97. https://doi.org/10.33102/mjsl.vol12no3.798.

Gruzd, Anatoliy, Jenna Jacobson, and Elizabeth Dubois. "Cybervetting and the Public Life of Social Media Data." *Social Media + Society* 6, no. 2 (2020). https://doi.org/10.1177/2056305120915618.

Iroegbu, Marvin, Freya O'Brien, Luna C. Muñoz, and Georgia Parsons. "Investigating the Psychological Impact of Cyber-Sexual Harassment." *Journal of Interpersonal Violence* 39 (February 2024): 3424–45. https://doi.org/10.1177/08862605241231615.

Issa, Hamzeh Abu, Mahmoud Ismail, and Omar Aamar. "Unauthorised Access Crime in Jordanian Law (Comparative Study)." *Digital Investigation* 28 (January 2019): 104–11. https://doi.org/10.1016/j.diin.2019.01.006.

Kelly, Christopher, and Tali Sharot. "Web-Browsing Patterns Reflect and Shape Mood and Mental Health." *Nature Human Behaviour*, ahead of print, Nature Portfolio, November 2024. https://doi.org/10.1038/s41562-024-02065-6.

Kutschera, Stefan. "Incidental Data: Observation of Privacy Compromising Data on Social Media Platforms." *International Cybersecurity Law Review* 4, no. 1 (2022): 91–114. https://doi.org/10.1365/s43439-022-00071-w.

Library of Congress, Washington, D.C. 20540 USA. "Jordan: New Anti-Cybercrimes Law Enacted." Web page. Accessed October 29, 2025. https://www.loc.gov/item/global-legal-monitor/2023-09-27/jordan-new-anti-cybercrimes-law-enacted/.

Liu, J. "Artificial Intelligence and International Law: The Impact of Emerging Technologies on the Global Legal System." *Economics Law and Policy* 7, no. 2 (2024). https://doi.org/10.22158/elp.v7n2p73.

Lu, Sylvia. *Regulating Algorithmic Harms*. January 2024. https://doi.org/10.2139/ssrn.4949052.

Maaytah, Sanaa, and Hiba Kobarie. "The Extent of the Impact of Cybersecurity Rules on Electronic Civil Transactions in Jordanian Law." *International Journal of Religion* 5, no. 10 (2024): 5191–98. https://doi.org/10.61707/ad442p10.

Machado, Helena, Susana Silva, and Laura Neiva. "Publics' Views on Ethical Challenges of Artificial Intelligence: A Scoping Review." In *AI and Ethics*. Springer Nature, December 2023. https://doi.org/10.1007/s43681-023-00387-1.

Magableh, Nabeel Zaid Suliman. "The Adequacy of the Laws Regulating Electronic Business in Jordan." *public administration and law review*, March 2024, 66–77. https://doi.org/10.36690/2674-5216-2024-1-66.

Maslej, Nestor, Loredana Fattorini, Raymond Perrault, et al. "Artificial Intelligence Index Report 2024." *arXiv (Cornell University)*, ahead of print, Cornell University, May 2024. https://doi.org/10.48550/arxiv.2405.19522.

Morandín-Ahuerma, Fabio. *Ten UNESCO Recommendations on the Ethics of Artificial Intelligence*. September 2023. https://doi.org/10.31219/osf.io/csyux.

Nguyen, Andy, Ha Ngan Ngo, Yvonne Hong, Belle Dang, and Bich-Phuong Thi Nguyen. "Ethical Principles for Artificial Intelligence in Education." *Education and Information Technologies* 28, no. 4 (2022): 4221–41. https://doi.org/10.1007/s10639-022-11316-w.

OECD. "State of Implementation of the OECD AI Principles." *OECD Digital Economy Papers*, ahead of print, June 2021. https://doi.org/10.1787/1cd40c44-en.

"Oman's Telecom Sector Powers Ahead with Surge in IoT, Mobile Connections | Arab News." Accessed October 25, 2025. https://www.arabnews.com/node/2608769/business-economy.

Pagliaccio, David, Kate T. Tran, Elina Visoki, Grace E. DiDomenico, Randy P. Auerbach, and Ran Barzilay. "Probing the Digital Exposome: Associations of Social Media Use Patterns with Youth Mental Health." *NPP—Digital Psychiatry and Neuroscience* 2, no. 1 (2024). https://doi.org/10.1038/s44277-024-00006-9.

"Personal Data Protection Law in Jordan." Accessed October 30, 2025. https://www.dentons.com/en/insights/articles/2023/october/4/personal-data-protection-law-in-jordan.

Ploug, Thomas. "The Right Not to Be Subjected to AI Profiling Based on Publicly Available Data—Privacy and the Exceptionalism of AI Profiling." *Philosophy & Technology* 36, no. 1 (2023). https://doi.org/10.1007/s13347-023-00616-9.

Pooranian, Zahra, Mauro Conti, Hamed Haddadi, and Rahim Tafazolli. "Online Advertising Security: Issues, Taxonomy, and Future Directions." *IEEE Communications Surveys & Tutorials* 23, no. 4 (2021): 2494–524. https://doi.org/10.1109/comst.2021.3118271.

Prihantoro, Hijrian Angga. "Examining Witness Interest: The Obstacles of Testimony in Islamic Jurisprudence and Positive Law." *Justicia Islamica* 21, no. 1 (2024): 1–22. https://doi.org/10.21154/justicia.v21i1.8653.

Reis, Andreas, Rohit Malpani, Effy Vayena, et al. "Ethics and Governance of Artificial Intelligence For Health : Who Guidance." In the *Research Portal Denmark*. Technical University of Denmark, 2021. https://local.forskningsportal.dk/

Saura, José Ramón, Vatroslav Škare, and Đurđana Ozretić Došen. "Is AI-Based Digital Marketing Ethical? Assessing a New Data Privacy Paradox." *Journal of Innovation & Knowledge* 9, no. 4 (2024): 100597–100597. https://doi.org/10.1016/j.jik.2024.100597.

SentinelOne. "What Is Spam? Types, Risks, and How to Protect Your Business." SentinelOne, July 17, 2025. https://www.sentinelone.com/cybersecurity-101/cybersecurity/what-is-spam/.

Serna, Francisco José Aranda. "The Legal Regulation of Spam: An International Comparative Study." *Journal of Innovations in Digital Marketing* 3, no. 1 (2022): 1–11. https://doi.org/10.51300/jidm-2022-44.

Sibawaihi, Muhammad, Devika Rosa Guspita, and Badriyah Badriyah. "Islamic Legal Strategies in Indonesian Contexts to Combat Cybercrime and the Spread of Illegal Data Dissemination." *Justicia Islamica* 21, no. 2 (2024): 357–76. https://doi.org/10.21154/justicia.v21i2.9587.

Solaiman, Barry, Ayesha Bashir, and Fama Dieng. "Regulating AI in Health in the Middle East: Case Studies from Qatar, Saudi Arabia and the United Arab Emirates." In *Edward Elgar Publishing eBooks*. Edward Elgar Publishing, 2024. https://doi.org/10.4337/9781802205657.00028.

Solove, Daniel J., and Woodrow Hartzog. "The Great Scrape: The Clash Between Scraping and Privacy." *SSRN Electronic Journal*, ahead of print, RELX Group (Netherlands), January 2024. https://doi.org/10.2139/ssrn.4884485.

Stahl, Bernd Carsten, Andreas G. Andreou, Philip Brey, et al. "Artificial Intelligence for Human Flourishing – Beyond Principles for Machine Learning." *Journal of*

Business Research 124 (December 2020): 374–88. https://doi.org/10.1016/j.jbusres.2020.11.030.

Stevens, Francesca, Jason R. C. Nurse, and Budi Arief. "Cyber Stalking, Cyber Harassment, and Adult Mental Health: A Systematic Review." In *Cyberpsychology, Behaviour and Social Networking*, vol. 24, no. 6. Mary Ann Liebert, Inc., November 2020. https://doi.org/10.1089/cyber.2020.0253.

Tridwip. "Phishing, Crypto and Fake Job Scams up 35% in Q1 2025 in Oman." *Muscat Daily| Oman News |Business | Sports |Lifestyle*, May 26, 2025. https://www.muscatdaily.com/2025/05/26/35-rise-in-cyber-fraud-crimes-in-q1-2025-rop/.

Trigui, Hana. "Exploring AI Governance in the MENA Region: Gaps, Efforts, and Initiatives." *SSRN Electronic Journal*, ahead of print, RELX Group (Netherlands), January 2024. https://doi.org/10.2139/ssrn.4796071.

Trigui, Hana, Fatma Z. Guerfali, Emna Harigua-Souiai, et al. "Exploring AI Governance in the Middle East and North Africa (MENA) Region: Gaps, Efforts, and Initiatives." *Data & Policy* 6 (January 2024). https://doi.org/10.1017/dap.2024.85.

Ullah, Imdad, Roksana Boreli, and Salil S. Kanhere. "Privacy in Targeted Advertising on Mobile Devices: A Survey." *International Journal of Information Security* 22, no. 3 (2022): 647–78. https://doi.org/10.1007/s10207-022-00655-x.

Zadjali, Halah Al. *Building the Right AI Governance Model in Oman*. September 2020, 116–19. https://doi.org/10.1145/3428502.3428516.

الأشقر, أحمد حسني علي. "الخصوصية الرقمية في عصر الذكاء الاصطناعي:, قراءة في التشريعين الأردني والفلسطيني." *مجلة جامعة القدس المفتوحة للبحوث الإنسانية والاجتماعية*, January 2025, 32–32. https://doi.org/10.33977/0507-000-066-003.