Scholar Insight Journal
https://scholarinsightjournal.com/
Volume.3, Issue.3 (Oct-Dec-2025)
Acceptance Date: 18-12-2025

HEC PAKISTAN Y Category
ONLINE - ISSN- 3006-9785
PRINT - ISSN- 3007-245X
Publication Date: 25-12-2025

Regulating the Future: A Comparative Analysis of Pakistan's Need for EU-Based Cyber Privacy Frameworks

[1]Muhammad Murtaza Chishti
PhD Law Scholar, Times University, Multan, Pakistan
Email: mmoeezmurtaza@gmail.com
https://orcid.org/0009-0000-5854-2222
[2]Dr. Malik Imtiaz Ahmad
Senior Member, IEEE
Assistant Professor, Times University, Multan, Pakistan
Imtiaz.malik.ahmed@gmail.com
https://orcid.org/0000-0001-7226-656X
[3]Prof. Dr. Matloob Ahmad (Corresponding Author)
Dean Faculty of Arts &Social Sciences
The University of Faisalabad, Pakistan
dean.is@tuf.edu.pk

Abstract

The use of cyber technologies in Pakistan has been both exposed in the governance system, commercial practices, law enforcement, and daily living, providing a great benefit by causing a real efficiency improvement, and at the same time, also presents severe threats to privacy and data security, among other essential rights. Without a regulatory framework of AI that is elaborate, enforceable, and solid in use rights-based protections, the remaining ones are still in bits, mostly aspirational, and poor. In comparison, the coherent risk-oriented regulatory model implemented in the European Union via the General Data Protection Regulation (GDPR) and the Artificial Intelligence Act (AI Act) is based on the principles of human dignity, accountability, and democratic control.

The article aims at achieving three research objectives: first, due to its doctrinal nature, to examine the current and proposed laws on data protection and AI-based decision-making in Pakistan; second, to comparatively explore how the EU GDPR and AI Act respond to analogous regulatory challenges with binding obligations, institutional regulation and risk classification; and third, to normatively evaluate the AI governance framework in Pakistan against the international human rights standards, specifically, the International Covenant on Civil and Political Rights (ICCPR) and the EU fundamental rights standards.

The methodological approach of the study is the doctrinal legal analysis, the comparative legal research, and normative evaluation of the statutory texts, policy documents, judicial principles, and scholarly literature. The analysis demonstrates that there are considerable regulatory gaps in Pakistan, such as a lack of enforceable limitations on automated decision-making, insufficient

HEC PAKISTAN Y Category
ONLINE - ISSN- 3006-9785
PRINT - ISSN- 3007-245X
Publication Date: 25-12-2025

transparency and accountability requirements on AI developers and implementers, ineffective redressing of rights infringements, and the absence of an independent regulatory body that has effective powers. The EU model, in its turn, combines the principles of data protection, including lawfulness, minimization of information, and limitation of purpose, transparency, and accountability, and AI-specific risk-based regulation and strong mechanisms of institutional enforcement.
Keywords: Digital rights, Cyber-policing, AI-enabled law enforcement, Algorithmic bias, Pakistan data protection.

Introduction

Artificial Intelligence (AI) has accelerated to a central infrastructure that defines the governance, economic frameworks, security, and daily social relations of people all over the world (Završnik, 2020; Yeung, 2018). The systems powered by AI are currently commonly used in automated decision-making, predictive analytics, biometric identification, surveillance, and data-driven administration of the population. These technologies hold great efficiency, accuracy, and innovation at the same time; they evoke significant legal and ethical issues associated with privacy, data protection, equality, due process, and democratic accountability (Binns, 2018; Mittelstadt et al., 2016). Such issues are especially acute in the developing jurisdictions where the legal and institutional structure has not kept up with the fast adoption of technology.

In Pakistan, AI-powered environments are being implemented in social governments, police, financial institutions, online resources, and monitoring systems. Rather, they are mostly used in a dis-organized and poorly developed regulatory environment. The legal tools available, including most famously suggested data protection laws and industry-specific regulations, are still either wishful or have few teeth, providing minimal protection against unaccountable automated decision-making and large-scale data processing (Digital Rights Foundation, 2020). The lack of AI-specific laws, meaningful regulators, and binding rights-based responsibilities leads to a regulatory vacuum where algorithmic systems are being run with very little transparency or accountability. Such a regulatory loophole serves as a great threat to constitutional duties of dignity, privacy and due process under Pakistani laws, especially due to the rising state and private-sector surveillance activities.

In comparison, the European Union (EU) has developed into a global norm-setter in the regulation of digital technologies with the implementation of the General Data Protection Regulation (GDPR) and the Artificial Intelligence Act (AI Act). The GDPR offers an extensive data protection framework of automated processing, profiling, and algorithmic decision-making to which tenets of lawfulness, transparency, limit of purpose, data minimization, and accountability (Regulation (EU) 2016/679) are embedded. On this basis, the AI Act introduces a risk-based regulatory framework that creates a binding structure by categorizing AI systems based on the extent of their effect on primary rights and subjecting them to equivalent requirements, such as bans on unacceptable-risk AI, ex ante compliance tests, and institutional supervision measures (European Union, 2024). All of these tools are indicative of a careful effort to make sure that technological innovation does not become the primary priority at the expense of human dignity, democratic governance, and the rule of law (Veale & Borgesius, 2021).

The regulatory difference between Pakistan and the EU is a strong argument in the comparative legal analysis. Although the regulatory framework of the EU cannot be

HEC PAKISTAN Y Category
ONLINE - ISSN- 3006-9785
PRINT - ISSN- 3007-245X
Publication Date: 25-12-2025

wholesale transferred to Pakistan because of the differences in socio-economic background, institutional capabilities, and constitutional systems, its rights-based and risk-based approach provides useful normative advice. This is especially applicable since Pakistan is a State Party to the International Covenant on Civil and Political Rights (ICCPR) which presents binding requirements of ensuring privacy (Article 17), equality before the law (Article 26), and the right to an effective remedy (Article 2(3)) which is being more and more engaged by AI-driven decision-making systems (ICCPR, 1966; UN Human Rights Committee, 2018).

It is against this background that this paper will discuss the possibility and manner in which Pakistan may establish a consistent, enforceable, and rights-based AI governance structure that is informed by the principles of EU regulation and the international law of human rights. It conducts a doctrinal review of the current and proposed legal frameworks on the protection of data and AI in Pakistan, and then compares the EU GDPR and AI Act. The paper also compares the regulatory framework of Pakistan with the global human rights standards, i.e. the ICCPR and EU basic rights norms. In so doing, the article serves as a contribution to the new body of research on the issue of AI regulation in the Global South and sets the agenda of context-sensitive legislative and institutional reforms that can help enhance not only fundamental rights but also responsible and accountable innovation.

The intensive implementation of Artificial Intelligence (AI) in the sphere of government, police activity, business, and social activity has transformed the state-market-individual relationships fundamentally. Although AI systems are expected to be efficient, predictive, accurate, and innovative in administration, they are also introducing unmatched risk to privacy, data protection, equality, due process, and democratic accountability (Mittelstadt et al., 2016; Završnik, 2020). Such risks are especially acute in the areas where regulatory institutions are poorly developed, enforcement mechanisms are not well established, and rights-based technology regulation is still at the wish level. In this context, the current research will have a significant legal, policy, and academic interest as it attempts to fill the most important regulatory and normative gaps in the emergent AI regulation environment in Pakistan.

On the doctrinal level, the study presents one of the limited systematic legal studies of the fragmented system of AI governance and data protection in Pakistan. Current AI regulation literature in Pakistan is predominantly descriptive, policy-driven, or technology-centered and does not apply many bindings legal norms, constitutional values, and enforceable rights standards (Digital Rights Foundation, 2020). This research paper makes clear the extent to which current legislative frameworks are inefficient in terms of legal regulation of automated decision-making, algorithmic profiling, and high-volume data processing.

The study also singles out structural shortcomings in the regulatory framework in Pakistan, such as a lack of clear restrictions on automated decision-making, a poorly defined transparency and explainability requirement, scanty right redress mechanisms, and the absence of an external monitoring body with investigatory and punitive facilities. The relevance of these doctrinal results is that they take the discussion out of the vague issue of AI risks, and rather show how the gap in the law turns into the gaps in the fundamental rights. By so doing, the study gives a foundation of evidence for future legislative reform and the judicial interpretation in Pakistan.

In comparison, the research works will further the emerging literature review that determines the involvement of the European Union as a global norm entrepreneur in technology regulation (Bradford, 2020). The regulatory system in the EU, based on the

HEC PAKISTAN Y Category
ONLINE - ISSN- 3006-9785
PRINT - ISSN- 3007-245X
Publication Date: 25-12-2025

General Data Protection Regulation (GDPR) and the Artificial Intelligence Act (AI Act), is the most detailed effort to balance the development of AI with the basic rights, democracy, and the rule of law (Veale & Borgesius, 2021). Through a systematic comparison of the regulatory approach of Pakistan with the rights-based and risk-based model of the EU, the research points to the legal differences as well as normative priorities that define the distinctions between the type of governance based on the rights-oriented and the market or security-oriented approaches.

Research Method

The research used qualitative legal research, based on the doctrinal legal analysis, comparative legal methodology, and normative human rights assessment. This multi-method legal approach is explained by the character of the research problem, which is related to the sufficiency of the existing and suggested legal frameworks that regulate Artificial Intelligence (AI) and data protection in Pakistan and their correspondence with the international and comparative regulations.

Since the AI governance is still mostly controlled by legal guidelines, policy tools, and judicial values and not by empirical data, the qualitative legal approach is the most suitable. The authors do not attempt to quantify the technological performance or the attitudes of the population, but inquire reflectively about the legal texts, institutional structures, and normative pledges to evaluate whether the regulatory system of Pakistan is effective in protecting the fundamental rights in AI-related contexts (McCrudden, 2006).

The main methodological pillar of the research is doctrinal legal research. It is the methodical study, explanation, and integration of the legal rules that are expressed in the constitutional provisions, statutes, the delegated laws, the policy documents and the judicial rulings (Hutchinson and Duncan, 2012).

The doctrinal analysis is used to analyse: in the Pakistani context.

- Guarantees under the constitution regarding the dignity, privacy, equality and due process;
- Current and suggested data protection laws;
- Sector-specific regulatory tools that pertain to digital governance and surveillance;
- Courts of law expressing judicial values on the issue of privacy and fundamental rights.

Such an approach allows the research to detect the internal inconsistency, normative gaps, and the weaknesses of the enforcement of the legal framework related to AI in Pakistan. The analysis of doctrine is especially important in determining whether automated decision-making is legally acceptable or not, whether remedies are available, and the degree of regulation.

This paper uses a functional and normative comparative legal framework to compare the regulatory framework of Pakistan with the General Data Protection Regulation (GDPR) and the Artificial Intelligence Act (AI Act) of the European Union. The application of comparative law does not form a form of legal transplantation, but rather a means of analysis to determine best practices, regulatory principles and institutional frameworks to be used in AI rights governance (Zweigelt and Kötz, 1998).

The EU framework is used as a comparative standard because it is a risk-based, binding, and comprehensive approach to AI regulation that is explicitly based on the protection of fundamental rights. The comparison focuses on:

HEC PAKISTAN Y Category
ONLINE - ISSN- 3006-9785
PRINT - ISSN- 3007-245X
Publication Date: 25-12-2025

- Regulatory goals and values underlining them;

Treatment of profiling and automated decision-making;

- Risk classification and proportionality mechanism;
- Accountability, transparency and enforcement mechanisms;

The comparison analysis makes it possible to identify the differences and similarities between the two jurisdictions and evaluate the possibility of transferring EU-inspired regulatory components into the constitutional and institutional context of Pakistan.

The normative approach to human rights is used to assess the AI governance framework of Pakistan in terms of international legal requirements, especially the International Covenant on Civil and Political Rights (ICCPR). This is not an analytical legal methodology that looks into the nature of the laws, but it evaluates whether current and proposed laws are in compliance with substantive human rights standards (Fredman, 2008).

The study uses some of the most important human rights principles, which serve as evaluative criteria, such as legality, necessity, proportionality, transparency, equality, and access to effective remedies. Applicable interpretative advice by the UN Human Rights Committee, such as General comments on privacy and non-discrimination, is included to help in seeking out what is required by the state in technologically mediated situations. Such normative evaluation is necessary to understand whether the regulatory framework of Pakistan provides suitable protection to individuals against arbitrary or discriminatory practices in decision-making and surveillance through AI, and to base reform proposals on the binding international law as opposed to policy discretion.

The research uses only secondary sources of law, which demonstrates its doctrinal and normative focus. These include:

The provisions of the constitution, laws, bills to be passed, EU laws, international treaties, and the official policy documents.

Rulings and principles, which have been expressed by Pakistani higher courts, the European Court of Justice and international human rights entities.

Articles in peer-reviewed journals, academic monographs, law commission reports, publications of civil society, and authoritative commentary on AI, data protection, and human rights. Credibility, relevance and normative authority are considered as priorities in the choice of sources. Analysis of policy documents or draft legislation critically evaluates the legal status and enforceability of that policy document or legislation.

The thematic and issue-based analysis is performed on the basis of the main regulatory dimensions, which are determined in the conceptual framework. These include:

Data processing legal bases;

- Data subject and affected individual rights;
- Developers and deployers of AI;
- Monitoring, responsibility and enforcement.

The themes are discussed individually in the context of the Pakistani law and then compared and contrasted with the EU model. Thereafter, normative benchmarks of human rights are used to measure compliance and determine shortcomings. This strategized analytical methodology guarantees methodological consistency and analytical profundity.

The research is restricted in a number of ways. To start with, it lacks empirical sampling of the field, technical assessment of AI systems, and quantitative measures of the results of AI marketing. Second, it concentrates more on the implications of AI on civil and political rights, not on the economic or social rights. Third, the comparative analysis is restricted to the EU as the main standard owing to the exclusion of the other jurisdictions,

HEC PAKISTAN Y Category
ONLINE - ISSN- 3006-9785
PRINT - ISSN- 3007-245X
Publication Date: 25-12-2025

including China.

Since the research is founded on publicly available legal and academic sources only, there are neither human participants in the research, personal data, nor confidential information. In this regard, it does not need formal ethical approval. However, academic integrity is ensured by properly citing sources, being faithful to their representation, and critically analyzing the current scholarship.

This approach offers a systematic and stringent framework for investigating AI governance in Pakistan by incorporating doctrinal analysis, comparative legal studies, and normative human rights analysis. It allows the research to surpass mere descriptive narratives, as well as to provide a change of legal and contextualized, rights-based reform proposals to entrench rights-based AI governance into the constitutional and international legal obligations of Pakistan.

Results and Discussion

In qualitative research that is doctrinal legal research, data is not represented by numerical data but rather by legal norms, regulatory texts, judicial interpretations, and authoritative policy instruments. Consequently, the chapter examines the statutory guidelines, draft laws, constitutional values, global treaties, and comparative EU tools that regulate Artificial Intelligence (AI), information protection, and automated decision-making. Analysis is organized in terms of a thematic and issue-based approach, and it is organized around the basic regulatory dimensions identified in the conceptual framework: legality, transparency, accountability, risk management, institutional oversight and protection of fundamental rights.

These materials are analyzed through the three perspectives of the human rights theory, surveillance theory and risk-based regulation, such that the study is able to evaluate not only what the law gives but also what it is unable to stop. Such a combined strategy would allow for a critical examination of the AI governance framework in Pakistan against the EU regulatory framework and the international human rights commitments.

Analysis demonstrates that Pakistan does not have a specific regulatory framework related to AI which is dedicated and enforced now. Legal instruments requiring data processing and digital governance are currently dealt with in a quite sectoral and fragmented way, and do not directly interact with AI-assisted decision-making, algorithmic profiling, and/or automated surveillance. This lack of regulation establishes a normative vacuum where AI systems are implemented with no legal frameworks or procedures of accountability.

In comparison to the EU AI Act, in which AI systems are outlined straight out and categorized based on risk, the Pakistani legal framework does not view AI as a specific subject of regulation. Consequently, AI technologies fall under the umbrella principle of general data protection or administrative law, which is inadequately suited to deal with the size, obscurity, and predictability of AI. This finding supports the concerns expressed in the literature that emerging jurisdictions tend to take reactive or technology-neutral approaches that do not reflect AI-specific harms.

The statistics also show excessive dependence on policy documents, draft legislation, and executive guidelines and instability over binding statutory norms. Although such instruments are indicative of regulatory intention, they are unenforceable and fail to constitute legally enforceable rights and duties. This is contrary to the binding regulatory model of the EU that both GDPR and AI Act establish tangible obligations on data controllers, AI developers, and deployers and provide sanctions and remedies. Theoretically, such reliance on soft law compromises the law's certainty and weakens the rule of law.

HEC PAKISTAN Y Category
ONLINE - ISSN- 3006-9785
PRINT - ISSN- 3007-245X
Publication Date: 25-12-2025

Considering the human rights approach, it does not comply with the aspect of legality in Article 17 of the ICCPR, in which interfering with privacy should be based on an accessible, accurate, and enforceable law.

A key observation of this paper is the fact that no legal boundaries on automated decision-making in Pakistan are explicitly given. The current structures do not limit AI system utilization in high-stakes areas like law enforcement, surveillance, credit rating, or service provision by the government. Neither do they need human supervision, performance evaluation, or explanation of algorithmic results. In comparison, the GDPR offers conditional limitations to only automated determinations, and the AI Act offers superior protection to high-risk AI systems, such as human-in-the-loop demands and conformity testing. In Pakistan, there are no similar protections, putting citizens at the risk of being exposed to opaque and, perhaps, arbitrary decisions, compromising procedural fairness and due process.

A deep lack of transparency is also found during the analysis. The legal tools in place in Pakistan do not subject AI deployers to any meaningful requirements on how they may arrive at decisions, the data they use, or the reduction of risks. The problem with such an opaqueness is especially troublesome in the context of surveillance and law enforcement, in which people might never learn that AI systems have contributed to making a decision that impacts their rights. The surveillance theory can be used to understand how this obscurity gains institutional authority and makes algorithmic power acceptable. AI systems can be viewed as an invisible governance system without transparency and contestability, and they support asymmetries between the state and individuals.

Among the most relevant structural gaps that have been identified is the absence of a truly independent supervisory authority that possesses sufficient powers to control AI and data protection. The executive influence in proposed regulatory bodies, the limitation of their mandates and their inability to enforce have become common in Pakistan. Contrary to this, the EU approach focuses on the independence of institutions, as an ingredient of sound rights protection. The GDPR and the AI Act supervisory authorities have investigative, corrective, and sanctioning forces that allow proactive control instead of reactive response to complaints. Lack of similar institutions in Pakistan is a big setback to accountability and compliance.

The information also indicates that the framework used in Pakistan offers few opportunities to people to question AI-based rights abuses. It is common that the remedies of the judiciary are inaccessible because of awareness, complexity of the procedures, and evidentiary barriers, especially in situations where the processes of algorithms are not transparent. Human rights-wise, this failure contravenes Article 2(3) of the ICCPR, which covers the right to an effective remedy. The discussion points out that remedies are not auxiliary measures but are critical elements of rights protection in algorithmic governance.

The contrastive analysis shows that the power of the EU is the combination of the principles of data protection with the regulation of AI. The GDPR provides minimum protections that are relevant to all data processing, and the AI Act expands these principles by a risk-based approach that is specific to AI systems. This regulatory framework deals with risks of AI either horizontally (across sectors) or vertically (based on the level of risk severity). The structure of Pakistan does not provide such integration, as the country has unequal protections.

This lack of risk classification in Pakistan is a critical finding. The law fails to regulate all digital processing as one where harm is most probable, regardless of whether the AI application is low-risk or high-risk. Operationalized in the EU AI Act, risk-based regulation is a systematic way of prioritizing regulation, resource allocation, and

HEC PAKISTAN Y Category
ONLINE - ISSN- 3006-9785
PRINT - ISSN- 3007-245X
Publication Date: 25-12-2025

proportionality. It has been argued that the solution is to go to a simpler risk-based approach, which could considerably improve the regulatory efficacy of Pakistan without stifling innovations.

Using the international human rights standard, the analysis discovers that AI governance in Pakistan is below the ICCPR provisions. The absence of legality, need, proportion, and proper solutions in the regulation of AI is a threat of capricious intrusion into privacy and discriminatory results. It is highlighted in the discussion that AI governance is not simply a policy option but a law that will come as a result of the international obligations of Pakistan. The inability to control AI properly can make the state vulnerable to international scrutiny and constitutional protection of dignity and equality.

The results overall show that the AI governance system in Pakistan is typified by regulatory fragmentation, lack of accountability, institutional weakness, and normative mismatch with the human rights norms. Conversely, the EU model demonstrates how rights protection can be incorporated in the governance of technology by means of binding law, risk-based regulation, and institutional control.

It is emphasized during the discussion that all of these deficiencies are not the unavoidable outcomes of technological progress but rather the outcomes of regulatory decisions. Pakistan can balance innovation and basic rights protection by implementing an EU-oriented, but context-sensitive approach that is based on the constitutional values and the international human rights law.

Conclusion

This study has discussed regulation issues in Pakistan with cyber advancement systems using a doctrinal, comparative, and human rights-based approach. The paper aimed to review both current and proposed legal systems regulating AI and data protection in Pakistan to contrast them with the rights-focused regulatory model of AI and big data in the European Union, specifically, the General Data Protection Regulation (GDPR) and the Artificial Intelligence Act (AI Act), and to analyze Pakistan in the context of the international human rights laws, and specifically the International Covenant on Civil and Political Rights (ICCPR).

The results prove that the existing cyber governance structure in Pakistan is still in fragments, poorly developed, and more of a vision document. The lack of cyber-specific laws, laxity in the regulation of automated decision-making, limited transparency and accountability requirements, and the absence of an independent control body all lead to an empty regulatory space. It is this vacuum that enables AI systems, especially in the fields of surveillance, law enforcement, and the running of government, to operate without significant legal challenge, and as such, individuals are exposed to additional risks of arbitrary decision making, discriminatory performance and the unlawful interception of privacy and dignity. In comparison, the regulatory strategy of the EU demonstrates how the principle of binding law, the regulation of risks, and institutional control can entrench the foundational rights protections in AI regulation. Both the GDPR and the AI Act show that technological innovation does not have to be against human dignity, democratic accountability, or the rule of law. Notably, the EU model demonstrates that proportional ex ante regulation is normal, desirable and legally viable.

The study concludes that Pakistan is unable to control AI in a consistent and enforceable way, not just a policy vacuum, but a constitutional and international issue of human rights. Being a State Party to ICCPR, Pakistan has the positive responsibility to make

HEC PAKISTAN Y Category
ONLINE - ISSN- 3006-9785
PRINT - ISSN- 3007-245X
Publication Date: 25-12-2025

sure that emerging technologies do not contravene protected rights. Devoid of immediate legal and institutional change, AI will simply establish surveillance, obscurity, and asymmetry of power that cannot coexist with the constitutional provisions in Pakistan and international obligations.

Recommendations

- Based on the results of the study, the following are the recommendations that will be made to enhance cyber governance in Pakistan in a way that is rights-centred, context-sensitive, and institutionally possible:
- Pakistan must also embrace specific AI laws that will specify the systems of AI, govern automated decision-making, and set binding responsibilities of both government and non-government stakeholders. Although wholesale transplantation of the EU AI Act is neither realistic nor even a good idea, its risk-based architecture is an important blueprint. There should be increased protection on high-risk AI systems, especially those implemented in law enforcement, surveillance, welfare administration, and biometric identification.
- The law protecting data must be clear in terms of AI processing, profiling, and making inferences. Enforceable rights to transparency, explanation, and challenge of automated decisions should be included in the law, provided with references to the GDPR, but with some adjustments to the Pakistani legal context.
- In order to govern AI successfully, an independent regulatory body that investigates, corrects and punishes is necessary. This power needs to be autonomous at the institution level without executive control, properly staffed and authorized by law to monitor state and private AI applications.
- Human rights and algorithmic impact assessment that should be performed before the implementation of AI systems should be legally enforced by the government and high-risk non-governmental actors. These evaluations must analyse the threats to privacy, equality and due process, and must be regulated.
- The courts must take the initiative in making interpretations of the constitutional rights in technologically mediated situations. There must be procedural reforms to enhance access to effective remedies, such as reducing evidentiary thresholds to which algorithmic opaqueness denies individuals the chance to establish harms.

HEC PAKISTAN Y Category
ONLINE - ISSN- 3006-9785
PRINT - ISSN- 3007-245X
Publication Date: 25-12-2025

- Institutional capacity-building, judicial training, and public awareness efforts should be supplemented by legal reform. An effective law is no guarantee of a successful implementation without a regulatory experience and social awareness of its significance.

References

1. Ahmed, M. W. (2024). Artificial intelligence and legal ethics. International Journal of Law and Politics Studies, 6(5), 226–227. https://doi.org/10.32996/ijlps.2024.6.5.12
2. Abolaji, E. O., & Akinwande, O. T. (2024). AI powered privacy protection: A survey of current state and future directions. World Journal of Advanced Research and Reviews, 23(3), 2687–2696. https://doi.org/10.30574/wjarr.2024.23.3.2869
3. Al-Billeh, T., Hmaidan, R., Al-Hammouri, A., & Al Makhmari, M. (2024). The risks of using artificial intelligence on privacy and human rights: Unifying global standards. Journal of Modern Humanities, 31(2). https://doi.org/10.18196/jmh.v31i2.23480
4. Bashir, M. (2021). Surveillance and panopticism in the digital age. Qatar Journal of Social Sciences and Humanities, 2(1), 11–16. https://doi.org/10.55737/qjssh.257455953
5. Bertaina, S., Biganzoli, I., Desiante, R., Fontanella, D., Inverardi, N., Penco, I. G., & Cosentini, A. C. (2025). Fundamental rights and artificial intelligence impact assessment: A new quantitative methodology in the upcoming era of AI Act. Computer Law & Security Review, 56, 106101. https://doi.org/10.1016/j.clsr.2024.106101
6. Busuioc, M. (2021). Accountable artificial intelligence: Holding algorithms to account. Public Administration Review, 81(6), 1049–1059. https://doi.org/10.1111/puar.13293
7. Custers, B. (2022). New digital rights: Imagining additional fundamental rights for the digital era. Computer Law & Security Review, 44, 105636. https://doi.org/10.1016/j.clsr.2021.105636
8. Donnelly, S., Ríos Camacho, E., & Heidebrecht, S. (2024). Digital sovereignty as control: The regulation of digital finance in the European Union. Journal of European Public Policy, 31(8), 2226–2249. https://doi.org/10.1080/13501763.2023.2295520

9. Fernández-Basso, C., Gutiérrez-Batista, K., Gómez-Romero, J., Ruiz, M. D., & Martín-Bautista, M. J. (2024). An AI knowledge-based system for police assistance in crime investigation. Expert Systems, 41(1), e13524. https://doi.org/10.1111/exsy.13524
10. Gul, S., Ahmad, F., & Ahmad, R. (2025). Digital evidence and procedural fairness: Reforming cybercrime prosecution in Pakistan. Journal for Social Science Archives, 3(2), 544–554. https://doi.org/10.59075/jssa.v3i2.260
11. Haley, P. (2025). The impact of biometric surveillance on reducing violent crime: Strategies for apprehending criminals while protecting the innocent. Sensors, 25(3160). https://doi.org/10.3390/s25103160
12. Joh, E. E. (2019). Policing the smart city. International Journal of Law in Context, 15(2), 177-182. https://doi.org/10.1017/S1744552319000107
13. Kausche, K., & Weiss, M. (2025). Platform power and regulatory capture in digital governance. Business and Politics, 27(2), 284–308. https://doi.org/10.1017/bap.2024.33
14. Lynch, N. (2024). Facial recognition technology in policing and security—Case studies in regulation. Laws, 13(3), 35. https://doi.org/10.3390/laws13030035
15. Mason, M. (2010). Sample size and saturation in PhD studies using qualitative interviews. Forum: Qualitative Social Research, 11(3), Article 8. https://doi.org/10.17169/fqs-11.3.1428
16. Mantelero, A. (2018). AI and big data: A blueprint for a human right, social and ethical impact assessment. Computer Law & Security Review, 34(4), 754–772. https://doi.org/10.1016/j.clsr.2018.05.017
17. Matar, R., & Murray, D. (2024). Re-thinking international human rights law's approach to identity in light of surveillance and AI. Queen Mary University London. https://doi.org/10.1093/hrlr/ngaf016
18. Mittelstadt, B. (2019). *Principles alone cannot guarantee ethical AI. Nature Machine Intelligence, 1*(11), 501-507. https://doi.org/10.1038/s42256-019-0114-4
19. Murray, D. (2024). "Police use of retrospective facial recognition technology: A step change in surveillance capability necessitating an evolution of human rights law." The Modern Law Review. https://doi.org/10.1177/09240519241253061

20. Nagy, N. (2023). "Humanity's new frontier": Human rights implications of artificial intelligence and new technologies. Hungarian Journal of Legal Studies, 64(2), 236–267. https://doi.org/10.1556/2052.2023.00481
21. Nshimiyimana, F. R. (2025). Balancing cybersecurity and fundamental rights: The responsibility of states to address cyber threats. Essays of Faculty of Law, University of Pécs Yearbook, (2025), 1–15. https://doi.org/10.15170/studia.2025.01.15
22. Safdar, M. A., & Ghafoor, S. (2025). Algorithmic justice: Reassessing legal ethics through the lens of AI and moral philosophy. International Journal of Linguistics Applied Psychology and Technology, 2(6). https://ijlapt.strjournals.com/index.php/ijlapt
23. Shad, K. B. (2023). Artificial intelligence-related anomies and predictive policing: Normative (dis)orders in liberal democracies. AI & Society, 40(2), 891–902. https://doi.org/10.1007/s00146-023-01751-9
24. Shaelou, S. L., & Razmetaeva, Y. (2023). Shaping the digital legal order while upholding rule of law principles and European values. European Journal of Law and Technology, 14(1), 1–20. https://doi.org/10.1007/s12027-023-00777-2
25. Suddle, F. R., Pervaiz, S., & Nawaz, S. (2025). Unmasking digital deviance: Analyzing cybercrime trends via social media in Pakistan. Advance Social Science Archive Journal, 4(1), 834–848. https://doi.org/10.55966/assaj.2025.4.1.064
26. Urquhart, L., & Miranda, D. (2022). Policing faces: The present and future of intelligent facial surveillance. Information, Communication & Society, 25(8), 1169–1186. https://doi.org/10.1080/13600834.2021.1994220.
27. Warso, Z. (2022). Human rights requirements for person-based predictive policing: Lessons from selected ECtHR case law and its limits. Technology and Regulation, 71–80. https://doi.org/10.26116/techreg.2022.007
28. Wei, W., & Liu, L. (2024). Trustworthy distributed AI systems: Robustness, privacy, and governance. ACM Computing Surveys, 56(5), Article 103. https://doi.org/10.1145/3645102
29. Završnik, A. (2020). Criminal justice, artificial intelligence systems, and human rights. ERA Forum, 20(4), 567–583. https://doi.org/10.1007/s12027-020-00602-0