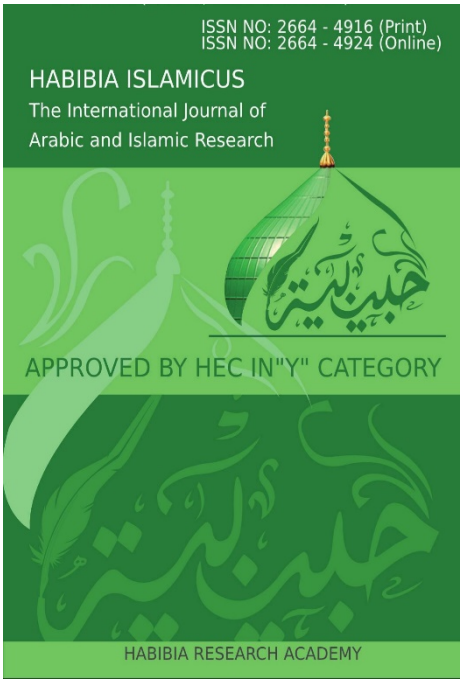
HABIBIA ISLAMICUS
(The International Journal of Arabic &Islamic Research) (Quarterly) Trilingual (Arabic, English, Urdu) ISSN:2664-4916 (P) 2664-4924 (E)
Home Page: http://habibiaislamicus.com
Approved by HEC in Y Category
We have indexed with IRI (AIOU), Australian Islamic Library, ARI, ISI, SIS, and Euro Pub.
PUBLISHER HABIBIA RESEARCH ACADEMY
Project of **JAMIA HABIBIA INTERNATIONAL,** Reg. No: KAR No. 2287 Societies Registration Act XXI of 1860 Govt. of Sindh, Pakistan.
Website: www.habibia.edu.pk,



TOPIC:

SECURING THE DIGITAL LANDSCAPE: ADVANCING DATA PRIVACY, CYBERSECURITY, AND AI ETHICS IN PAKISTAN

AUTHORS:

1- *Aliya Saeed, Research Scholar PhD(LAW), School Of Law, University Of Karachi, Email ID: aaliasaeed@yahoo.com Orcid ID: https://orcid.org/0009-00001-3823-4123*
2- *Dr. Abdullah Jumani, Deputy District Attorney Law/ Solicitor, Government of Sindh Email ID: Abdullahjumani1@gmail.com Orcid ID: https://orcid.org/0000-0001-7801-059x*

How to Cite: Saeed, Aliya, and Dr. Abdullah Jumani. 2025. "SECURING THE DIGITAL LANDSCAPE: ADVANCING DATA PRIVACY, CYBERSECURITY, AND AI ETHICS IN PAKISTAN". *Habibia Islamicus (The International Journal of Arabic and Islamic Research)* 9 (1):01-13
DOI: https://doi.org/10.47720/hi.2025.0901e01.
URL: https://habibiaislamicus.com/index.php/hirj/article/view/314
Vol. 9, No.1 || January –March 205 || P. 01-13
Published online: 2025-03-30

QR. Code

SECURING THE DIGITAL LANDSCAPE: ADVANCING DATA PRIVACY, CYBERSECURITY, AND AI ETHICS IN PAKISTAN

Aliya Saeed, *Dr. Abdullah Jumani,*

ABSTRACT:
In order to better understand how data security, cybersecurity, and AI ethics, are changing in Pakistan, this study employs a method of qualitative investigation that includes stakeholder interviews and an analysis of current regulatory frameworks. To determine the degree to which present legislation addresses the issue of digital rights, the study examines the views of cybersecurity, AI governance, and legislative experts as well as business executives. Although Pakistan has made significant progress in passing digital legislation, the statistics indicate that much more work has to be done in the areas of cybersecurity infrastructure and comprehensive data protection laws. The analysis also demonstrates that the ethical standards for AI development are still unclear, highlighting the need for improved legal protections and the suggestions that came out of this inspection, which include drafting ethical AI frameworks that adhere to international standards, strengthening cybersecurity, and adopting a national data privacy legislation. These findings will assist researchers and policymakers in determining what constitutes a good, moral, cyberspace in Pakistan.

KEYWORDS: *Cybersecurity; Digital Rights; AI Ethics; Legal Frameworks; Data Privacy*

1. INTRODUCTION:

Many elements of contemporary society have been greatly changed by the swift change in digital technologies, resulting in a rapid, but deeply intertwining convolution between data privacy, cybersecurity and AI ethics. With the rise of digital interactions turning ubiquitous, legal implications of these areas are being looked in detail by the policymakers, legal scholars and technology specialists. Protecting people's personal information against misuse and unlawful reuse is the goal of data protection laws like the “General Data Protection Regulation (GDPR)” in the European Union (Korff, 2023). But there are difficulties involved, because there's a fine line to be drawn between innovation and regulation. Yet, these laws are important but it is often difficult to enforce them. The latter also underscores the continued need for dialogue among stakeholder.

Like for cybersecurity regulations, regulations regarding AI ethics are meant to prevent critical infrastructure and sensitive information from being attacked by cyberspace, whereas AI ethics frameworks imply promoting and making the development and use of technologies based on artificial intelligence respect human rights and social values (Ali, 2022). While there are some extensive data privacy and cybersecurity regulations in place in different areas, there still stands a gap in analysis of them as far as the legal scope on the digital development is concerned. So far, most of cybersecurity and data protection analysis has focused on the technical aspects; however, there has been a lack of the broader legal and ethical issues taken into consideration (Blauth et al., 2022; Ashraf and Mustafa, 2025). This research gap, therefore, motivates a need for more integrated approach linking the

legal analysis to technological factors to grapple the challenges of digital transformation (Treleaven et al., 2023; Shamiulla, 2019; Zahid et al., 2024).

The urgency of this research is underscored by the escalating frequency and sophistication of cyber-attacks, which pose substantial risks to both individuals and organizations (Saleem et al., 2023; and Rasyid et al., 2024). Moreover, the proliferation of AI technologies raises critical ethical questions regarding bias, accountability, and transparency (Wang (2020); Walters and Novak (2021); and Solove (2010)). Addressing these issues is crucial not only for protecting individual rights but also for maintaining public trust in digital systems and promoting a secure and equitable digital society (King et al., 2020; LOZONSCHI and BAKHAYA, 2023).

Although much of the existing literature has delved into numerous facets of data privacy, cybersecurity and AI ethics, there is (however) a significant deficiency in research that thoroughly investigates the intersection of these areas and their collective legal ramifications (Pagallo and Quattrocolo, 2018). This study aims to bridge this gap: it provides an integrated analysis of the legal frameworks that govern data privacy, cybersecurity and AI ethics. Furthermore, it evaluates their effectiveness in confronting the challenges posed by a digital society (Velasco, 2022).

As nations across the globe persist in grappling with these challenges, Pakistan's digital landscape is concurrently evolving, thereby introducing a unique array of legal and regulatory considerations. In this regard, this research aims to investigate the legal ramifications of data privacy legislation, cybersecurity protocols and AI ethics within Pakistan's digital framework. Specifically, the study will tackle the following research inquiries: How do current legal structures in Pakistan confront the challenges presented by data privacy, cybersecurity and AI ethics? What gaps and overlaps exist within these frameworks and how can they be improved to effectively address the burgeoning digital issues in Pakistan? However, it is essential to recognize that these considerations are not isolated; rather, they are interconnected in significant ways.

The rest of the paper is organized as: section 2 explains literature review; section 3 discusses methodology part; section 4 discusses results and discussion and finally section 5 concludes this research.

2. Literature Review:

The enhanced proliferation of technology-based solutions has created a significant number of discussions among scholars concerning the laws governing data protection, cyber security and artificial intelligence morality. This paper provides an overview of how the General Data Protection Regulation (GDPR) has affected the discussion of data privacy around the globe. The GDPR was passed in 2018 and sets very high requirements for data protection, it stresses concepts including, but not limited to: transparency, responsibility and consent (Erikha & Saptomo, 2024; Jabeen et al., 2024; Johns, 2021). Previous authors include Meghana et al. (2024) who have explored privacy in a theoretical context recommending for contextual essentially that are flexible given the dynamic nature of digital worlds. However, this approach is not without problems, because it demands a broad

understanding of dynamic technologies. However, there is ongoing discussion of such frameworks across the board, even as many believe the general concept to be sound See Chauhan et al. 2024 for details. In the United States, the prolonged lack of federal legislation means that the legislative structure is becoming scattered, and regional laws like the California Consumer Privacy Act (CCPA) try to resolve the issue. Chitimira and Ncube (2021) consider such a decentralised structure, thus, advocating for a coordinated global approach addressing standardisation of the cross border data flows. Moving forward, Custers (2022) builds on the definition with the more elaborated study of contextual integrity where he introduces a framework that correlates privacy norms with specific contexts of a society.

The growth economy has also featured predominantly across the global discourse concerning data protection. For instance, India's Personal Data Protection Bill (PDPB) intends to achieve user rights and innovation objectives. However, it has been criticised for not having the enforcement measures, which are provided in the GDPR (Dilek et al., 2015). The same applies to China in its Data Security Law that props up state dominance over data, which is troubling with regard to privacy and surveillance (Mijwil et al., 2023). These risks have increased in numbers and sophistication, thus the call for sound regulation of cybersecurity. Cybersecurity regulations play a crucial role in protecting critical assets and data (Blauth et al., 2022). Over the United States, there is the Cybersecurity Information Sharing Act (CISA) while in the EU there is the Network and Information Systems (NIS) Directive, whose main aim is to boost cooperation and protection. However, Shepitko et al. (2024) notes that such regulations are often travelled and rarely synchronized with the rapidly changing threat landscape. The issue of international cooperation can be identified as a common trend in cybersecurity research. In LOZONSCHI and BAKHAYA (2023), the authors discuss the centrality of multilateralism with regards to threat such as ransomware attacks and state-sponsored cyber espionage. The Budapest Convention on Cybercrime serves as a basic framework; however, its weak ratification in a number of states including Asian countries makes the need for more open agreements evident (Zarina et al., 2019).

Unfortunately, the adoption of cybersecurity regulation encounters numerous hurdles in most developing countries. For instance, specific regional conventions such as the Africa's Malabo Convention provided an exhaustive legal regime on cybersecurity and data protection but is scarcely implemented due to financial challenges as noted by Yeoh (2019). Likewise, the efforts to harmonize cybersecurity laws through regional contracts face obstacles in regions like South America, that obstacle is usually linked with the political and economic differences (Yadav, 2021). As it is often the case, the concept is clear while execution complexities reduce the chances of implementing changes.

This concept of the ethical implication of artificial intelligence has been receiving some attention in the past few years. Ashraf and Mustafa (2025) have put forward a model for AI Ethics based on four fundamental principles namely – transparency, accountability, and

fairness. In the study, ethical challenges related to algorithmic decision making are discussed by Omar and Zangana (2024) such as discrimination. In particular, Puchalski et al. (2024) provides a comparative overview of four sets of AI ethics guidelines and brings to light such frequently appearing concepts as beneficence, and justice.

The use of AI and related ethical issues has some remarkable relevance to law: Duan (2022) argues that current legislation still has drawbacks regarding autonomous decision-making or data-focused profiling. In their conjectural study published in 2024, Shetty et al. raise awareness of the need to implement ethical audit and control mechanisms to make use of the AI results that are considered relevant to society. Sibai (2020) agrees also pointed out that the development of AI technologies can increase the status of dominance gap in society. However, it is important to also look at these ethical dimensions because they define the future development of technology and the role that is has in society.

What is important to note is that the ethical questions related to AI in the Global South are often colored by completely different socio-economic realities. For example, India intending to develop AI National Strategy focuses on AI solutions to developmental problems; nonetheless, the document acknowledges the need for holistic ethical frameworks (Sikos, 2021). In the same way, Call for Papers African scholars have also decried for AI for Good Research that highlight issues faced by African and other developing countries, and more importantly champion the causes that are close to the African and other Third World values (Trajkovska et al., 2024). Privacy, Cybersecurity and Artificial Intelligence are a rapidly emerging intersection that has gained a lot of importance in recent years.

Mijwil, Gaviria, and Poot (2023) advocate that use of a contextual integrity framework; which can explain privacy cohesively as a concept in the modern technological world. The integration of the concepts is important because it responds to the needed concerns about the ethical and effectiveness. In Walters and Novak (2021), the authors discuss legal effects of big data analytics and call for the need to establish rules that would control big data as well as protect civil liberties at the same time. Erikha and Saptomo (2024) inspected the synthesis of legal analysis with technology and ethical points of view. Their investigations are concerned that the fragmented approaches are inadequate to address the challenges arising from AI digital transformation where data privacy and cybersecurity meet. This point of view is supported by Solove (2010), who underlines the need for the joint work done by technical, legal and ethical disciplines.

3. Methodology

This study aims to determine the legal issues of data privacy laws, cybersecurity regulations, and AI ethical standard in Pakistan's digital society whereby it adopted a qualitative research design. There are insightful approaches to elaborate the mentioned subject, but qualitative research appears to be most appropriate for the inquiry; it is based on the fact that it is capable to provide deeper understanding of the multifaceted legal and ethical problems and attempt to look at them from different viewpoints, through the lens

of experiences. This approach of course provides detailed examination but also places these details in the broader perspective that is necessary when looking at law, technology and ethics in Pakistan. However, such an exploration can be a little tricky since several aspects have to be taken into consideration even as the return on the investment is felt.

The primary data sources are spread across different categories of resources such as legal and policy documents, journals and articles and expert interviews. Underlying legal documents including the "Prevention of Electronic Crimes Act (PECA) 2016" and MoITT (2021) are most scrutinized in the present study in order to assess the contemporary ecosystem. Reference has also been made to the general data protection regulation — GDPR as well as the cybersecurity standards described by the International Telecommunication Union — ITU so as to make comparative analysis. To a certain extent, documents such as the DRF yearly reports, for the years 2018 to 2023, help identify the challenges and gaps within legal frameworks in Pakistan. Furthermore, not a single work of academic literature is insignificant to this line of research.

Interview with specialists is another important segment of data collection method that needs to be mentioned. A series of semi-structured interviews are conducted with respondents across a range of professions (scholars of law, policy makers and specialists in cybersecurity and Artificial Intelligence ethicists). The typical stakeholders include executives from PTA; officials from NR3C; and technology law firms that are highly influential within the country. These interviews provide first-hand information on the various impediments and the practical consequences of operationalizing privacy and cybersecurity rules and regulations in Pakistan. However, the major challenge which arises when addressing the examined issues is the fact that the issue under discussion is often a multifaceted one, and therefore can be viewed from different standpoints. While all of these impressions are admittedly useful, they may also highlight a few internally contradictory features of the current regulation.

The process of data collection utilizes two central methodologies: document analysis and semi structured interviews. The concept of document analysis involves the assessment of the legislation texts, policies, and articles to identify appropriate trends, patterns and shortcomings of the regulations. For example, while the PECA 2016ossier examines the provisions related to the prevention of cybercrime, the (PDPB) 2021ossier is evaluated on the basis of norms related to data protection. Semi-structured interview also contains specific questions as well but give the participants the right to explain their experience and perception. Policy makers are asked questions regarding enforcement while computer security experts focus on the open insecurity in Pakistan information technology. While these methodologies may appear somewhat different the combination thereof helps in providing a complete picture of the matters under consideration because, indeed, there is a need for qualitative and quantitative approaches. This way of conducting analysis appears to be much more comprehensive and detailed.

The collected data is analyzed using thematic analysis which is a method of identifying, analyzing patterns and reporting themes in collected data. This process begins with the

practise of familiarisation (the role of the researcher in the data); the legal texts, the tapes and the policy documents are re-read. Following this, coding occurs: terms are identified and grouped into significant and comprehensive patterns. For instance, code such as "regulatory gaps", "cybersecurity threats" and "AI ethical issues" are helpful in sorting the information out nicely. The codes generated later on are then grouped into larger categories for easier identification of patterns such as 'conformity with global standards' and 'difficulties experienced in implementing' the laws. The indicated themes are then reviewed and purified with a view of ensuring their reliability and connection with the research objectives. Thus, the identified legal topics are compared with those elicited from interviews with experts in international law field. This is important for achieving comprehensive knowledge though it requires caution when performing the process.

Finally, these findings are discussed within the context of Pakistani socio-legal context with the help of quotes from the informants and selected legal documents. This paper highlights that this qualitative approach allows for a better, sensitive and detailed understanding of the legal implications of data privacy laws, cybersecurity regulations, and ethic of AI in Pakistan. Through analysing legal materials, scholarly approaches and professionals' views, the study identifies loopholes in regulation; as a result, it provides recommendations for enhancing Pakistan's laws. The results aim at providing useful insights to policymakers, legal scholars and technologists, and promote the progress of more well-coordinated and effective legal approaches to the issues stemming from digital transformation. However, these research findings are very favourable and while appreciating this research, it is important to respect the fact that there are if form qualitative research.

4. Results and Discussion

The analysis of the existing Pakistani laws (supplemented by the information obtained from the interviews) identifies tensions and weaknesses concerning the application of data protection legislation and cyber security measures as well as the absence of proper policies on the use of AI. Key findings include: nevertheless, such gaps are very important as they slow the development in the protection of the citizens' data. While there are some attempts to solve these problems, the absence of the coordinated action is still an obstacle. This situation necessitates urgent attention, but stakeholders must collaborate to devise effective solutions.

4.1. Inadequate Legal Frameworks:

The Prevention of Electronic Crimes Act (PECA) 2016 primarily focuses on cybercrime prevention; however, it lacks comprehensive provisions for data protection and privacy. The draft Personal Data Protection Bill (PDPB) 2021 proposes a foundational framework for data protection, but it remains unimplemented this leaves critical legal voids. Interviewees highlighted those existing regulations are reactive (rather than proactive), failing to adequately address the emerging challenges posed by AI technologies. Although

there are attempts to regulate, the current state of the law is insufficient because it does not anticipate future developments.

4.2. Misalignment with International Standards:

Comparison of Pakistan's standards with the international best practices, including the EU's GDPR shows the Pakistani laws are considerably behind. For instance, while GDPR entails the user's consent and data minimisation, it did not find substantial implementation in the PDPB. However, this disparity makes one wonder about the viability of the strategies that Pakistan involved in avalanche. Somewhat improvement has however been made but this shows why there is need for better regulation of the market, consumer protection is still an important matter.

4.3. Weak Enforcement Mechanisms:

Interviews with informants from the PTA and the NR3C have disclosed that enforcement is highly constrained mainly because of resource mobilization and lack of adequate technical capability. The participants, however, noted that there is still a serious problem of sometimes lack of cohesiveness among the regulation agencies; this, they said, aggravates the problems of enforcement. Still, there are some attempts to enhance this issue; however, the problem faced is still a concern due to several factors.

4.4. Ethical Concerns in AI Deployment:

In Pakistan, there is (currently) no particular legal policy that exists regarding ethics of artificial intelligence. This absence of rigidity is dubious when it comes to algorithms, especially about questions related to bias, oversights and explanation of the function. Experts have emphasized the risks associated with unregulated AI deployment: problems like risk of misuse for surveillance, data use and potential other negative impacts that could well be realized at some time in the future. Nevertheless, the need to solve these problems is acute, because their consequences can be dramatic. While there are debates on how such information have to be controlled, the lack of an official system still raises concern.

4.5. Public Awareness and Digital Literacy:

From the documents available and interviews carried out as part of this research, there was a notable lack of public awareness, to a big extent, of their data privacy rights as well as cybersecurity. This lack of awareness prevents effective compliance and campaigning for stiffer laws though these issues should be solved because education can bring about a knowledgeable society. Thus, despite the new efforts being already made, the situation cannot be considered as pressing enough; therefore, there is a should continuing of focusing on this problem.

4.6. Discussion

Thus, the results stress on the urgent need and demand for the establishment and implementation of effective legal strategies, which address the emerging issues of the rapidly evolving digital world in Pakistan. Lagging within the current regulatory environment, especially concerning the slow compliance of the Personal Data Protection Bill (PDPB) 2021, threatens the citizen and businesses with data leakage and cyber threats. Currently, given the lack of adequate data protection law, those whose rights to data privacy

has been infringed have very few legal remedies they can avail themselves of. It is only when it is compared with other developed countries' standard like GDPR, possible to highlight many loopholes in regulations in Pakistan. For instance, data minimization and accountability principles of GDPR are important for building people's confidence in technology; but these principles are not well reflected in Pakistani laws. Adopting such standards could help enhance Pakistan's rank within the global economy and improve the trust of the stakeholders within its digital environments.

The enforcement challenges described in this study (which are not negligible) confirm the need for institutional changes. There is therefore the need to enhance the technical capability of agencies as the PTA and NR3C among others. However, promoting cooperation with other agencies could improve enforcement outcomes and solve the existing problem of fragmentation of regulating authorities. The lack of regulation IA ethics remains worrying since PA has has started implementing more AI Technologies. There options as the kind of long-term approach to reduce moderate risks that was discussed or prevent them at all might include the creation of ethical standards of AI, which were mentioned in a work by Mijwil et al. (2023), to prevent the situations like algorithmic bias or lack of responsibility into consequential actions taken by AI systems. However, public awareness and digital literacy come out as critical success factors, this is important in creating effectiveness of data privacy and cybersecurity regulation frameworks. Awareness campaigns as well as local organizational projects could help people pressure authorities to provide better security.

Altogether, Pakistan's digital society is at the crossroads; on one hand, there is the rapid advancement in technology, on the other there needs to be progressive legal and ethical responses.

The findings of this study underscore the urgency of a multi-faceted approach: The integrated one, which includes legislative changes, capacity development and communication with the public. It is this approach that is fundamental to meeting the data privacy, cybersecurity and AI ethical headline challenges. Nevertheless, these requirements are critical to ensure that the United States develops the proper foundation for a safe and inclusive cyberspace that complies with international norms because they promote the protection of the interests of all the affected subjects. Nonetheless, the direction ahead may not be clear, and everyone understands that only action must be taken.

5. Conclusion:

In conclusion therefore, it can be said that Pakistan's legal policies that regulate data protection, cyber security and AI regulation are still in their evolutionary phase in the country. However, much work still has to be done: research administered from the USA is more advanced, while parts of the world, such as the Middle East, are not represented enough. However, continuous evolving of these frameworks is required because these frameworks will define what shape the technological development in the country in the future There is still a long way to go.

The codes (and standards) are inconsequential to address the rapidly evolving threats brought by technological advancements. In order to protect the rights of the citizens and foster security The Constitution of each country provides for the following regime in the context of the contemporary digital landscape. It is crucial for Pakistan to adopt the more extensive and liberal legal systems which conform to procedures acceptable in other developed countries. Enhancing the protection of personal data is very important; improving cyber security and developing well-defined ethical standards for its applications will be useful for creating a more robust and credible digital environment. However, this challenge is multifaceted because, while the dominant idea is that of creativity, there are also ethical factors to consider. Although some improvements have been made, still a number of barriers exist.

The policy prescriptions for Pakistan include the critically urgent need for the government and its agencies to update and enforce strict data protection policies (for example, the introduction of general data protection regulation-like legislation). Besides, introducing the needed cybersecurity infrastructures and advancing a strategic and integrative national cybersecurity plan would help in mitigating the rising threats of cyber threats.

While artificial intelligence technologies are continuously evolving, Pakistan has to also establish an ethical guideline with which it will be moulding these systems so as to uphold their efficiency, fairness and responsiveness. This is important because the stakeholder awareness campaigns and institutional development projects are required to introduce new audiences of citizens to key legal developments affecting them in the context of the digital environment. Thus, the problem persists on the infant level despite the general move forward, largely due to the combination of technology and law.

Ideally for future research it is appropriate to look for the effectiveness of Pakistan current digital laws especially when Pakistan laws are analysed against those countries which have similar socio-economic and technological fabric. Future research can also focus on the developments of human rights and technology research is also important because investigations of legal possibilities to harmonize innovation and protection are essential. But investigating how those regulations impacted AI innovation, however, or evaluating the local ethical issues arising from AI rules, would prove valuable. This could in the future help to inform in the county of Pakistan policy formulation, a move that would however warrant a formulation of a balanced strategy. However, examining the influence of AI regulations on innovation, as well as ethical considerations within the local context, would yield significant insights. This could ultimately aid in shaping policy in Pakistan, although it requires a nuanced approach.

REFERENCES:

1. Ali, A. (2022). Cyber Crime Investigation and Forensics: Leveraging AI and Big Data for More Effective Solutions.

2. Ashraf, Z. A., & Mustafa, N. (2025). AI and Cyber Laws. In *Intersection of Human Rights and AI in Healthcare* (pp. 353-376). IGI Global Scientific Publishing.

3. Blauth, T. F., Gstrein, O. J., & Zwitter, A. (2022). Artificial intelligence crime: An overview of malicious use and abuse of AI. *Ieee Access*, *10*, 77110-77122.

4. Chauhan[1], R., Mehtar, K., Kaur, H., & Alankar, B. (2024). Evaluating Cyber-Crime Using Machine Learning and AI Approach for Environmental Sustainability. *SUSTAINABLE DEVELOPMENT THROUGH MACHINE LEARNING, AI AND IOT: Second*, 37.

5. Chitimira, H., & Ncube, P. (2021). The regulation and use of artificial intelligence and 5g technology to combat cybercrime and financial crime in south african banks. *Potchefstroom Electronic Law Journal/Potchefstroomse Elektroniese Regsblad*, *24*(1).

6. Custers, B. (2022). AI in Criminal Law: an overview of AI applications in substantive and procedural Criminal Law. *Law and artificial intelligence: regulating AI and applying AI in legal practice*, 205-223.

7. Dilek, S., Çakır, H., & Aydın, M. (2015). Applications of artificial intelligence techniques to combating cyber crimes: A review. *arXiv preprint arXiv:1502.03552*.

8. Digital Rights Foundation (DRF) Reports (2018–2023).

9. Duan, Z. (2022). Artificial Intelligence and the Law: Cybercrime and Criminal Liability. By Dennis J. Baker and Paul H. Robinson (Routledge, 2021, 280pp.£ 120 hb).

10. Erikha, A., & Saptomo, A. (2024). Dilemma of Legal Policy to Address Cybercrime in the Digital Era. *Asian Journal of Social and Humanities*, *3*(3), 499-507.

11. Jabeen, M., Aakif, Z., & Afridi, H. A. (2024). Unlocking Pakistan's digital potential: A roadmap for workforce digitalization and economic transformation. *Journal of Information Technology Teaching Cases*, 20438869241280980.

12. Johns, I. (2021). Role of AI in Tackling Cybercrime. *Jus Corpus LJ*, *2*, 1233.

13. King, T. C., Aggarwal, N., Taddeo, M., & Floridi, L. (2020). Artificial intelligence crime: An interdisciplinary analysis of foreseeable threats and solutions. *Science and engineering ethics*, *26*, 89-120.

14. Korff, D. (2023). Tricking an AI system & the Cybercrime Convention. *Available at SSRN 4584116*.

15. Kolochenko, I., & Heiskell, M. P. Generative AI, Cybersecurity And Cybercrime For Lawyers: Myths, Risks And Benefits.

16. LOZONSCHI, C., & BAKHAYA, I. (2023, May). Artificial Intelligence and its Impact on Cybercrime. In *International Conference on Cybersecurity and Cybercrime* (Vol. 10, pp. 120-126).

17. Meghana, G. V. S., Afroz, S. S., Gurindapalli, R., Katari, S., & Swetha, K. (2024, May). A Survey paper on Understanding the Rise of AI-driven Cyber Crime and Strategies

for Proactive Digital Defenders. In *2024 4th International Conference on Pervasive Computing and Social Networking (ICPCSN)* (pp. 25-30). IEEE.

18. *Ministry of Information Technology and Telecommunication (MoITT), 2021 as a source for the draft Personal Data Protection Bill (PDPB) (2021-2023)*

19. Mijwil, M. M., Aljanabi, M., & ChatGPT, C. (2023). Towards artificial intelligence-based cybersecurity: The practices and ChatGPT generated ways to combat cybercrime. *Iraqi Journal For Computer Science and Mathematics*, *4*(1), 8.

20. Omar, M., & Zangana, H. M. (Eds.). (2024). *Redefining Security With Cyber AI*. IGI Global.

21. Pagallo, U., & Quattrocolo, S. (2018). The impact of AI on criminal law, and its two fold procedures. In *Research handbook on the law of artificial intelligence* (pp. 385-409). Edward Elgar Publishing.

22. Prevention of Electronic Crimes Act (PECA) 2016.

23. Puchalski, D., Pawlicki, M., Kozik, R., Renk, R., & Choraś, M. (2024, July). Trustworthy AI-based Cyber-Attack Detector for Network Cyber Crime Forensics. In *Proceedings of the 19th International Conference on Availability, Reliability and Security* (pp. 1-8).

24. Rasyid, M. F. F., SJ, M. A., Mamu, K. Z., Paminto, S. R., Hidaya, W. A., & Hamadi, A. (2024). Cybercrime Threats and Responsibilities: The Utilization of Artificial Intelligence in Online Crime. *Jurnal Ilmiah Mizani: Wacana Hukum, Ekonomi Dan Keagamaan*, *11*(1), 49-63.

25. Saleem, M. S., Malhooz, F., & Fatima, T. (2023). From Cyber-crimes to Cyber-Security: Exploring Legal Minefield of Artificial Intelligence in Pakistan. *Pakistan Research Journal of Social Sciences*, *2*(3).

26. Shamiulla, A. M. (2019). Role of artificial intelligence in cyber security. *International Journal of Innovative Technology and Exploring Engineering*, *9*(1), 4628-4630.

27. Shetty, S., Choi, K. S., & Park, I. (2024). Investigating the Intersection of AI and Cybercrime: Risks, Trends, and Countermeasures. *International Journal of Cybersecurity Intelligence & Cybercrime*, *7*(2), 3.

28. Shepitko, V., Shepitko, M., Latysh, K., Kapustina, M., & Demidova, E. (2024). Artificial intelligence in crime counteraction: From legal regulation to implementation. *Social and Legal Studios*, *1*(7), 135-144.

29. Sikos, L. F. (2021). AI in digital forensics: Ontology engineering for cybercrime investigations. *Wiley Interdisciplinary Reviews: Forensic Science*, *3*(3), e1394.

30. Sibai, F. N. (2020, June). AI crimes: a classification. In *2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)* (pp. 1-8). IEEE.

31. Solove, D. J. (2010). *Understanding privacy*. Harvard university press.

32. Treleaven, P., Barnett, J., Brown, D., Bud, A., Fenoglio, E., Kerrigan, C., ... & Schoernig, M. (2023). The future of cybercrime: AI and emerging technologies are creating a cybercrime tsunami.

33. Trajkovska, E., Del Becaro, T., & Mijalkov, B. (2024, September). PREVENTION OF CYBERCRIME IN THE AGE OF ARTIFICIAL INTELLIGENCE (AI) WITHIN THE EUROPEAN UNION. In *Proceedings of the International Scientific Conference" Social Changes in the Global World"* (Vol. 11, No. 11, pp. 178-190).

34. Velasco, C. (2022, May). Cybercrime and Artificial Intelligence. An overview of the work of international organizations on criminal justice and the international applicable instruments. In *ERA Forum* (Vol. 23, No. 1, pp. 109-126). Berlin/Heidelberg: Springer Berlin Heidelberg.

35. Walters, R., & Novak, M. (2021). Artificial intelligence and law. In *Cyber security, artificial intelligence, data protection & the law* (pp. 39-69). Singapore: Springer Singapore.

36. Wang, X. (2020, April). Criminal law protection of cybersecurity considering AI-based cybercrime. In *Journal of Physics: Conference Series* (Vol. 1533, No. 3, p. 032014). IOP Publishing.

37. Yadav, A. (2021). Education regarding impact of AI on cybercrimes and liability for AI. *Psychol. Educ.*, *58*(5), 1553-6939.

38. Yeoh, P. (2019). Artificial intelligence: accelerator or panacea for financial crime?. *Journal of Financial Crime*, *26*(2), 634-646.

39. Zahid, M. A., Muhammad, A., Khakwani, M. A. K., & Maqbool, M. A. (2024). Cybercrime and Criminal Law in Pakistan: Societal Impact, Major Threats, and Legislative Responses. *Pakistan Journal of Criminal Justice*, *4*(1), 223-245.

40. Zarina I, K., Ildar R, B., & Elina L, S. (2019). Artificial Intelligence and Problems of Ensuring Cyber Security. *International Journal of Cyber Criminology*, *13*(2).