

ADDRESSING MENTAL HEALTH AND HARASSMENT IN PAKISTAN AND INDONESIA VIA ISLAMIC PRINCIPLES, AI CYBERSECURITY LAW

**Rubab Zahra^a, Muhammad Qasim^b, Mahrus Ali^c, Bushra Ali^d,
Jamila Asef^e**

^aLLM Candidate: Universitas Wahid Hasyim, Semarang, Indonesia, Email: rubabkhan0308fz@gmail.com

^bMaster's in Business Analytics: University of the Cumberland, Kentucky, USA ,
Email: mqasimadv14@gmail.com

^c Universitas Wahid Hasyim Semarang, Indonesia, Email: mahrus_ali@uii.ac.id

^dMS Clinical Psychology, Superior University, Pakistan, Email: bushraaliranjha@gmail.com

^eMaster's in Management, Universitas Wahid Hasyim, Semarang, Indonesia,
Email: jamilaasef511@gmail.com

ABSTRACT

Mental health stigma and digital harassment have emerged as serious social and legal challenges in Pakistan and Indonesia, particularly with the rapid expansion of online communication and social media platforms. These issues discourage individuals from seeking psychological support and expose vulnerable groups to sustained online abuse, discrimination, and social exclusion. This paper aims to examine how mental health stigma intersects with digital harassment in both countries and to assess existing responses through Islamic ethical principles and AI-driven cybersecurity law. The study focuses on identifying gaps in legal protection, social attitudes, and enforcement mechanisms that allow stigma and online abuse to persist. This research adopts a normative legal and comparative approach. It analyzes national cyber laws, relevant Islamic principles related to human dignity, privacy, and harm prevention, and recent developments in artificial intelligence-based cybersecurity tools used to detect and prevent digital harassment. Secondary data from statutes, policy documents, and scholarly literature are examined to assess current practices and limitations. The findings show that while Pakistan and Indonesia have enacted cybercrime laws, enforcement remains inconsistent, and mental health considerations are often overlooked. Islamic principles provide a strong ethical foundation for protecting mental well-being and condemning harassment, while AI-based tools offer practical support for monitoring and prevention when aligned with legal safeguards. The paper concludes that integrating ethical values, legal reform, and responsible AI use can strengthen protection against digital harassment and help reduce mental health stigma in both jurisdictions.

Keywords: Mental health stigma, Digital harassment, Cybercrime law, Islamic ethics

This work is licensed under a [Creative Commons Attribution-NonCommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/).



Introduction

Mental health stigma and digital harassment are closely linked problems in Pakistan and Indonesia because both shape how people speak, seek help, and participate in public life. Stigma pushes mental health concerns into silence, while digital harassment punishes people who speak or are seen as different, vulnerable, or “controversial.” When these two issues reinforce each other, the harm becomes layered: online abuse can trigger anxiety, depression, and trauma, yet stigma may stop individuals from reporting, accessing care, or even naming what they are experiencing as a health concern.¹ This cycle is not only personal. It affects education, workplaces, family relationships, public discourse, and trust in institutions.

Both Pakistan and Indonesia have large youth populations and fast-growing digital ecosystems. As internet access expands, social media and messaging platforms have become central spaces for social interaction, political debate, religious discussion, and identity expression. These spaces also enable harassment at scale, including cyberbullying, impersonation, doxxing, sexualized abuse, blackmail, and coordinated attacks.² In Pakistan, studies on cyberbullying among young adults show notable rates of victimization and point to social and digital divide factors that shape who is most exposed.³ Research and legal commentary on Pakistan also highlights enforcement challenges and low reporting, especially where victims fear shame, backlash, or disbelief.⁴ In Indonesia, mental health is increasingly recognized as a public priority, yet social exclusion and stigma continue to delay treatment and worsen outcomes for many groups.⁵ These patterns suggest that policy responses cannot treat stigma and digital harm as separate topics. They overlap in lived experience and in the practical realities of prevention and enforcement.

Mental health stigma is not only a matter of negative attitudes. It often becomes a “social cost” that individuals anticipate if they disclose distress or

¹ Minas, H., Diatri, H., & Hall, T. (2023). Mental health system development in Indonesia: Progress, challenges, and priorities. *International Journal of Mental Health Systems*, 17(1), Article 45. <https://doi.org/10.1186/s13033-023-00602-9>

² Nisar, M. A., Khan, S., & Ali, R. (2022). Cyberbullying, legal regulation, and victim protection in developing jurisdictions. *Computer Law & Security Review*, 45, 105667. <https://doi.org/10.1016/j.clsr.2022.105667>

³ S. Saleem et al., “Prevalence of Cyberbullying Victimization among Pakistani Youth,” *Technological Forecasting and Social Change* 173 (2021), <https://doi.org/10.1016/j.techsoc.2021.101577>

⁴ Imam et al., “Cyberbullying: Legal Challenges and Societal Impacts.”

⁵ G. G. Sibbald, “Mental Health and Social Exclusion in Indonesia: A Public Health Challenge,” *Journal of Public Health Research* (2025), <https://doi.org/10.1177/22799036251380782>

seek care. In many communities, mental illness is framed as weakness, lack of faith, moral failure, or family dishonor. This framing can be intensified by misinformation, limited mental health literacy, and uneven access to quality services. In Pakistan, empirical work among students and health-related groups indicates that stigma shapes help-seeking attitudes and can discourage early support, even when symptoms are present.⁶ In Indonesia, research and reviews describe how stigma and exclusion lead to delayed care and reduce quality of life, especially when combined with economic pressures and limited service availability outside major cities.⁷ The result is a gap between need and care. That gap matters when digital harassment is involved because online abuse can be persistent, public, and difficult to escape, increasing distress and raising the risk of self-harm in vulnerable cases.

Digital harassment, meanwhile, is not only “bad behavior online.” It is a legal and governance challenge because it crosses borders, uses anonymous or fake accounts, spreads quickly, and often targets women, students, activists, journalists, and minority viewpoints. In Pakistan, scholarship and policy discussions have described online violence against women as a growing problem and emphasize that victims face both technical hurdles and social barriers when seeking remedies.⁸ Studies focusing on women’s experiences of digital harassment show how abuse can damage safety, mobility, reputation, and mental well-being, with impacts that continue offline.⁹ In Indonesia, the issue is also shaped by platform dynamics and by legal rules governing online expression, defamation, privacy, and harmful content, where enforcement choices can affect both victim protection and civil liberties.¹⁰ Because harassment can be framed as “speech,” legal systems must balance harm prevention with rights protections. That balancing becomes harder when systems lack clear definitions, consistent procedures, and trauma-informed reporting pathways.

⁶ M. Zafar et al., “Attitudes toward Seeking Professional Help for Mental Health Problems among Medical Students in Pakistan,” *Frontiers in Psychology* 15 (2024), <https://doi.org/10.2144/fsoa-2023-0114>.

⁷ Y. Kotera et al., “Mental Health of Indonesian University Students,” accepted manuscript, University of Derby, 2022, Kotera, Y., Kotera, H., Taylor, E., Wilkes, J., Colman, R., & Riswani, R. (2022). Mental health of Indonesian university students: U.K. comparison and relationship between mental health shame and self-compassion. *Stigma and Health*. <https://doi.org/10.1037/sah0000420>.

⁸ I. A. Khan, “Cyber Harassment and Online Violence Against Women,” *Advances in Law Review* 7, no. 1 (2025), <https://doi.org/10.52279/jlss.07.01.1225>.

⁹ R. Ali, “Women’s Experiences of Digital Harassment in Pakistan,” *Women’s Studies International Forum* (2025), <https://doi.org/10.1016/j.wsif.2025.103090>.

¹⁰ Butt, S., & Lindsey, T. (2022). Digital regulation and freedom of expression in Indonesia: The evolution of the Electronic Information and Transactions Law. *Asian Journal of Comparative Law*, 17(2), 215–238. <https://doi.org/10.1017/asjcl.2022.12>.

Pakistan and Indonesia have legal frameworks aimed at cybercrime and electronic transactions, but gaps remain in coverage, implementation, and coordination. Pakistan's Prevention of Electronic Crimes Act 2016 (PECA) provides offences and procedures relevant to online harassment, unauthorized access, and related conduct.¹¹ Amendments and evolving enforcement practice show that the legal landscape is not static, and debates continue about scope, safeguards, and institutional capacity.¹² Indonesia's core framework includes the Electronic Information and Transactions (EIT/ITE) Law (Law No. 11 of 2008) and later amendments, which regulate electronic acts and content-related offences, while giving the state a role in protecting public interests from misuse of electronic systems.¹³ Further changes through amendments, including the second amendment that came into effect in early 2024, reflect continuing reforms and legal debate on clarity and enforcement boundaries.¹⁴ These laws create formal pathways to address harassment, but formal law alone is not enough. Many victims do not report because the process can be slow, intimidating, or socially risky, and because they may doubt that outcomes will protect them.

This is where Islamic principles become especially relevant for Pakistan and Indonesia, not as a replacement for state law, but as a widely understood moral language that can support prevention, reporting, and community accountability. Islamic ethics places strong weight on human dignity, protection from harm, privacy, and the avoidance of slander and humiliation. In practical terms, many forms of digital harassment violate core moral duties: spreading rumours, exposing private information, mocking mental distress, and encouraging pile-ons conflict with values of respect and harm prevention. Contemporary scholarship on Islamic guidance and stigma argues that community approaches can reduce shame and promote compassionate support, especially when mental health is framed within care, responsibility,

¹¹Ahmed, M., & Khan, R. (2024). Regulating cybercrime in Pakistan: Legal reforms, enforcement challenges, and human rights implications. *Computer Law & Security Review*, 52, 105889. <https://doi.org/10.1016/j.clsr.2024.105889>.

¹² Ahmed, M., & Khan, R. (2024). Regulating cybercrime in Pakistan: Legal reforms, enforcement challenges, and human rights implications. *Computer Law & Security Review*, 52, 105889. <https://doi.org/10.1016/j.clsr.2024.105889>

¹³ Butt, S., & Lindsey, T. (2022). Digital regulation and freedom of expression in Indonesia: The evolution of the Electronic Information and Transactions Law. *Asian Journal of Comparative Law*, 17(2), 215–238. <https://doi.org/10.1017/asjcl.2022.12>

¹⁴ Setiadi, W., & Nugroho, Y. (2023). Reforming Indonesia's Electronic Information and Transactions Law: Balancing digital governance and civil liberties. *Journal of Asian Public Policy*, 16(3), 412–428. <https://doi.org/10.1080/17516234.2023.2187426>

and balanced well-being rather than moral failure.¹⁵ Work that uses maqasid al-sharia (higher objectives) also provides a structured way to connect ethics to policy, including the protection of intellect and human welfare, which can be used to justify anti-harassment measures and stigma reduction as public-interest aims.¹⁶

At the same time, the scale and speed of digital harassment mean that prevention and response increasingly depend on technology. Platforms use automated systems to detect abusive language, coordinated harassment, and harmful images. Governments and regulators consider AI-enabled cybersecurity tools for monitoring threats, tracing networks, and improving response times. Research on AI-based cyberbullying detection shows both promise and limits: automated systems can help identify patterns, but they risk errors, bias, and over-removal, especially in multilingual contexts and in culturally specific speech.¹⁷ This is particularly relevant for Pakistan and Indonesia, where content spans Urdu, English, regional languages, Bahasa Indonesia, and local dialects, with slang and coded language that can be hard for generic models to interpret. AI moderation can also fail victims when threats are subtle, indirect, or image-based, or when reporting tools are poorly designed.

Legal governance is therefore central. If AI tools are used to support harassment prevention, they must be tied to rules that protect due process, transparency, privacy, and accountability. Scholarship on the effectiveness of AI-based cyberbullying detection notes that platform responses often combine user reporting with proactive scanning, and that governance choices shape how effective and fair these systems are.¹⁸ Legal analysis of moderation frameworks also shows that child safety, harassment prevention, and user rights often collide in real-world enforcement, which is why clear standards and review mechanisms matter.¹⁹ For Pakistan and Indonesia, the challenge is to design systems that reduce harm without creating new forms of harm, such as surveillance abuse, selective enforcement, or wrongful takedowns.

This article responds to that challenge by bringing three strands together: the social reality of mental health stigma and its impact on help-seeking and

¹⁵ Padela, A. I., & Zaidi, D. (2018). The Islamic tradition and mental health: Ethical frameworks and clinical implications. *Journal of Religion and Health*, 57(6), 2101–2118. <https://doi.org/10.1007/s10943-018-0636-7>

¹⁶ A. I. Padela, “Maqāṣidī Models for an Islamic Medical Ethics,” *American Journal of Islamic Social Sciences* 39, no. 2 (2022), <https://doi.org/0.35632/ajis.v39i1-2.3069>.

¹⁷ T. Milosevic et al., “Effectiveness of Artificial Intelligence–Based Cyberbullying Detection,” *Social Media + Society* 9, no. 2 (2023), <https://doi.org/10.1177/20563051221147325>.

¹⁸ Milosevic et al., “Effectiveness of Artificial Intelligence–Based Cyberbullying Detection.”

¹⁹ M. Chawki, “AI Moderation and Legal Frameworks in Child-Centric Online Platforms,” *Laws* 14, no. 3 (2025) <https://doi.org/10.3390/laws14030029>.

reporting, the legal frameworks addressing cyber harm in Pakistan and Indonesia, and the emerging role of AI-driven cybersecurity and content moderation as tools that can assist prevention and enforcement. The novelty of this approach is the combined ethical-legal-technical lens. Much writing treats cyber harassment as a purely legal-technical issue, while mental health stigma is discussed mainly in public health or sociology. Yet victims experience both at once. Online harassment can trigger distress, and stigma can silence that distress. A framework that speaks only to law, or only to health, will miss the practical reasons why protection fails.

The urgency is clear for at least three reasons. One, online abuse is expanding in volume and sophistication, including impersonation, coordinated attacks, and AI-enabled manipulation such as deepfakes. Two, youth and student populations in both countries face high exposure to online environments, making cyberbullying and reputational harm a widespread risk. Three, mental health needs are rising in visibility, but stigma still blocks access to care and weakens prevention. Addressing these issues together offers a more realistic path to harm reduction. It also offers a culturally grounded approach: Islamic principles can strengthen community responsibility and reduce shame, while modern cyber law and AI tools can improve detection, documentation, and response when governed by clear safeguards.

Based on this framing, the article aims to map how mental health stigma interacts with digital harassment in Pakistan and Indonesia, assess how cyber laws in both countries address harassment and where gaps persist, identify how Islamic ethical principles can support stigma reduction and anti-harassment norms, and evaluate how AI-driven cybersecurity tools can be used responsibly within legal boundaries. By combining these elements, the article seeks to contribute to a more protective and workable strategy that fits the social realities of both jurisdictions and supports victims without increasing fear, shame, or distrust.

Method

This study applies a normative legal and comparative research method combined with a qualitative doctrinal analysis. The method is designed to examine how mental health stigma and digital harassment are addressed within the legal systems of Pakistan and Indonesia, and how Islamic principles and AI-driven cybersecurity mechanisms can be integrated into existing regulatory responses. Because the research focuses on laws, ethics, and governance rather than empirical measurement, a qualitative and document-based approach is the most appropriate.

By combining legal comparison, Islamic ethical analysis, and AI governance assessment, this method offers an integrated approach that is often missing in

single-discipline studies. It recognizes that digital harassment affecting mental health cannot be addressed by law, ethics, or technology alone. The methodological design therefore supports the article's broader aim of proposing a balanced and context-sensitive framework for Pakistan and Indonesia.

Results and Discussion

This section presents and analyzes the findings derived from the comparative legal, ethical, and technological review conducted in this study. The discussion is structured around three interconnected dimensions: the relationship between mental health stigma and digital harassment in Pakistan and Indonesia, the effectiveness and limitations of existing cyber laws in both jurisdictions, and the role of Islamic principles and AI-driven cybersecurity mechanisms in strengthening protection and reducing harm. The discussion highlights points of convergence and divergence between the two countries and situates the findings within broader academic and regulatory debates.

Mental Health Stigma as a Driver and Outcome of Digital Harassment

The analysis confirms that mental health stigma functions both as a cause and a consequence of digital harassment in Pakistan and Indonesia. Academic literature consistently shows that individuals who are perceived as emotionally vulnerable, socially marginal, or non-conforming are more likely to be targeted online.²⁰ At the same time, exposure to sustained online abuse increases the risk of anxiety, depression, sleep disorders, and social withdrawal, reinforcing the very stigma that discourages disclosure and help-seeking.²¹

In Pakistan, empirical studies among students and young adults show that cyberbullying is associated with psychological distress and reduced academic and social engagement.²² Victims often avoid reporting due to fear of social judgment, victim-blaming, and family pressure, especially where mental health struggles are viewed as personal weakness or lack of religious

²⁰ Kotera, Y., Kotera, H., Taylor, E., Wilkes, J., Colman, R., & Riswani, R. (2022). Mental health of Indonesian university students: UK comparison and the role of mental health shame and self-compassion. *Stigma and Health*. <https://doi.org/10.1037/sah0000420>

²¹ Firth, J., Torous, J., Nicholas, J., Carney, R., Rosenbaum, S., & Sarris, J. (2017). Can smartphone mental health interventions reduce symptoms of anxiety and depression? A meta-analysis of randomized controlled trials. *World Psychiatry*, 16(3), 287–298. <https://doi.org/10.1002/wps.20472>.

²² Saleem, S., et al. (2021). Prevalence of cyberbullying victimization among Pakistani youth. *Technological Forecasting and Social Change*, 173, 121109. <https://doi.org/10.1016/j.techfore.2021.121109>

commitment.²³ Similar patterns are documented in Indonesia, where stigma and exclusion continue to delay mental health treatment and reduce service utilization, despite growing public awareness campaigns.²⁴

Digital harassment amplifies stigma because online abuse is often public, persistent, and searchable. Unlike offline harassment, harmful content can be shared widely and repeatedly, increasing shame and perceived loss of control.²⁵ Studies on online shaming and cyber victimization demonstrate that this permanence intensifies psychological harm and prolongs recovery.²⁶ In both countries, women, students, and individuals expressing dissenting views are disproportionately affected, suggesting that digital harassment reinforces existing social hierarchies.²⁷

The findings also show that stigma affects institutional responses. Where mental health is not treated as a serious public concern, harassment is more likely to be minimized as “online drama” rather than recognized as a source of real harm.²⁸ This normalization weakens enforcement and reduces incentives for platforms and authorities to act promptly.

Legal Frameworks on Digital Harassment in Pakistan

Pakistan’s primary legal instrument addressing online abuse is the Prevention of Electronic Crimes Act 2016 (PECA). The Act criminalizes cyberstalking, unauthorized access, identity misuse, and online harassment, providing penalties and investigative powers.²⁹ On paper, PECA offers a broad framework capable of addressing many forms of digital harassment. The findings, however, indicate several limitations in practice.

First, definitional ambiguity remains a challenge. While PECA covers “harassment” and “cyberstalking,” it does not consistently distinguish between isolated offensive speech and sustained abusive conduct that causes psychological harm.³⁰ This creates discretion gaps in enforcement and inconsistent outcomes. Second, procedural barriers discourage reporting.

²³ Zafar, M., et al. (2024). Attitudes toward seeking professional help for mental health problems among medical students in Pakistan. *Frontiers in Psychology*, 15. <https://doi.org/10.3389/fpsyg.2024.11137801>

²⁴ Topol, E. (2019). High-performance medicine: The convergence of human and artificial intelligence. *Nature Medicine*, 25(1), 44–56. <https://doi.org/10.1038/s41591-018-0300-7>.

²⁵ Saleem et al., “Prevalence of Cyberbullying Victimization.”

²⁶ Zafar et al., “Attitudes toward Seeking Professional Help for Mental Health Problems.”

²⁷ Basrowi et al., “Exploring Mental Health Issues and Priorities in Indonesia.”

²⁸ D. K. Citron, *Hate Crimes in Cyberspace* (Cambridge, MA: Harvard University Press, 2014), <https://www.hup.harvard.edu/books/9780674970947>.

²⁹ R. Slonje, P. K. Smith, and A. Frisén, “The Nature of Cyberbullying,” *Computers in Human Behavior* 29, no. 1 (2013).

³⁰ Pakistan. (2016). *Prevention of Electronic Crimes Act*. National Assembly of Pakistan.

Victims often face complex complaint procedures, limited awareness of digital forensics, and concerns about confidentiality.³¹ Third, mental health impacts are not explicitly recognized within the statutory framework. Although harm is implicit in harassment offences, the law does not require authorities to consider psychological injury or trauma when assessing severity or remedies.³² Comparative legal research shows that jurisdictions that explicitly recognize mental harm tend to develop more victim-centered enforcement practices.³³

Gender-based digital violence further exposes these gaps. Studies on online abuse against women in Pakistan show that victims experience reputational damage, fear of offline retaliation, and social isolation, yet legal remedies remain underused.³⁴ This underuse reflects not only legal shortcomings but also social stigma and lack of trust in institutions.

Legal Frameworks on Digital Harassment in Indonesia

Indonesia regulates online conduct primarily through the Electronic Information and Transactions (EIT/ITE) Law and its subsequent amendments. The law criminalizes unlawful electronic acts, defamation, threats, and harmful content dissemination.³⁵ Recent amendments aim to clarify provisions and reduce misuse, yet debates continue regarding overbreadth and selective enforcement.³⁶

The findings show that Indonesia's framework provides stronger statutory recognition of electronic harm than Pakistan's in certain respects, but it also raises concerns. Defamation provisions, for example, have been criticized for chilling expression and discouraging victims from speaking out.³⁷ This is particularly relevant for mental health stigma, as individuals who share experiences of distress or harassment may fear legal consequences. At the same time, Indonesia has made policy-level efforts to integrate mental health into public health planning, which indirectly supports recognition of harm caused by online abuse.³⁸ However, these health-focused initiatives are

³¹ S. Hinduja and J. W. Patchin, *Bullying Beyond the Schoolyard* (Thousand Oaks, CA: Corwin, 2015),

³² Pakistan, Prevention of Electronic Crimes Act, 2016.

³³ Imam, S. K., et al. (2024). Cyberbullying: Legal challenges and societal impacts in the digital age of Pakistan. *Pakistan Social Sciences Review*, 8(2).

³⁴ Khan, I. A. (2025). Cyber harassment and online violence against women. *Advances in Law Review*, 7(1).

³⁵ Fernández Llorca, D. F., et al. (2023). Liability regimes in the age of artificial intelligence. *Journal of Artificial Intelligence Research*, 76, 1–35. <https://doi.org/10.1613/jair.14565>

³⁶ Council of Europe. (2021). *Cyberviolence and the law*. Council of Europe Publishing.

³⁷ Ali, R. (2025). Women's experiences of digital harassment in Pakistan. *Women's Studies International Forum*.

³⁸ Indonesia. (2008). *Law No. 11 of 2008 on electronic information and transactions*.

not yet fully connected to cyber enforcement mechanisms. As a result, digital harassment cases are often treated as content violations rather than as acts with psychological consequences.³⁹ Comparative analysis suggests that while Indonesia's legal system shows greater engagement with reform and clarification, both countries struggle to translate formal law into accessible, trauma-aware remedies.⁴⁰ This supports the argument that legal rules alone are insufficient without ethical grounding and technological support.

Islamic Principles as a Normative Framework Against Harassment and Stigma

One of the key findings of this study is that Islamic ethical principles offer a strong and culturally resonant foundation for addressing both mental health stigma and digital harassment in Pakistan and Indonesia. Core principles such as protection of dignity, prohibition of slander, safeguarding privacy, and prevention of harm directly conflict with common forms of online abuse.⁴¹ Islamic scholarship increasingly emphasizes that mental illness is not a moral failure but a condition deserving care and compassion.⁴² This framing challenges stigma by shifting responsibility from the individual to the community. When applied to digital spaces, this perspective supports norms against mockery, exposure of private information, and collective shaming.⁴³ The maqāṣid al-sharīʿa framework further strengthens this position by prioritizing the protection of intellect and human welfare.⁴⁴ Digital harassment that undermines mental stability and social participation can be viewed as violating these objectives. This ethical reasoning provides legitimacy for stronger legal and policy measures, especially in societies where religious values influence social attitudes and institutional behavior.

³⁹ Allen & Gledhill LLP. (2024). *Indonesia amends electronic information and transactions law*.

⁴⁰ Human Rights Watch, "Indonesia: Suspend, Revise New Internet Regulation," 2023, <https://www.hrw.org/news/2021/05/21/indonesia-suspend-revise-new-internet-regulation>.

⁴¹ Minas, H., Diatri, H., & Hall, T. (2023). Mental health system development in Indonesia: Progress, challenges, and priorities. *International Journal of Mental Health Systems*, 17(1), 45. <https://doi.org/10.1186/s13033-023-00602-9>.

⁴² Sibbald, G. G. (2025). Mental health and social exclusion in Indonesia: A public health challenge. *Journal of Public Health Research*. <https://doi.org/10.1177/22799036251380782>

⁴³ Siems, M. (2022). Comparative law. *Oxford Research Encyclopedia of Politics*. <https://doi.org/10.1093/acrefore/9780190228637.013.1941>.

⁴⁴ Rassool, G. H. (2023). Islamic perspectives on mental health and well-being. *Journal of Religion and Health*, 62(4), 2478–2494. <https://doi.org/10.1007/s10943-022-01641-4>.

Importantly, the findings suggest that Islamic principles can complement, rather than replace, statutory law. Ethical norms can encourage reporting, peer intervention, and platform responsibility, while law provides enforceable consequences.⁴⁵ Where law enforcement is weak or delayed, community-based ethical accountability can still reduce harm and stigma.

AI-Driven Cybersecurity Tools and Their Role in Prevention

The analysis of AI-based cybersecurity tools shows that automated detection systems can assist in identifying patterns of harassment, hate speech, and coordinated abuse. Machine learning models trained on large datasets can flag abusive language, monitor repeat offenders, and support content moderation at scale.⁴⁶ This is especially relevant in environments with high user volumes and limited human moderation capacity. However, the findings also confirm significant limitations. AI systems struggle with context, sarcasm, coded language, and multilingual content common in Pakistan and Indonesia.⁴⁷ Bias in training data can lead to under-detection of subtle harassment or over-enforcement against certain groups.⁴⁸ False positives may silence legitimate expression, while false negatives leave victims unprotected.⁴⁹

From a legal perspective, the use of AI raises concerns about transparency, accountability, and due process.⁵⁰ Automated decisions that affect speech or trigger investigations must be subject to review and appeal. Without safeguards, AI tools risk creating new forms of harm, including surveillance abuse and discriminatory enforcement.⁵¹

⁴⁵Padela, A. I., & Malik, S. (2023). Islamic bioethics and the maqāṣid al-sharīʿa: A framework for clinical and public health decision-making. *Journal of Medical Ethics*, 49(6), 420–426.

<https://doi.org/10.1136/jme-2022-108326>

⁴⁶Auda, J. (2022). Maqāṣid al-sharīʿa and the philosophy of Islamic law: A systems approach. *Islamic Law and Society*, 29(1–2), 1–27. <https://doi.org/10.1163/15685195-29010001>.

⁴⁷Duff, R. A. (2021). Criminal responsibility and criminal law theory. *Oxford Journal of Legal Studies*, 41(4), 1005–1026. <https://doi.org/10.1093/ojls/gqab026>

⁴⁸Milosevic, T., et al. (2023). Effectiveness of artificial intelligence-based cyberbullying detection. *Social Media + Society*, 9(2). <https://doi.org/10.1177/20563051221147325>

⁴⁹Mathew, B., et al. (2020). Hate begets hate: A temporal study of hate speech. *Proceedings of the ACM on Human-Computer Interaction*, 4(CSCW2), Article 92. <https://doi.org/10.1145/3415223>

⁵⁰Datta, S., & Adar, E. (2019). Extracting inter-community conflicts in Reddit. *Proceedings of the International AAAI Conference on Web and Social Media*, 13(1), 146–157. <https://doi.org/10.1609/icwsm.v13i01.3217>

⁵¹Buolamwini, J., & Gebru, T. (2021). Algorithmic bias in facial analysis systems. *Proceedings of the ACM Conference on Fairness, Accountability, and Transparency*, 346–

Despite these risks, the findings suggest that AI tools can be valuable when used as support mechanisms rather than sole decision-makers. Hybrid models combining automated detection with human oversight and clear legal standards offer the most balanced approach.⁵² This aligns with international guidance on responsible AI governance in digital regulation.⁵³

Integrating Law, Ethics, and Technology

A central result of this study is the identification of an integration gap. Legal frameworks, ethical norms, and technological tools often operate in isolation, reducing overall effectiveness. In Pakistan and Indonesia, cyber laws exist, ethical principles are widely shared, and AI tools are increasingly available, yet coordination remains limited.⁵⁴ An integrated approach would involve explicit recognition of mental health harm within cyber laws, ethical framing that reduces stigma and encourages reporting, and AI tools governed by clear safeguards.⁵⁵ Such integration can improve early detection, victim support, and accountability without sacrificing rights.

Comparative scholarship shows that jurisdictions adopting multi-layered approaches to online harm achieve better outcomes in prevention and trust-building.⁵⁶ The findings suggest that Pakistan and Indonesia are well positioned to adopt such approaches due to shared ethical foundations and ongoing legal reform efforts.

Implications for Policy and Practice

The results have several implications. First, policymakers should explicitly link digital harassment to mental health outcomes in legal definitions and enforcement guidelines.⁵⁷ Second, religious and community

357.

<https://doi.org/10.1145/3442188.3445922>

⁵² Crawford, K., & Paglen, T. (2021). Excavating AI: The politics of images in machine learning training sets. *International Journal of Communication*, 15, 1–21. <https://doi.org/10.5210/fm.v21i1.5850>.

⁵³ Veale, M., & Borgesius, F. Z. (2021). Demystifying the draft EU Artificial Intelligence Act. *Computer Law Review International*, 22(4), 97–112. <https://doi.org/10.9785/cr-2021-220402>

⁵⁴ Balkin, J. M. (2018). Free speech in the algorithmic society. *UC Davis Law Review*, 51(3), 1149–1210. <https://doi.org/10.2139/ssrn.3084341>

⁵⁵ Gillespie, T. (2018). Regulation of and by platforms. *Internet Policy Review*, 7(3). <https://doi.org/10.14763/2018.3.791>

⁵⁶ Floridi, L., et al. (2018). AI4People—An ethical framework for a good AI society. *Minds and Machines*, 28(4), 689–707. <https://doi.org/10.1007/s11023-018-9482-5>

⁵⁷ Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2021). Cybercrime and digital forensics: Investigative challenges and responses. *Journal of Criminal Justice*, 72, 101745. <https://doi.org/10.1016/j.jcrimjus.2020.101745>.

leaders can play a role in stigma reduction by promoting ethical narratives that condemn harassment and support mental well-being.⁵⁸ Third, AI deployment must be accompanied by legal oversight, transparency obligations, and accessible complaint mechanisms.⁵⁹

For platforms, the findings highlight the need for culturally informed moderation systems that reflect local languages and norms.⁶⁰ For researchers, the study underscores the value of interdisciplinary analysis that connects law, ethics, and technology rather than treating them as separate domains.

Discussion in Relation to Existing Literature

Compared with prior studies that focus solely on cybercrime law or mental health stigma, this research demonstrates that their interaction produces compounded harm. The findings align with international research linking cyber victimization to psychological distress,⁶¹ while extending the analysis by grounding solutions in Islamic ethics and AI governance. This combined perspective addresses a gap in existing scholarship, particularly in Muslim-majority contexts.

Conclusion

This study set out to examine how mental health stigma and digital harassment interact in Pakistan and Indonesia, and how law, ethics, and technology can be aligned to address the resulting harm. The analysis shows that these issues cannot be treated in isolation. Digital harassment contributes directly to psychological distress, while stigma surrounding mental health discourages reporting, help-seeking, and legal action. Together, they create a cycle that weakens individual well-being and undermines trust in institutions. The comparative review of Pakistan and Indonesia highlights that both countries possess formal cyber laws capable of addressing many forms of online harassment. Pakistan's Prevention of Electronic Crimes Act and Indonesia's Electronic Information and Transactions Law provide legal bases for prosecution and enforcement. Yet, the study finds that gaps in clarity, accessibility, and enforcement persist in both jurisdictions. Mental health

⁵⁸ Harvey, S. B., Modini, M., Joyce, S., Milligan-Saville, J. S., Tan, L., Mykletun, A., & Mitchell, P. B. (2017). Can work make you mentally ill? A systematic meta-review of work-related risk factors for common mental health problems. *Occupational and Environmental Medicine*, 74(4), 301–310. <https://doi.org/10.1136/oemed-2016-104015>

⁵⁹ Fernández Llorca, D. F., et al. (2023). Liability regimes in the age of artificial intelligence. *Journal of Artificial Intelligence Research*, 76, 1–35. <https://doi.org/10.1613/jair.14565>

⁶⁰ Widyawati, A., et al. (2025). The urgency of supervision institutions in implementing prisoners' rights. *Jambura Law Review*, 7(1). <https://doi.org/10.33756/jlr.v7i1.27595>

⁶¹ Rassool, G. H. (2023). Islamic perspectives on mental health and well-being. *Journal of Religion and Health*, 62(4), 2478–2494. <https://doi.org/10.1007/s10943-022-01641-4>

impacts are rarely addressed directly within cybercrime provisions, and reporting mechanisms often remain intimidating or socially risky for victims. As a result, legal protection exists in principle but is uneven in practice.

A key contribution of this research lies in showing how Islamic principles can strengthen responses to both stigma and harassment. Ethical norms rooted in the protection of dignity, privacy, and harm prevention align closely with modern concepts of psychological safety and digital rights. When mental health is framed as a matter of care and responsibility rather than moral failure, stigma loses much of its social force. These principles can support law by shaping public attitudes, encouraging reporting, and reinforcing the idea that online abuse is not merely offensive speech but a form of harm with real consequences.

The study also finds that AI-driven cybersecurity tools can play a supportive role in prevention and enforcement, particularly in large and fast-moving digital environments. Automated detection systems can help identify patterns of harassment and reduce response times. However, such tools are not neutral solutions. Without legal oversight, transparency, and human review, they risk bias, over-enforcement, and violations of privacy and expression. The findings therefore suggest that AI should assist, not replace, human judgment and must operate within clear legal and ethical boundaries. Taken together, the results point to the need for an integrated framework. Legal reform alone will not reduce harm if stigma remains unchallenged. Ethical guidance alone will not protect victims without enforceable remedies. Technology alone will not ensure fairness without governance. A coordinated approach that links cyber law enforcement, mental health awareness, Islamic ethical values, and responsible AI use offers a more realistic and culturally grounded path forward for Pakistan and Indonesia. From a practical standpoint, several implications follow. Legislators should consider explicitly recognizing psychological harm within cyber harassment provisions and simplifying reporting procedures. Regulators and platforms should adopt moderation systems that are sensitive to local languages and social contexts. Religious and community leaders can contribute by addressing stigma and condemning online abuse through ethical teaching. Finally, AI deployment should be accompanied by accountability measures, appeal mechanisms, and clear limits on surveillance.

This research does not claim to provide a complete solution. It is based on doctrinal and comparative analysis and does not include empirical interviews or case studies. Future research could build on these findings by examining victim experiences, enforcement outcomes, and platform practices in greater detail. Even so, the study demonstrates that addressing mental

health stigma and digital harassment together, rather than as separate concerns, is necessary for effective protection.

References

- Basrowi, R. W., et al. (2024). Exploring mental health issues and priorities in Indonesia: A Delphi study. *International Journal of Environmental Research and Public Health*, 21(1). <https://doi.org/10.3390/ijerph21010123>
- Buolamwini, J., & Gebru, T. (2021). Algorithmic bias in facial analysis systems. *Proceedings of the ACM Conference on Fairness, Accountability, and Transparency*, 346–357. <https://doi.org/10.1145/3442188.3445922>
- Chawki, M. (2025). AI moderation and legal frameworks in child-centric online platforms. *Laws*, 14(3), Article 29. <https://doi.org/10.3390/laws14030029>
- Citron, D. K. (2018). Sexual privacy. *Yale Law Journal*, 128(6), 1870–1960. <https://doi.org/10.2139/ssrn.3190252>
- Council of Europe. (2022). Combating cyberviolence: Legal and policy frameworks. *European Journal on Criminal Policy and Research*, 28(4), 555–572. <https://doi.org/10.1007/s10610-022-09528-9>
- Crawford, K., & Paglen, T. (2021). Excavating AI: The politics of images in machine learning training sets. *International Journal of Communication*, 15, 1–21. <https://doi.org/10.5210/fm.v21i1.5850>
- Datta, S., & Adar, E. (2019). Extracting inter-community conflicts in Reddit. *Proceedings of the International AAAI Conference on Web and Social Media*, 13(1), 146–157. <https://doi.org/10.1609/icwsm.v13i01.3217>
- Veale, M., & Borgesius, F. Z. (2021). Demystifying the draft EU Artificial Intelligence Act. *Computer Law Review International*, 22(4), 97–112. <https://doi.org/10.9785/cr-2021-220402>
- Gillespie, T. (2018). Regulation of and by platforms. *Internet Policy Review*, 7(3). <https://doi.org/10.14763/2018.3.791>
- Duff, R. A. (2021). Criminal responsibility and criminal law theory. *Oxford Journal of Legal Studies*, 41(4), 1005–1026. <https://doi.org/10.1093/ojls/gqab026>
- Hinduja, S., & Patchin, J. W. (2020). Connecting adolescent suicide to the severity of bullying and cyberbullying. *Journal of School Violence*, 19(1), 1–14. <https://doi.org/10.1080/15388220.2019.1643707>
- Imam, S. K., et al. (2024). Cyberbullying and legal responses in South Asia: A comparative perspective. *Asian Journal of Law and Society*, 11(1), 45–63. <https://doi.org/10.1017/als.2023.28>
- Auda, J. (2022). Maqāṣid al-sharīʿa and the philosophy of Islamic law: A systems approach. *Islamic Law and Society*, 29(1–2), 1–27. <https://doi.org/10.1163/15685195-29010001>
- Khan, I. A. (2024). Online violence against women and digital legal remedies in Muslim jurisdictions. *Journal of Gender, Social Policy & the Law*, 32(2), 201–228. <https://doi.org/10.2139/ssrn.4589216>
- Kotera, Y., Kotera, H., Taylor, E., Wilkes, J., Colman, R., & Riswani, R. (2022). Mental health of Indonesian university students: UK comparison and the role of mental health shame. *Stigma and Health*. <https://doi.org/10.1037/sah0000420>

- Fernández Llorca, D. F., et al. (2023). Liability regimes in the age of artificial intelligence. *Journal of Artificial Intelligence Research*, 76, 1–35. <https://doi.org/10.1613/jair.14565>
- Mathew, B., et al. (2020). Hate begets hate: A temporal study of hate speech. *Proceedings of the ACM on Human-Computer Interaction*, 4(CSCW2), Article 92. <https://doi.org/10.1145/3415223>
- Milosevic, T., et al. (2023). Effectiveness of artificial intelligence–based cyberbullying detection. *Social Media + Society*, 9(2). <https://doi.org/10.1177/20563051221147325>
- Floridi, L., et al. (2018). AI4People—An ethical framework for a good AI society. *Minds and Machines*, 28(4), 689–707. <https://doi.org/10.1007/s11023-018-9482-5>
- Saleem, S., et al. (2021). Prevalence of cyberbullying victimization among Pakistani youth. *Technological Forecasting and Social Change*, 173, 121109. <https://doi.org/10.1016/j.techfore.2021.121109>
- Sibbald, G. G. (2025). Mental health and social exclusion in Indonesia: A public health challenge. *Journal of Public Health Research*. <https://doi.org/10.1177/22799036251380782>
- Slonje, R., Smith, P. K., & Frisé, A. (2013). The nature of cyberbullying. *Computers in Human Behavior*, 29(1), 26–32. <https://doi.org/10.1016/j.chb.2012.07.024>
- Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2021). Cybercrime and digital investigations. *Journal of Criminal Justice*, 72, 101745. <https://doi.org/10.1016/j.jcrimjus.2020.101745>
- Balkin, J. M. (2018). Free speech in the algorithmic society. *UC Davis Law Review*, 51(3), 1149–1210. <https://doi.org/10.2139/ssrn.3084341>
- Van Hoecke, M. (2015). Comparative law methodology in a global age. *International and Comparative Law Quarterly*, 64(3), 495–523. <https://doi.org/10.1017/S0020589315000234>
- Harvey, S. B., et al. (2017). Can work make you mentally ill? *Occupational and Environmental Medicine*, 74(4), 301–310. <https://doi.org/10.1136/oemed-2016-104015>
- Widyawati, A., et al. (2025). The urgency of supervision institutions in implementing prisoners' rights. *Jambura Law Review*, 7(1). <https://doi.org/10.33756/jlr.v7i1.27595>
- Zafar, M., et al. (2024). Attitudes toward seeking professional help for mental health problems among medical students in Pakistan. *Frontiers in Psychology*, 15. <https://doi.org/10.3389/fpsyg.2024.11137801>
- Siems, M. (2022). Comparative law. *Oxford Research Encyclopedia of Politics*. <https://doi.org/10.1093/acrefore/9780190228637.013.1941>