ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.04 (2025)

ARTIFICIAL INTELLIGENCE, HUMAN RIGHTS AND CYBER LAW: EMERGING LEGAL CHALLENGES FOR PRIVACY, EQUALITY AND FREEDOM OF EXPRESSION IN PAKISTAN

Amina Bari*
LLM, PU, Deputy Director (Legal) / Program Manager LMS/Punjab E-Law Manager, Directorate of Monitoring and Evaluation, Government of the Punjab, Law and Parliamentary Affairs Department
Correspondence Email ID: aminabari.dd@gmail.com

Abstract
This research paper examined emerging human-rights challenges associated with artificial intelligence in Pakistan, focusing on privacy, equality, and freedom of expression. It developed a quantitative framework linking perceived algorithmic opacity and perceived adequacy of legal safeguards with three distinct categories of perceived rights risk. The legal context distinguished constitutional protections, cybercrime legislation, the approved National Artificial Intelligence Policy 2025, and the draft Personal Data Protection Bill 2023. A cross-sectional analytical design was demonstrated using 300 simulated records representing hypothetical legal professionals, technology professionals, journalists, and digital-rights practitioners. Twenty-five items measured five constructs through five-point response scales. Descriptive statistics, internal consistency analysis, Pearson correlations, and three multiple regression models were calculated. Perceived algorithmic opacity was positively associated with privacy risk, equality risk, and freedom-of-expression risk, with standardized coefficients of .343, .258, and .372, respectively. Perceived adequacy of legal safeguards showed negative associations with these outcomes, with corresponding coefficients of −.330, −.293, and −.216. The models explained 19.0%, 12.9%, and 15.9% of the variance in the respective simulated outcomes. These relationships reflected the constructed dataset and did not establish actual rights violations or protective effects in Pakistan. The research paper concluded that separate measurement of rights risks provided a useful foundation for empirical investigation. It recommended research combining professional assessments, affected users' experiences, technical audits, and legal analysis. Its contribution remained methodological and conceptual rather than evidence of real-world institutional performance.

Keywords: *Artificial intelligence; human rights; cyber law; privacy; algorithmic discrimination; freedom of expression; Pakistan.*

1. Introduction

Artificial intelligence raised legal questions because automated systems could influence how personal information was processed, how individuals were classified, and how information circulated online. These functions connected technological development with rights protection. The United Nations High Commissioner for Human Rights examined AI-related privacy concerns and their implications for other freedoms, demonstrating why the consequences of automated processing required assessment beyond technical performance alone. The present research paper approached these concerns through privacy, equality, and freedom of expression as separate analytical domains. (OHCHR, 2021)

Pakistan's constitutional framework provided relevant starting points. Article 14 addressed human dignity and, subject to law, privacy of the home; Article 19 protected speech and expression subject to specified reasonable restrictions imposed by law; and Article 25 addressed equality before law and equal protection. These provisions supplied constitutional reference points, although their application to a particular AI system required contextual legal interpretation. They were not treated as a detailed statutory code governing every form of automated decision-making. (National Assembly of Pakistan, 2018)

The policy and legislative context also required careful differentiation. The Ministry of Information Technology and Telecommunication listed the National Artificial Intelligence Policy as approved on 31 July 2025. The National Assembly separately recorded the Prevention of Electronic Crimes (Amendment) Act, 2025, as Act No. II of 2025. Meanwhile,

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.04 (2025)

the ministry's legislation catalogue identified the May 2023 Personal Data Protection Bill as a draft. Consequently, an approved policy, an enacted amendment, and a draft bill were not treated as interchangeable sources of enforceable obligations. (MoITT, 2025; National Assembly of Pakistan, 2025; MoITT, 2023)

Against this background, the research paper developed an illustrative framework examining perceived algorithmic opacity and perceived adequacy of legal safeguards. Algorithmic opacity referred to difficulty understanding the basis of automated outputs or decisions. Legal-safeguard adequacy referred to assessments of available oversight, complaint handling, and corrective procedures. The framework related these perceptions to separate rights-risk outcomes, drawing on international attention to transparency, accountability, and human oversight. (UNESCO, 2021)

2. Rationale of the Study

The rationale concerned the need to move from broad concerns about AI towards clearly specified research questions. Privacy risks involved personal-data processing, equality risks concerned differential treatment, and expression risks involved participation in the information environment. Combining these issues into a single measure could have concealed meaningful differences. The study therefore adopted separate outcomes while recognising that the underlying technologies and institutional practices could connect them. This approach reflected international discussion of AI's implications across multiple rights. (OHCHR, 2021; Kaye, 2018)

A second rationale concerned the relationship between technical transparency and institutional protection. A system could have been difficult to explain even where complaint procedures existed, while accessible explanations alone did not guarantee effective remedies. The framework consequently treated opacity and safeguard adequacy as distinct predictors. This analytical choice was informed by the NIST framework's treatment of AI risk management as an organisational responsibility extending across development, deployment, and evaluation. (NIST, 2023)

3. Statement of the Problem

The legal challenge concerned how AI-related decisions and information practices could be evaluated against human-rights protections in Pakistan. Policy approval and cybercrime legislation did not, by themselves, establish whether individuals could understand automated decisions, contest discriminatory outcomes, or obtain effective remedies. International evidence demonstrated reasons to investigate these questions, but it did not establish their prevalence in Pakistani institutions. The specific research problem therefore concerned the relationships between perceived opacity, perceived safeguard adequacy, and perceived risks to privacy, equality, and expression. The research paper addressed this measurement problem through a simulated quantitative demonstration. (UNESCO, 2021; NIST, 2023)

4. Research Objectives

1. To examine the associations between perceived algorithmic opacity and perceived risks to privacy, equality, and freedom of expression in the selected Pakistani professional context.
2. To assess the associations between perceived adequacy of legal safeguards and the same three perceived rights-risk outcomes.

5. Research Questions

1. How was perceived algorithmic opacity associated with perceived privacy risk, equality risk, and freedom-of-expression risk?
2. How was perceived adequacy of legal safeguards associated with perceived privacy risk, equality risk, and freedom-of-expression risk?

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.04 (2025)

6. Significance of the Study

The study provided researchers with an analytical framework for distinguishing technical concerns, institutional assessments, and perceived human-rights risks associated with artificial intelligence in Pakistan. By examining algorithmic opacity and legal-safeguard adequacy separately, it clarified how different dimensions of AI governance could be investigated quantitatively. Privacy, equality, and freedom of expression were treated as distinct outcomes rather than combined into a single measure. This separation supported clearer interpretation and identified relationships requiring empirical investigation. The framework's significance therefore concerned the organisation of research questions and measurement rather than confirmation of actual institutional performance or rights violations (NIST, 2023).

For legal scholars, the study identified questions requiring examination through applicable legislation, constitutional protections, and documented circumstances. It highlighted the importance of distinguishing perceived risk from demonstrated harm and legally established liability. For technology professionals, it emphasized understandable explanations, review procedures, and clearly assigned responsibility for consequential automated decisions. These considerations provided starting points for evaluating how technical systems interacted with institutional practices. The study also encouraged collaboration between legal and technical researchers because neither professional perceptions nor system-performance measures alone could resolve every question concerning accountability and human-rights protection in particular deployment contexts (UNESCO, 2021).

For policymakers, the study suggested categories of evidence that could inform future assessments of AI governance, including user experiences, complaint outcomes, institutional procedures, and technical evaluations. Such evidence could help distinguish formal commitments from their practical implementation. However, the study's significance remained methodological because synthetic responses did not establish the experiences of actual individuals or the effectiveness of Pakistani institutions. Its findings therefore supplied no independent basis for claims about national conditions. Instead, the framework offered a foundation for subsequent empirical research using validated instruments, justified sampling, and observed evidence to examine the relationships between AI practices, safeguards, and perceived rights risks (Creswell & Creswell, 2018).

7. Literature Review

7.1 Artificial Intelligence and Privacy

The OHCHR's 2021 report examined how AI affected privacy through data-intensive processing and related practices. It connected privacy interference with possible consequences for other human rights. This perspective demonstrated why evaluation required attention to the purposes and consequences of processing. The present study accordingly distinguished perceived privacy risk from general dissatisfaction with technology. However, its survey framework did not determine whether any particular processing activity had violated Pakistani law. (OHCHR, 2021)

7.2 Algorithmic Bias and Equality

Buolamwini and Gebru (2018) documented substantial differences in the performance of commercial gender-classification systems across demographic groups. Their findings demonstrated that aggregate accuracy could conceal unequal error distributions. The study concerned particular systems and did not establish equivalent disparities in Pakistan. Nevertheless, it provided an empirical reason to examine differential outcomes rather than assume technical neutrality. The present framework therefore treated equality risk as distinct from privacy concerns. (Buolamwini & Gebru, 2018)

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.04 (2025)

7.3 Artificial Intelligence and Freedom of Expression

Kaye's 2018 report examined AI technologies and their implications for the information environment. This work supported examining how automated systems influenced the availability and circulation of expression. It also indicated that technological interventions required consideration of human-rights responsibilities. The present study focused on perceived risks associated with automated restriction and reduced visibility of legitimate expression. These assessments were not treated as proof that a particular moderation decision had been unlawful. (Kaye, 2018)

7.4 Cyber Law and AI Governance in Pakistan

Pakistan's reviewed governance materials included legislation, policy, and a draft data-protection proposal. The 2025 PECA amendment was recorded as an enacted statute, while the National AI Policy was identified as an approved policy. The ministry's catalogue separately labelled the 2023 Personal Data Protection Bill as a draft. These distinctions prevented proposed provisions from being presented as established legal rights or duties. The study's contribution concerned an analytical framework for investigating perceived protection, rather than a claim that no Pakistani AI research or relevant law existed. (National Assembly of Pakistan, 2025; MoITT, 2025; MoITT, 2023)

8. Methodology

8.1 Research Methodology

The research paper adopted a quantitative, cross-sectional analytical design with a deductive orientation. Two predictor constructs were specified in relation to three separate outcomes. Legal and policy sources supplied contextual interpretation; their inclusion did not constitute qualitative participant research or make the study mixed methods. The numerical component used simulated individual-level responses. Accordingly, neither causal relationships nor changes over time were inferred. (Creswell & Creswell, 2018)

8.2 Population

The intended population comprised legal professionals, AI and information-technology professionals, journalists, and digital-rights practitioners in Lahore, Karachi, Islamabad, and Peshawar. Eligibility was defined as adulthood, at least two years of relevant professional experience, and familiarity with automated systems or digital-rights issues. Each individual was assigned one primary professional category. The intended population excluded persons without relevant exposure, and no verified population register was obtained. These boundaries limited the proposed study to selected professional perspectives. (Creswell & Creswell, 2018)

8.3 Sampling and Sample Size

A purposive quota framework was specified for the demonstration. The hypothetical sample comprised 300 records, divided equally across four professional categories and four cities. The number was selected for analytical illustration rather than presented as a power-based minimum or nationally representative sample. An actual study required advance justification based on its intended effects, predictors, subgroup analyses, and expected nonresponse. Sample size alone did not compensate for nonprobability selection. (Lakens, 2022)

8.4 Research Instrument

The illustrative questionnaire comprised demographic questions and 25 researcher-developed items distributed across five constructs. Each item used a five-point response format ranging from strongly disagree to strongly agree. Algorithmic opacity addressed the difficulty of understanding decision criteria, data inputs, and automated outputs. Safeguard adequacy addressed perceived access to oversight, complaints, review, and correction. The

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.04 (2025)

framework drew conceptually on AI-governance guidance, but no previously validated questionnaire was claimed. (NIST, 2023)

Privacy-risk items addressed concerns about excessive collection, secondary use, sensitive inference, and unwanted disclosure. Equality-risk items addressed concerns about unfair exclusion and differential treatment. Expression-risk items addressed concerns about erroneous restriction or suppression of legitimate content and participation. These outcomes measured perceived risks rather than personally experienced violations. Separating them followed the broader human-rights orientation of international AI guidance. (UNESCO, 2021)

8.5 Data Collection

No human-participant data were collected. Synthetic responses were generated using correlated latent variables, item-specific random variation, and rounding to the five-point scale. The simulation deliberately incorporated positive relationships between opacity and rights risks, together with negative relationships between safeguard adequacy and those risks. All 300 generated records contained complete item responses. Consequently, no response rate, fieldwork period, consent process, or institutional approval was reported as completed. (Creswell & Creswell, 2018)

8.6 Data Analysis Techniques

Frequencies and percentages described the hypothetical demographic composition. Means, standard deviations, and Cronbach's alpha described the simulated scales, while Pearson correlations examined pairwise associations. Three ordinary least squares regressions estimated associations with privacy, equality, and expression risks separately. Each model contained opacity and safeguard adequacy as predictors, and calculations were performed in Python. Confidence intervals and significance tests described the simulated model outputs rather than population evidence. (Field, 2018)

Here, AOAO represented perceived algorithmic opacity, LSLS represented perceived legal-safeguard adequacy, and YkY_k represented each rights-risk outcome. No interaction term was included, so the study did not test whether safeguards moderated the association between opacity and risk. No demographic or institutional controls were included either. Multicollinearity was assessed, while measurement validation and fuller diagnostics remained requirements for an empirical application. (Field, 2018)

9. Data Analysis

Table 1 *Hypothetical demographic characteristics, N = 300*

Characteristic	Category	Frequency	Percentage
Gender	Male	180	60.0
	Female	120	40.0
Age	25–34 years	120	40.0
	35–44 years	105	35.0
	45 years and above	75	25.0
Primary profession	Legal professional	75	25.0
	AI/IT professional	75	25.0
	Journalist	75	25.0
	Digital-rights practitioner	75	25.0
Relevant experience	2–5 years	120	40.0

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.04 (2025)

Characteristic	Category	Frequency	Percentage
	6–10 years	105	35.0
	More than 10 years	75	25.0
City	Lahore	75	25.0
	Karachi	75	25.0
	Islamabad	75	25.0
	Peshawar	75	25.0

Table 1 described the predetermined demographic profile. Male records represented 60.0%, while female records represented 40.0%. The largest age group was 25–34 years, comprising 40.0%. Each professional category and city received an equal allocation of 25.0%. These allocations illustrated quota reporting and did not establish population representativeness. (Creswell & Creswell, 2018)

Table 2 *Descriptive statistics for simulated constructs*

Construct	Items	Mean	SD	Cronbach's α
Algorithmic opacity	5	3.509	0.655	.811
Legal-safeguard adequacy	5	2.871	0.728	.834
Privacy risk	5	3.651	0.626	.797
Equality risk	5	3.487	0.675	.831
Freedom-of-expression risk	5	3.613	0.667	.834

Note. N = 300. Possible scores ranged from 1 to 5. Higher safeguard scores represented stronger perceived protection; higher risk scores represented greater perceived risk.

Table 2 showed that privacy risk had the highest simulated mean of 3.651. Freedom-of-expression risk and equality risk recorded means of 3.613 and 3.487, respectively. Legal-safeguard adequacy had a mean below the neutral midpoint, at 2.871. Cronbach's alpha ranged from .797 to .834 across the five scales. These values described the generated responses and did not establish measurement validity or actual weaknesses in Pakistani legal protection. (Field, 2018)

Table 3 *Selected Pearson correlations in the simulated dataset*

Predictor	Outcome	r	p
Algorithmic opacity	Privacy risk	.290	< .001
Algorithmic opacity	Equality risk	.212	< .001
Algorithmic opacity	Expression risk	.337	< .001
Legal-safeguard adequacy	Privacy risk	−.276	< .001
Legal-safeguard adequacy	Equality risk	−.252	< .001
Legal-safeguard adequacy	Expression risk	−.156	.007

Note. N = 300. The correlation between the two predictors was .159.

Table 3 indicated positive correlations between opacity and all three risk outcomes. The largest of these correlations concerned expression risk, at .337. Safeguard adequacy correlated negatively with privacy, equality, and expression risks. Its weakest relationship concerned expression risk, at −.156. These associations reflected the simulation and did not show that opacity caused harm or that safeguards prevented actual violations. (Creswell & Creswell, 2018)

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.04 (2025)

Table 4 *Simulated regressions predicting perceived rights risks*

Outcome	Predictor	B	SE	β	t	p	95% CI for B
Privacy risk	Constant	3.318	.205	—	16.154	< .001	[2.913, 3.722]
	Opacity	.327	.051	.343	6.479	< .001	[.228, .427]
	Safeguards	−.284	.045	−.330	−6.244	< .001	[−.374, −.195]
Equality risk	Constant	3.333	.230	—	14.510	< .001	[2.881, 3.785]
	Opacity	.266	.057	.258	4.710	< .001	[.155, .377]
	Safeguards	−.272	.051	−.293	−5.342	< .001	[−.372, −.172]
Expression risk	Constant	2.853	.223	—	12.792	< .001	[2.414, 3.292]
	Opacity	.378	.055	.372	6.893	< .001	[.270, .486]
	Safeguards	−.197	.049	−.216	−3.997	< .001	[−.295, −.100]

Note. Each model used N = 300. B = unstandardised coefficient; β = standardised coefficient.

Table 4 showed positive opacity coefficients in all three models after accounting for safeguard adequacy. Its standardised coefficients were .343 for privacy risk, .258 for equality risk, and .372 for expression risk. Safeguard adequacy showed corresponding negative coefficients of −.330, −.293, and −.216. All six predictor associations achieved significance below .001 within the simulation. Differences in coefficient sizes were not formally tested and therefore did not establish that one right was more vulnerable than another. (Field, 2018)

Table 5 *Fit statistics for the simulated regression models*

Outcome	R^2	Adjusted R^2	F(2, 297)	p
Privacy risk	.190	.185	34.931	< .001
Equality risk	.129	.123	21.908	< .001
Expression risk	.159	.153	28.074	< .001

Note. VIF = 1.026 for both predictors in each model.

Table 5 showed that the predictors accounted for 19.0% of simulated privacy-risk variance. The corresponding proportions were 12.9% for equality risk and 15.9% for expression risk. The VIF indicated little linear overlap between the predictors. Substantial outcome variance remained unexplained in every model. These percentages did not represent rates of rights violations or reductions in harm attributable to legal protection. (Field, 2018)

10. Findings

The first research objective examined the relationship between perceived algorithmic opacity and perceived risks to privacy, equality, and freedom of expression. Positive regression coefficients appeared across all three outcomes after accounting for perceived legal-safeguard adequacy. The standardised coefficients were .343 for privacy risk, .258 for equality risk, and .372 for expression risk. These results indicated that higher opacity scores accompanied higher risk scores within the simulated dataset. However, the relationships had been deliberately incorporated into data generation and therefore did not independently confirm theoretical expectations or establish harmful practices among Pakistani organisations. Their significance remained illustrative (Creswell & Creswell, 2018).

The second objective assessed whether perceived adequacy of legal safeguards was associated with the three rights-risk outcomes. Negative coefficients showed that stronger safeguard assessments accompanied lower simulated risk scores after accounting for opacity. The standardised coefficients were −.330 for privacy risk, −.293 for equality risk, and −.216 for expression risk. All six predictor associations achieved statistical significance below .001 within the demonstration. Nevertheless, statistical significance did not establish that any

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.04 (2025)

particular oversight mechanism, complaint procedure, or legal remedy had prevented harm. Evaluating protective effects required direct evidence concerning implementation, accessibility, and experiences of affected individuals in relevant settings (UNESCO, 2021).

Together, the two predictors accounted for 19.0% of simulated privacy-risk variance, 12.9% of equality-risk variance, and 15.9% of expression-risk variance. These percentages described model fit rather than the prevalence of rights violations or reductions in harm. Substantial variance remained unexplained, while differences between coefficients were not formally tested. The findings therefore identified a framework for subsequent empirical investigation rather than conclusions about national institutional performance. Future testing required validated instruments, appropriately selected participants, documented organisational practices, and user evidence. Such research could examine whether perceived accountability corresponded with accessible remedies and demonstrable rights protection in actual deployments (Creswell & Creswell, 2018).

11. Discussion

The analysis demonstrated the value of distinguishing three rights-risk outcomes. Privacy concerned processing of personal information, equality concerned differential treatment, and expression concerned participation in the information environment. Their separation prevented one favourable or unfavourable overall score from concealing differences between domains. Nevertheless, the models did not determine whether respondents understood those distinctions in practice because no actual questionnaire administration occurred. Empirical research required both measurement validation and context-specific evidence. (Creswell & Creswell, 2018)

The equality component was conceptually supported by evidence that some tested systems had performed unevenly across demographic groups. Buolamwini and Gebru's research demonstrated the importance of disaggregated evaluation, but it did not establish comparable performance in Pakistani deployments. A local investigation required appropriate datasets, documented system functions, and clearly specified comparison groups. Moreover, a technical performance disparity and a legal finding of discrimination were related but distinct questions. The simulated perception scale answered neither conclusively. (Buolamwini & Gebru, 2018)

The expression component required attention to automated decisions within the information environment. A perceived risk could have arisen from uncertainty about a system, dissatisfaction with a decision, or an actual restriction. These possibilities required different evidence. A stronger study could have examined documented moderation decisions and available review procedures alongside participant accounts. Kaye's report supplied a human-rights context for such investigation rather than proof of particular Pakistani violations. (Kaye, 2018)

The legal context also limited interpretation. Approval of the National AI Policy established a policy development, while enactment of the PECA amendment established a legislative development. Neither fact alone demonstrated how institutions implemented protections or how individuals experienced them. Likewise, draft data-protection provisions could not be assumed to supply enforceable remedies. The research paper therefore treated implementation and accessibility as empirical questions rather than consequences automatically established by formal documents. (MoITT, 2025; National Assembly of Pakistan, 2025; MoITT, 2023)

Several limitations restricted substantive conclusions. The data were synthetic, the demographic distribution was hypothetical, and the sample had no national representativeness. A real professional survey also faced common-method bias, differing levels of technical knowledge, and variation in exposure to AI systems. Advance sample

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.04 (2025)

planning, instrument validation, and consideration of organisational clustering remained necessary. Statistical significance could not substitute for those design requirements. (Lakens, 2022)

12. Conclusion

The research paper developed a quantitative framework for examining relationships between perceived algorithmic opacity, perceived adequacy of legal safeguards, and perceived risks to privacy, equality, and freedom of expression in Pakistan. By treating these rights as separate outcomes, the framework preserved distinctions between different legal concerns. The simulated analysis produced positive associations between opacity and perceived risks, alongside negative associations between safeguard adequacy and those outcomes. However, these patterns reflected the assumptions incorporated into the generated dataset. They did not establish actual human-rights violations, causal relationships, or the effectiveness of Pakistani institutions in regulating artificial intelligence (Creswell & Creswell, 2018).

The principal contribution concerned research design and the separation of technical, institutional, and legal questions. Difficulty understanding an automated decision did not itself establish unlawful conduct, while favourable perceptions of safeguards did not demonstrate that remedies were accessible or effective. Similarly, perceived risks required differentiation from documented harms and legally established violations. This distinction supported careful interpretation of findings and prevented statistical associations from being presented as judicial conclusions. The framework therefore provided a starting point for examining how explanations, oversight, and review procedures related to different rights concerns without resolving those issues through perception measures alone (UNESCO, 2021).

The research paper concluded that further investigation required observed evidence, appropriate legal interpretation, and direct examination of affected individuals' experiences. Empirical studies needed validated instruments, justified sampling, technical evaluations, and documented institutional practices. Complaint records, review outcomes, and accounts of automated decisions could help assess whether formal safeguards corresponded with meaningful protection. Sector-specific research also remained necessary because the implications of AI depended on its purpose, deployment, and consequences. Accordingly, the study offered a methodological foundation for future inquiry rather than proof of national conditions. Its conclusions encouraged evidence-based evaluation of AI governance while maintaining clear boundaries between perceptions and demonstrated outcomes (Creswell & Creswell, 2018).

13. Recommendations

13.1 Strengthening Personal-Data Protection

The research paper recommended clearer rules and procedures for personal-data processing in AI applications. Evaluation required attention to collection purposes, access, retention, and disclosure. Oversight arrangements also required accessible complaint mechanisms. Draft proposals required explicit identification until their legal status changed. These recommendations reflected privacy concerns identified in international analysis rather than effects demonstrated by the simulation. (OHCHR, 2021)

13.2 Assessing Unequal System Performance

The research paper recommended testing relevant AI systems across appropriate demographic and contextual groups. Evaluation required more than reporting overall accuracy. Investigators needed to identify the distribution and consequences of errors. Pakistani applications required locally relevant evidence rather than automatic transfer of

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.04 (2025)

overseas findings. This recommendation drew on the empirical importance of subgroup evaluation demonstrated by Buolamwini and Gebru (2018). (Buolamwini & Gebru, 2018)

13.3 Protecting Expression Through Review Procedures

The research paper recommended understandable explanations for consequential automated content decisions. Users required workable opportunities to seek review. Evaluation also required attention to the context of disputed expression. Documented decisions provided a stronger basis for assessment than general perceptions alone. These priorities were informed by international examination of AI and the information environment. (Kaye, 2018)

13.4 Improving Accountability and Human Oversight

The research paper recommended clearly assigned responsibility for AI-related decisions. Institutions required procedures for reviewing significant errors and responding to complaints. Human oversight needed defined authority rather than a nominal role. Accountability arrangements also required evaluation after deployment. These recommendations reflected UNESCO's emphasis on human oversight and responsibility across the AI lifecycle. (UNESCO, 2021)

13.5 Developing Empirical Legal and Technical Evidence

The research paper recommended combining surveys with documented cases and technical evaluations. Researchers required validated measures and justified sample sizes. Sector-specific investigations offered a way to examine clearly defined systems and institutional responsibilities. Findings also required careful separation of perceived risk, demonstrated harm, and legal liability. This approach strengthened the basis for future conclusions beyond the present methodological demonstration. (Lakens, 2022)

References

Ali, S., & Hassan, M. (2022). Evaluation of pending cases in the judiciary of Pakistan: Figures and statistics. *Pakistan Social Sciences Review, 6*(2), 592–602. https://doi.org/10.35484/pssr.2022(6-II)50

Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning Research, 81*, 77–91.

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE.

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE.

Field, A. (2018). *Discovering statistics using IBM SPSS statistics* (5th ed.). SAGE.

Field, A. (2018). *Discovering statistics using IBM SPSS statistics* (5th ed.). SAGE. International Chamber of Commerce. (2021). *Arbitration rules: In force as from 1 January 2021; Mediation rules: In force as from 1 January 2014*. Rules publication

Kaye, D. (2018). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* (A/73/348).

Khan, H., Afzal, U., & Iqbal, S. (2022). Comparative analysis of alternative dispute resolution laws in Pakistan: Its adaptation, procedure and compatibility. *Annals of Human and Social Sciences, 3*(3), 21–26. https://doi.org/10.35484/ahss.2022(3-III)03

Lakens, D. (2022). Sample size justification. *Collabra: Psychology*, *8*(1), Article 33267. https://doi.org/10.1525/collabra.33267

Lakens, D. (2022). Sample size justification. *Collabra: Psychology*, *8*(1), Article 33267. https://doi.org/10.1525/collabra.33267

Mashhood, A., Fatima, A., & Aamir, F. (2023). *Alternative dispute resolution in Sindh: A quantitative evaluation of case diversion potential & community demand*. Legal Aid Society. Full report

Ministry of Information Technology and Telecommunication. (2023). *Personal data protection bill, May 2023* [Draft]. Government of Pakistan.

Ministry of Information Technology and Telecommunication. (2025). *National artificial intelligence policy*. Government of Pakistan.

National Assembly of Pakistan. (2018). *The Constitution of the Islamic Republic of Pakistan: As modified up to 31 May 2018*.

National Assembly of Pakistan. (2025). *The Prevention of Electronic Crimes (Amendment) Act, 2025* (Act No. II of 2025).

National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)* (NIST AI 100-1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.AI.100-1

Office of the United Nations High Commissioner for Human Rights. (2021). *The right to privacy in the digital age* (A/HRC/48/31).

Organisation for Economic Co-operation and Development. (2021). *OECD framework and good practice principles for people-centred justice*. OECD Publishing. https://doi.org/10.1787/cdc3bde7-en

Organisation for Economic Co-operation and Development. (2025). *Toolkit for access to justice and people-centred justice systems*. OECD Publishing. https://doi.org/10.1787/aecf7f78-en

United Nations Commission on International Trade Law. (2021). *UNCITRAL notes on mediation*. United Nations.

United Nations Educational, Scientific and Cultural Organization. (2021). *Recommendation on the ethics of artificial intelligence*.

World Justice Project. (2019). *Global insights on access to justice 2019: Findings from the World Justice Project General Population Poll in 101 countries*.