INTERNATIONAL JOURNAL OF SOCIAL SCIENCES BULLETIN
ISSN: (E) 3007-1917 (P) 3007-1909
Volume 4, Issue 1, 2026

PROCEDURAL JUSTICE IN THE ERA OF ALGORITHMS: A CRITICAL EVALUATION OF AI GOVERNANCE AND DIGITAL RIGHTS

Ashraf Ali[1], Muhammad Aatif[*2], Aftab Haider[3]

[1]*Associate Professor, Dept of Law, Abdul Wali Khan University, Mardan*
[*2]*LLM Scholar Dept of Law, Abdul Wali Khan University, Mardan*
[3]*PhD Scholar in International Law at Southwest University of Political Science and Law, China*

[1]ashrafali@awkum.edu.pk, [*2]atifmayo.jag110@gmail.com, [3]aftabhaider516@gmail.com

Corresponding Author: *
Muhammad Aatif
DOI: https://doi.org/10.5281/zenodo.18586156

Received	Accepted	Published
20 November 2025	05 January 2026	20 January 2026

ABSTRACT

Today, AI is being added to government and business so quickly that international law cannot keep up, creating a risky situation for basic rights and freedoms. We argue that while AI offers unmatched efficiency, it simultaneously acts as a conduit for systemic risks, primarily through the mechanisms of algorithmic bias, opacity, and unauthorized data exploitation. This paper highlights critical disparities, such as commercial facial recognition systems exhibiting error rates of up to 35% for darker-skinned women compared to less than 1% for lighter-skinned men. Furthermore, we examine how algorithms in U.S. hospitals were found to be less likely to refer Black patients to healthcare programs than equally ill white counterparts. Our core thesis suggests that existing legal instruments—conceived for a pre-digital, human-centric era—lack the technical specificity and agility required to regulate autonomous black box systems. We adopt a multidisciplinary methodology, synthesizing doctrinal legal analysis with empirical evaluations of AI's impact on vulnerable populations. By critically examining the limitations of current regimes like the GDPR, we highlight the widening gap between technological capability and legal accountability. We conclude that without mandatory human-rights impact assessments and strong liability standards for developers, AI risks entrench historical inequalities. Lastly, we propose a shift toward adaptive regulation that prioritizes the right to an explanation to preserve human dignity in the digital age.

Keywords: *Artificial Intelligence, Algorithmic Bias, Human Rights, Procedural Justice, Adaptive Regulation, Data Privacy, Transparency, Digital Accountability.*

1.INTRODUCTION

In the contemporary digital landscape, the rapid proliferation of Artificial Intelligence (AI) has transcended mere technological advancement, evolving into a pervasive force that fundamentally reshapes the interaction between state authority, corporate power, and individual liberties. As we embark on this scholarly inquiry, our main thesis suggests that while AI offers unprecedented benefits in processing speed and decision-making efficiency, it simultaneously introduces grave risks of algorithmic bias, systemic discrimination, and the erosion of privacy rights. This article aims to critically examine these dualities, arguing that current international legal frameworks—conceived in a pre-digital era—are largely inadequate to meet the specialized challenges posed by autonomous systems. Our objective is to delineate the specific mechanisms through which AI infringes upon fundamental human rights and to propose a normative shift toward *adaptive regulation* and strong accountability structures.

To understand the gravity of this shift, one must first master the terminology central to the AI-human rights nexus. We define *Algorithmic Bias* as the systematic disadvantaging of specific individuals or groups due to prejudiced training

data or flawed system design. Parallel to this is the concept of *Explainable AI* (hereinafter referred to as XAI), which refers to the technical capacity of a system to provide understandable reasons for its conclusions, thereby mitigating the black box phenomenon where decisions are made without human-readable logic. We also use *Procedural Justice Theory* as our main perspective. Instead of only looking at the final result of an AI decision, we focus on how fair, transparent, and trustworthy the decision-making process is.

Our methodological approach is multidisciplinary, integrating legal scholarship with empirical case studies and statistical analysis of human rights violations. We move beyond abstract theory to examine real-world disparities, such as those found in facial recognition systems that exhibit significantly higher error rates for darker-skinned women compared to lighter-skinned men. By synthesizing international human rights conventions with the latest technological developments, we provide a comprehensive evaluation of how high-stakes fields—namely, criminal justice, healthcare, and employment—are being transformed by opaque algorithms.

One major concern we address is the conflict between data-heavy AI development and privacy rules like the General Data Protection Regulation (hereinafter referred to as GDPR) (Strzępek, 2025). While regulations have attempted to enforce data minimization, AI systems are inherently "data-hungry," often leading to the accumulation of sensitive personal information and the potential for re-identification of anonymized datasets. These privacy risks are not merely theoretical; they manifest in AI-powered surveillance systems and predictive analytics that monitor behavior without informed consent, fundamentally threatening the right to a private life as protected under the *Universal Declaration of Human Rights* (Haider, 2024); (Haider et al., 2025); (Ahmad & Haider, 2025).

Lastly, we advocate for a modernization of international law that explicitly recognizes *digital rights*, including the right to an explanation and the right to a remedy against automated decisions. We believe that the current fragmented regulatory landscape must be replaced by a dynamic and flexible framework capable of evolving alongside technological innovation (Ahmad et al., 2024). By establishing clear liability standards for developers and implementing mandatory human-rights impact assessments, we can ensure that AI serves as a tool for societal progress rather than perpetuating historical inequalities. Our contribution is a call for jurists and policymakers to close the growing gap between technological advances and legal protection (Hui et al., 2025); (Mathlouthi et al., 2025).

2. Algorithmic bias and discrimination

The artificial intelligence tools can carry significant benefits, yet they come with grave risks. A significant issue is algorithmic bias discrimination. Bias occurs when an AI system decides or predicts that systematically advantages or disadvantages some individuals or groups, and such Bias occurs when an AI system makes decisions or predictions that systematically advantage or disadvantage certain individuals or groups, and such patterns can perpetuate existing inequalities. An AI model favors one group due to poor or biased training. In case of biased training data, the AI will learn and propagate these biases (Jain & Verma, 2025). To give a specific example, an AI employed to assist companies in the selection of candidates might tend to prefer candidates in demographic groups that were historically favored during the hiring process, regardless of whether the algorithm itself is programmed to do this.

Data may also be imbalanced or incomplete. Consider facial recognition victims. Facial recognition programs that have been developed using primarily white faces might fail to detect people of different racial groups. This discrimination may translate to poor treatment and, in some cases, policing with the use of AI-enabled facial recognition, incorrectly identifying people of color, resulting in false arrests or unnecessary surveillance. Bias can also be introduced through the design of an AI system. Developers determine the inclusion of features and variables, as well as the algorithms to use. Otherwise, they may end up designing systems that discriminate against the marginalized without careful consideration of the social and ethical consequences of their decisions (Bharati, 2025).

The outcomes of biased AI systems are severe when they concern criminal justice, employment, lending, and healthcare. Unfair AI may shut the door and limit the chance to get opportunities, maintaining inequality. Discriminatory predictive policing systems may target minority neighborhoods more frequently, which increases

police stops and racial profiling (Haider, Ahmad, et al., 2023). When it comes to hiring, the algorithms could also discriminate against females or individuals of diverse backgrounds, which increases the current gender and racial disparities. In health care, algorithms can prescribe inferior care to minority patients simply because the data that was used to train the system was biased. As an example, the AI models may not be as accurate in diagnosing conditions in racial or ethnic minorities, thus making health gaps even bigger (Goswami, 2025).

3. Addressing Algorithmic Bias

Several measures are required to prevent algorithmic bias. First, the data that is going to be used to train AI should be varied. To minimize bias, systems should be trained on data that consists of numerous distinct groups. Maintaining such data by collecting and curating it is a continuous process. Second, developers should prioritize transparency and accountability. Periodic audits should be done to see that there is fairness of the results. Explainable AI (XAI) models assist everyone in comprehending the process through which the system arrives at its conclusions and identify potential discrimination patterns and biases. Third, there must be clear-cut ethics and rules (Haider, Ali, et al., 2024); (Haider, Raza, et al., 2023). Governments, regulatory authorities, and industry associations must collaborate to establish standards in the name of fairness and equality (Haider & Afzal, 2025). The standards are supposed to ensure that AI systems do not establish or increase discrimination (Ferreira & Gromova, 2025).

AI systems require huge datasets to train the algorithms; hence, they perform very well in tasks such as image recognition, natural language processing, and decision making. However, although the data is useful when it comes to the work of AI, the collection and utilization of personal information in AI raises significant privacy issues. Facial recognition and surveillance through social media are AI-powered surveillance systems that may violate the right to privacy (Manheim & Kaplan, 2019). Such tools monitor the movements, behavior, and interactions of people, and this may take place without their knowledge, causing the loss of privacy rights. Sensitive personal data such as health records, financial information, and browsing habits can also be collected and analyzed using AI technologies. AI can predict human behavior. It is used by companies, governments, and others to make decisions, profile, or do ads that target people. In some cases, the information gathered is highly personal, such as the political views, sexual orientation, and medical history of an individual. Predictive analytics may also pose a threat to privacy, since AI examines individual data to make assumptions about what an individual may do in the future, like default on a loan or commit a crime. Such guesses may be unjust, particularly when the AI is fed with biased data. As an example, AI-based police predicting crimes may discriminate against minority groups, which is detrimental to their privacy and rights (Shahriar et al., 2023); (Haider, Yousaf, et al., 2024); (Haider, Ali, et al., 2023).

Regulations like the GDPR in the EU are laws that ensure the protection of personal data. Nevertheless, such rules become harder to follow when AI is utilized on a global scale (Yanamala & Suryadevara, 2024).The main problems are:

Data Minimization: AI systems are usually quite data-intensive, which conflicts with the GDPR mandate that the minimum possible amount of data should be collected. This can lead to the accumulation of data.

Data Anonymization: Many AI applications need the hiding or modification of personal data of individuals to preserve their anonymity. According to the latest studies, AI can sometimes recognize the owner of the data by connecting the anonymized data to other data sets and compromising privacy (Meurisch and Muhlhauser, 2022).

Cross-Border Data Flow: AI systems often exchange data across borders, and it is hard to enforce data protection laws. There is no guarantee that personal data will be as secure when it is sent to other nations that have different privacy laws (Meurisch and Muhlhauser, 2022).

In order to diminish the privacy risks of artificial intelligence (AI) systems, a complex of comprehensive steps can be adopted (Haider et al., 2026). First of all, the governmental bodies need to change and modernize the existing data protection legislation, ensuring that the legal frameworks are created with the peculiarities of AI technologies in mind. Such legislative modifications should be timely and in accordance with the pace of technological development and should contain a

provision that safeguards personal information in AI.

Second, AI systems must be developed in a manner that involves transparency and accountability mechanisms. This will enable individuals to know how their data is processed, and they will be informed. In addition, accountability in the organization should be developed efficiently to avoid the abuse of personal information, which Ikwuanusi et al. (2023) observe.

Third, privacy-enhancing technologies (PETs) like encryption and other technologies of this kind can be implemented to guarantee the security of personal data and, conversely, to provide organizations with the benefits of AI analytics. Such technical controls may be used to assist organizations in maintaining user privacy without affecting organizational efficiency. Finally, the ethical development of AI demands that developers go through rigorous training on privacy-oriented design principles. One of the methods that will ensure the design of AI systems considers user privacy at the initial stages is a privacy-by-design paradigm, which is advocated by Paul (2024).

Transparency and Accountability in AI Decision-Making: A Critical Analysis

AI systems are more pervasive and achieve a higher processing speed in healthcare, finance, and criminal justice. The systems are now able to make critical decisions independently. Fairness, trust, and ethics become a big issue because they operate without a clear explanation. We require regulations and frameworks that make AI decisions transparent and accessible, particularly when the consequences will have significant impacts on people's lives (Aftab Haider & Ayesha Sadiq, 2025). Transparency in this context refers to the capacity to understand and to describe the path through which AI systems come to their conclusions, and Accountability implies that the people involved are accountable for their decisions. Procedural Justice theories may be helpful to understand these ideas better. This theory focuses on justice in action that precedes a decision being made, and it can give us some important insights into why transparency and accountability are important elements of AI (Perla & Di Grassi, 2025).

According to the Procedural Justice Theory, individuals tend to accept outcomes that appear to be fair, even though they may not be what they want to see. The theory is concerned with the running of the process and not the product. People accept and trust what an AI system proposes when decision transparency and accountability are constructed during decision-making. In potentially dangerous areas like criminal justice, employment, or loan authorization, AI can lock or unlock the gate for individuals. To be considered legitimate, the process that takes place to arrive at a verdict or recommendation has to be transparent, with clear steps that can be examined or challenged. Transparency can cause individuals to observe the way an AI system gets its answer, disclosing its algorithms, data sources, and reasoning. This allows even non-technical users to know what is going on. Accountability is a method to hold people responsible and dispute errors or wrong results. It takes accountability of developers, organizations, and regulators for their effect (Gabriel, 2022).

Transparency in AI enables all parties involved (users, developers, regulators, and society) to understand how AI systems work. However, deep learning and neural networks tend to be used as a "black box" in AI models. It implies that the process of making AI decisions is often not clear, the data is not always used, and the model may be biased. Critics believe that in the absence of transparency, AI results may be discriminatory or unfair. As an example, an AI-based hiring system can discriminate against one group of people because of biased training data. In the absence of transparency, these problems will be concealed, and AI systems can be based on unreliable or biased data. To solve this, explainable AI (XAI) has been introduced to make AI models more interpretable so that humans can comprehend and question the decision-making process (Gordon, 2013). Nevertheless, complete transparency is hard to achieve. Most AI and deep learning models are difficult to understand. Accuracy and interpretability also have a trade-off: complex models are more accurate and less interpretable, whereas simple models are easier to understand and less accurate. This leads to the question of whether transparency is enough and whether full transparency is possible without diminishing the performance of AI systems (Guler et al., 2025).

Responsibility in AI implies that the developers, users, and organizations that deploy artificial intelligence are responsible to its actions. This is

also a current concern in the spheres that directly impact human well-being, such as criminal justice and healthcare. When it comes to detrimental mistakes on the part of AI, such as the categorization of criminal behavior, hiring discrimination, or giving faulty medical guidance, it is essential to define who should be held responsible. In the absence of clear guidelines, the blame game, whether it is on the developer, the user, or the organization that manages the system, becomes very hard, particularly when AI systems are used on their own without human oversight. Accountability is therefore needed to foster equity and to create credibility among the population (Doshi-Velez et al., 2019).

There must be clear laws to establish the functions of policing artificial intelligence, to establish mechanisms through which the individuals can challenge AI decisions, and to establish remedial actions that may be taken in case of any mistakes. Without human control, the responsible AI operation would not be possible. Transparency and sound accountability systems interact is a necessity to build the fairness and reliability of AI systems.

Artificial intelligence liability is complicated due to the presence of numerous stakeholders, including data providers, developers, and implementing bodies, and it might be incomprehensible who should be held accountable when the system collapses. The regulatory frameworks are often outpaced by the fast rate of AI development and, therefore, result in the absence of accountability. Most jurisdictional laws on current liabilities have not been designed to address AI-related problems, particularly those decisions that are products of complex algorithms that are not easily understood, interpreted, or audited (Tatipamula, 2025).

AI is hard to control. We must create a balance between three things: transparency, accountability, and innovation. Accountability and reporting protect human rights and create trust in AI. Nevertheless, in cases where the rules are strictly maintained, they may stifle new ideas. Developers can be forced to reveal all the details about their models or even be legally responsible when an AI is making a decision. To balance out these requirements, we must integrate openness and responsibility of the means through which AI systems are created without hindering progress. This balance is something that can manifest itself in ethical principles of design: conducting fairness audits and bias testing as a system is constructed, and post-deployment check and update of the system (Kashefi et al., 2024).

5. Impacts on Vulnerable Populations (e.g., marginalized groups)

5.1 Facial Recognition Accuracy Disparities

Study: A 2018 study by Joy Buolamwini and Timnit Gebru revealed that commercial facial recognition systems exhibited error rates of up to **35%** when identifying darker-skinned women, compared to less than **1%** for lighter-skinned men. > (Buolamwini & Gebru, 2018)
2. AI Hiring Bias
Study: An Australian study found that AI hiring tools often penalize candidates with employment gaps, affecting women who take time off for caregiving or health reasons. Additionally, speech-to-text AI used in video interviews has high error rates for non-native English speakers, particularly Chinese speakers. (Zeng et al., 2025)
3. Healthcare Disparities
Study: A 2019 study found that an algorithm used in U.S. hospitals was less likely to refer Black patients to healthcare programs than equally sick white patients. The software, which used healthcare costs in the preceding year as a primary indicator for the seriousness of a disease, did not recognize that Black patients were substantially sicker and received less access to care. (Wordpress, 2021)
4. Ride-Hailing Price Discrimination
Study: Research analyzing 100 million ride-hailing samples from Chicago indicated that neighborhoods with larger non-white populations, higher poverty levels, younger residents, and high education levels were significantly associated with higher fare prices. (Pandey & Caliskan, 2021)

6. Statistical Evidence of Human Rights Violations in AI

With the growing adoption of AI technologies in various industries, including law enforcement, employment, medical care, and finance, the idea of their threat to human rights is becoming increasingly popular. The statistical data indicate that AI is used to violate rights in several critical areas, especially in the fields of discrimination, privacy, fairness, and accountability. These statistics give a numerical perspective of the impact of AI on human rights and the necessity to establish stronger regulatory frameworks to make sure that AI is created and utilized ethically (Raso et al., 2018b).

Surveillance and data collection systems based on AI are dangerous to privacy. They can trace the people, their activities, and even predict what they will do tomorrow. This steady loss of privacy harms individual rights. Governments and businesses are using facial-recognition tools that often discriminate against minority groups and raise fears of mass surveillance. According to the 2021 report of Amnesty International, the same type of AI-based systems in the United States and Europe infringe the privacy as well, with particular concern related to the placement of such systems in public areas, with a lack of clarity among the audience. In a test last year, Amazon Recognition facial-recognition software falsely identified 28 members of Congress as criminals, which shows how AI-based surveillance can be inaccurate, particularly when it is not transparent and accountable (Mahmoudi, 2021).

Human rights are also violated using AI tools in healthcare. They may exacerbate inequalities and result in discrimination. According to a 2019 article published in Science magazine, an algorithm that U.S. hospitals utilized in predicting medical needs was much less likely to recommend Black patients to health care programs than their equally ill counterparts, white patients. Since Black patients have traditionally been undermined in medical care, their needs were distorted in the system (Obermeyer et al., 2019). The inequality in access to care and the violation of the right to health occurred because of that bias. In 2020, the National Institutes of Health (NIH) remarked that the accuracy of AI-based diagnostic systems implemented to predict diseases such as cancer was lower among minorities. AI systems that had been trained primarily on the data of white patients did not identify some conditions in Black or Hispanic patients. This generated disparate health results and violated the right to health and the right to non-discrimination (Li et al., 2024).

It is challenging to ensure that AI systems have human rights when they are black-box-like. The decision-making process of the computer is beyond the eyes of most people. According to a 2019 report released by the AI Now Institute, tools deployed in criminal justice and immigration enforcement did not have sufficient transparency and accountability. Police departments across the country made use of predictive policing algorithms and risk-assessment algorithms that were very biased in their datasets and would produce discriminatory results against Black and Hispanic people (Kossow et al., 2022). In the absence of strong monitoring and accountability, there are limited means by which individuals may challenge such decisions, and this contravenes the right to an effective remedy and to a fair trial. The same problem is present in AI-based credit-scoring systems. They make decisions to lend to an individual based on a lot of data: behavior on the internet, on social media. Such systems have, on other occasions, caused adverse disproportionate harm to low-income people and minority groups, violating their right to equal treatment and non-discrimination in financial services (Diakopoulos, 2020).

7. Recommendations for Strengthening International Law and AI Governance

The sphere of artificial intelligence is changing at an incredibly fast pace, and it is touching nearly every sphere of contemporary life. Through this, there is a need to establish stronger international laws and more open regulations to protect human rights. The current legislation is a rough structure, but it is not able to follow the pace of the development of AI and its influence on the basic rights, including privacy, equality, and fairness. This section suggests new ideas, changes to the existing policies, and flexible structures that can change according to the dynamic and complex nature of AI (Maas, 2021).

1. The Need for a Dynamic Regulatory Framework

The most significant change in AI regulation that has taken place recently is the shift to a more flexible legal framework. It is not only a responsive

system, but also a predictive one. Existing regulations such as the EU AI Act and GDPR are a good starting point, but they are constructed on rigid rules, which will soon be obsolete because of the advancement in technology. This is added to the fact that numerous ethical concerns and novel risks are not tackled in a proper way (Zaidan and Ibrahim, 2024).

The international law must also be elastic. The rules must not lag behind the technology since AI can be not only current but also at the new standards. Adaptive regulation implies that AI laws are updated on a regular basis as new circumstances emerge. The international bodies such as the United Nations (UN) and OECD can intervene by regularly updating AI regulations and creating special committees to discover how emerging AI technologies influence human rights. Such panels are then able to suggest changes to the law at a later date. It is an active methodology that helps to close the technological-legal divide to hold governments more responsible to technological issues like algorithmic bias, AI surveillance, and privacy threats (Lescrauwaet et al., 2022).

2. Strengthening Human Rights Protections through International Treaties

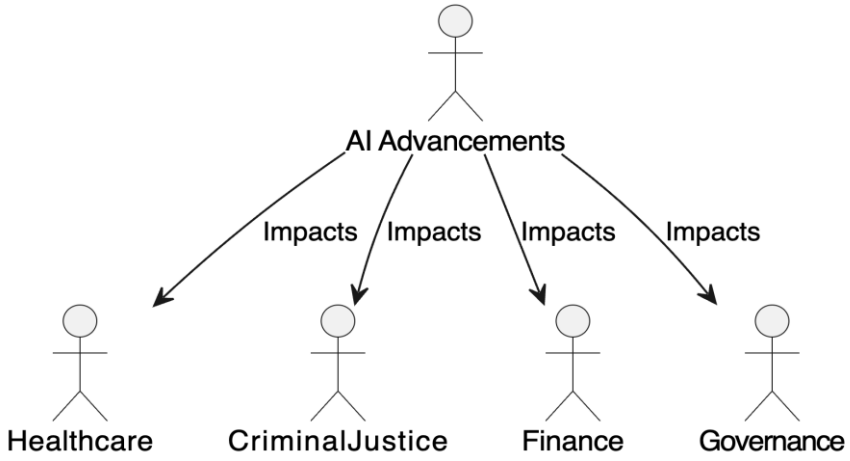
The influence of AI on society is immense, and to save humanity, the countries should have a powerful international consensus on AI ethics and human rights. The common set of rules in the use of AI on a global scale would be created by such a treaty. It must be grounded on the current human rights conventions, such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. Meanwhile, the treaty should address emerging AI issues, including the transparency of algorithms, privacy, and decision responsibility. Another of the improvements would be a separate section on AI and human rights, which explicitly establishes the right to explanation and the right to remedy. As an illustration, the GDPR already provides the right to an explanation to the Europeans in the case of automated systems decision-making (Latonero, 2018). This right must be global and extend to all the individuals who are impacted by the use of AI in decision-making. It also allows individuals to know how the AI systems make decisions that will impact their lives, and it becomes less challenging to question biased or discriminatory behavior. New AI transparency rules would be another major change. The treaty must demand that AI systems, particularly high-stakes models such as those utilized in criminal justice and employment, display explicit data concerning their training, decision-making process, and biases put in place. Lastly, the treaty should emphasize responsibility. Governments, companies, and developers should be held accountable for AI systems that infringe human rights or strengthen discrimination (Hogan & Lasek-Markey, 2024).

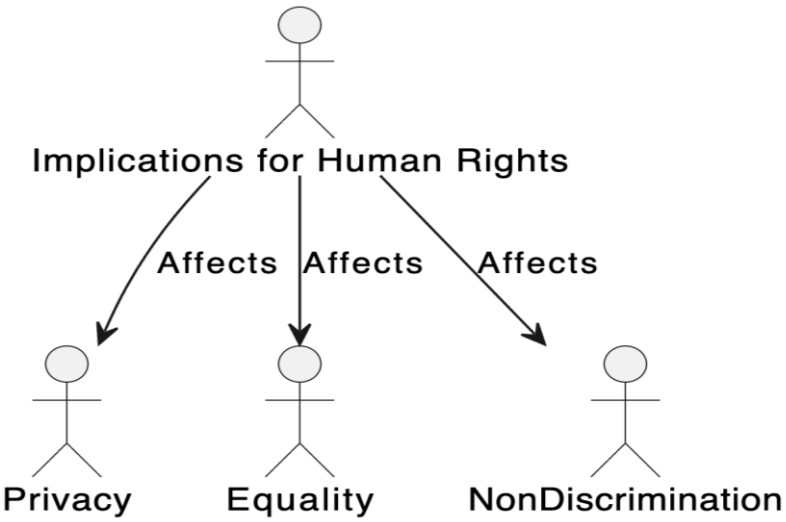
3. Modifying Existing Legislation to Address AI Risks

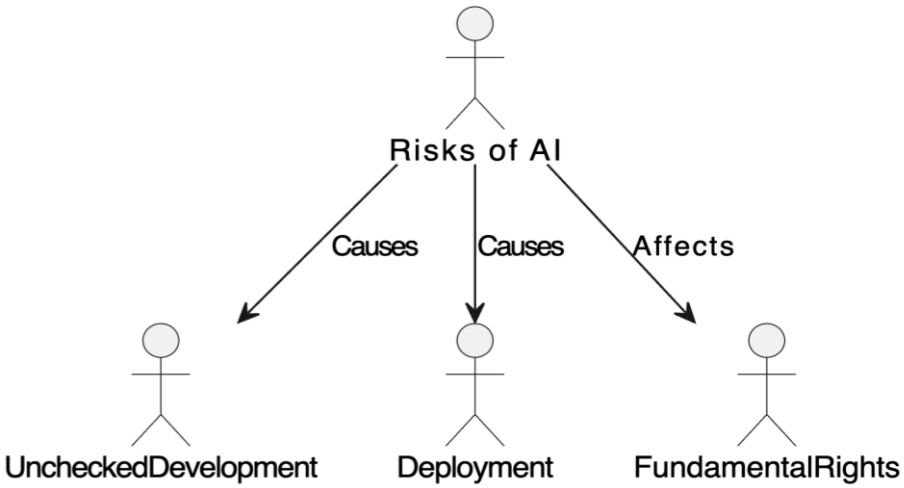
The law must be modernized to address the current AI threats. Some of the provisions of international human rights law demand amendments that incorporate AI issues. According to Article 12 of the Universal Declaration of Human Rights, individuals are entitled to privacy and freedom from unjustified interference. However, everyday AI tools, like facial recognition technology and surveillance cameras, are all pervasive now. Such an article should be corrected to include the fact that digital privacy also applies to situations where automated data collection occurs. That may imply offering a degree of protection to digital data (including biometric data) against unwarranted AI-enabled surveillance (Scherer, 2015). The right to participate in government is provided by Article 21 of the Universal Declaration. It ought to be revised to capture the right to be involved in AI governance. Since AI-based systems are being applied to governance (such as predictive policing and election systems), citizens need an opportunity to shape the application of AI to governance so that it does not adversely affect their rights, such as through biased or impervious algorithms. The right to a fair trial is guaranteed by Article 10 of the European Convention on Human Rights. It should clearly state AI-based decision-making. Criminal justice, healthcare, and finance AI systems should be transparent and accountable to ensure that the decisions generated by the systems can be analyzed in court and are not protected by algorithmic opaqueness (Nations, 2000).

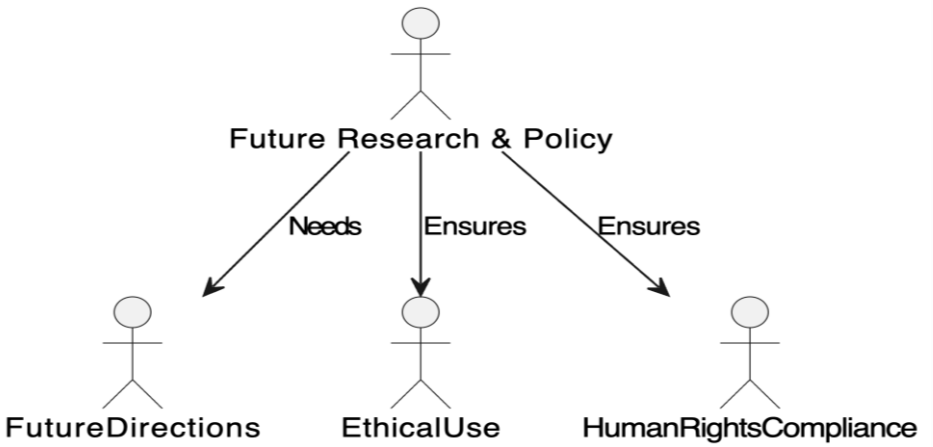
8. Future Directions for Research and Policy in AI and Human Rights

Following Figure 1,2,3, and 4 shows the future research direction;









9. Establishing Ethical AI Frameworks and Standards

Future research projects may seek to create artificial intelligence that is morally acceptable in every situation. At this point, a lack of a global regulatory framework that would encompass all the potential effects of AI on human rights is present. Regulations on AI must go beyond technical aspects and include both social, cultural, and psychological consequences of the technology. There is a need to question the transformations of power relations among people and how AI can cause harm to vulnerable groups. New scholarship must develop strategies that are based on fairness, honesty, responsibility, and inclusion. These strategies should be based on conceptual foundations that include algorithmic fairness, data equality, and discrimination avoidance (McKenzie, 2023). Since AI has a wide range of occupational settings where it is applied, multidisciplinary knowledge must be incorporated into ethical AI studies. This integration must be a combination of legal scholarship, social science, philosophy, and technological expertise. The stakeholders of the geopolitical borders should work together to ensure that the AI systems not only perform effectively, but also protect human rights. As an example, when combating gender bias in AI-based recruitment systems or racial bias in predictive policing, ethicists, sociologists, technologists, and legislators are to work together to prevent the spread of harmful biases.

The governmental authorities ought to put in place clear laws that regulate the development and implementation of AI in a moral way. They can set up special agencies that would ensure compliance in all sectors. Such agencies should also liaise with international organizations, including the United Nations and the European Union, to have common standards, as AI is ubiquitous all over the world (Zhou et al., 2025).

10. Advancing AI Accountability Mechanisms

The more autonomous AI systems are, the harder it is to define responsibility. It is particularly significant in such high-stakes fields as criminal justice and finance when the decisions made by AI can have severe consequences on the lives of people. Thus, the decisions made by AI should be constantly controlled with the help of special oversight devices. Explainable AI (XAI) is one such example and is expected to make AI transparent, understandable, and capable of explaining its decision to non-experts.

New ethical and legal issues are also brought about by AI. Legislators must determine whether existing regulations suffice to make an individual responsible in case of AI-related harm (Schmidt et al., 2025). Some of the questions are: Who is liable in case an autonomous AI system harms a person, and there is no human operator? This might require new legislation to make companies and developers more accountable in making AI safe, fair, and legal.

There should be clear and transparent laws that specify who will make the decisions regarding AI and how people can seek redress in case they are harmed by AI. To oversee AI systems, governments

need to create AI ethics committees or independent audit bodies to make sure that the systems are fair, transparent, and accountable. Such agencies would hold developers and companies accountable for any adverse impact of AI on human rights (Meduri et al., 2025).

11. Promoting Inclusive AI and Data Diversity

The problem of bias in AI systems is that the diversity of the training data is limited. The problem is that a lot of AI systems are constructed using datasets that lack all human experiences, which is why the outcomes are biased and unfair. An example of this is that facial-recognition technology tends not to perform well when used with black people, since they were not well-represented during training (Güven et al., 2025). The task of future research should be to expand the data range to ensure that AI systems represent the global population. It implies gathering data about the marginalized and underrepresented groups to ensure that AI does not recreate current disparities. Researchers ought to also develop equitable methods of data collection, and data collection methods that do not compromise the privacy and consent of people. Privacy-preserving machine learning methods like federated learning and differential privacy ought to be investigated in order to enable AI models to access sensitive data to learn without breaching privacy (Shams et al., 2025).

The policymakers must enact policies that will require data diversity in AI training data sets and demand transparency on the origins of the data. They must also enforce legal regulations that prioritize individual privacy and consent. GDPR has a strong basis, yet such protection needs to be adapted and extended further by governments worldwide to be able to address emerging AI-related concerns (Emma, 2024).

12. Expanding Human Rights Law to Address AI-Specific Issues

The existing laws regarding human rights do not provide people with absolute security against the dangers posed by AI systems. Further studies are needed in the development of special laws on AI, where the use of the former is explained, and the protection of fundamental human rights is emphasized. It entails the application and expansion of existing documents, such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, and new concerns, such as the right to explanation, the right to remedy, and the right to non-discrimination in AI decision-making. The human-rights-based approach to AI governance, such as the utilization of human-rights impact assessment (HRIAs) in the process of creating AI systems, should also be empirically examined. Such evaluations would reveal any possible human-rights risks before deployment and enable developers to minimize them (Li, 2025).

Policy implication: International organizations and governments ought to incorporate specific AI-related human rights clauses as part of their legal frameworks. International conventions, like the EU AI Act or the OECD AI Principles, ought to be developed that specifically protect human rights in AI systems. Such treaties should not be rigid and should be able to adapt to new challenges and technologies involving AI (R. Ahmad et al., 2025).

13. Addressing the Social and Economic Impacts of AI

Artificial intelligence (AI) is transforming the labor market and life in general. The consequences of these changes to individual actors, particularly those who are the most vulnerable to these changes, should be questioned in future studies. The low-skilled workers, minorities, and women should be the priority of the research because these populations have increased susceptibility to displacement due to automation. Researchers should also determine whether AI is causing an increase in the digital divide, a rise in socioeconomic inequality, or an increase in job loss and underemployment. As a result, policy tools like universal basic income (UBI) and mass reskilling programmes should be considered to make a worker change in an AI-dominated economy.

To address the displacing effects of artificial intelligence on the labor market, policymakers have a responsibility of developing robust safety-net programs, particularly universal basic income programs and targeted re-training programs, to cushion those workers who lose employment opportunities to AI. Therefore, the government will have to spend a substantial amount of money on education and professional training courses that will help to prepare the workforce to operate in an AI-based economy, so that people will be able to be flexible and saleable in the changing technological environment. In the meantime, the

strong protection of equity should also be included in such policy interventions to ensure that the positive contributions that AI brings to society could also be evenly distributed so that the increase in economic and social inequalities could be avoided.

Conclusion

This study describes how artificial intelligence (AI) could be used to protect human rights. It also outlines the ethical concerns of AI and proposes a new legal framework to govern its use. It is addressed to a deeper understanding of the law, its postulates and dogmas, in a manner that the production and use of AI cannot be used to violate human dignity and the fundamental freedoms.

AI governance should be based on procedural justice and due process. It is not only the responsibility of the developers of AI decision-making systems to strive to attain fair results but also to establish trust in individuals by ensuring the decision-making process is fair, transparent, and open. There should be procedural justice in AI architectures, where the algorithms behind AI decisions can be questioned and challenged. The right to explanation is one of them, which gives individuals the right to understand and object to decisions about them, which is often missing in contemporary AI systems. AI must not be a black box but be transparent and legally accountable.

It should develop new laws or amend the current laws that would protect human rights as well as address the new challenges posed by AI. International human rights declarations such as the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR) have long been protecting the basic rights, but they are not keeping up with the technological development of AI

UDHR should be extended to digital privacy by applying Article 12 that forbids unlawful intrusion of privacy. Facial recognition and predictive policing may be applied with or without consent or awareness, therefore violating the privacy of individuals and placing them under unreasonable surveillance. Thus, I can conclude that the UDHR should be revised to provide protection to privacy rights in the era of AI and grant online and biometric data the same protection as standard privacy rights (Nyst & Falchetta, 2017). The General Data Protection Regulation (GDPR), created by the European Union, is a great move in protecting personal data, yet it must be expanded to AI-related issues. The right to explanation outlined in GDPR is heading in the right direction, but it must be more prescriptive and more effective, particularly regarding personal data utilization by the AI systems in making decisions. All that would be needed to fix it is to introduce a legal requirement that AI systems should be able to explain how they made their decision and be subject to independent auditing to demonstrate that it is fair and meets human rights standards. Due to this fact, I consider that GDPR needs to require the human rights impact assessment (HRIA) of AI systems before their application, particularly in high-risk environments (Juliussen, 2025).

We require definitive guidelines displaying who is liable in the case of damage done by AI systems. Criminal justice, finance, and medical applications of AI already exist, and therefore, it is pressing to establish legal frameworks that allocate responsibility. People should know how to seek assistance when the technology produces unfair outcomes: AI bias in recruitment tools or biased predictive policing, to name but a few. The development of new laws must hold developers and companies that work with AI responsible. They are obliged to establish means through which people can claim redress when AI systems harm. The rules must also specify who will bear the impact of an AI decision: the developers who made the system, the businesses that made use of it, or the governments that control its application. Finally, we must have a theory of adaptive regulation to stay abreast of the blistering development of AI. Existing legislation, such as the AI Act introduced by the EU, is useful but unchanging; it is likely to become obsolete shortly, as AI continues to evolve. The adaptive regulation theory demands dynamic and flexible rules that are adaptive to technology. In this theory, the control of AI must involve periodic periods of review, which would enable it to make amendments when new AI technologies and applications are discovered. The theory must also promote inter-regulatory cooperation so that the laws can be easily adjusted to reflect new ethical issues, including how AI is used in autonomous weapon systems, deepfakes, or predictive analytics in hiring, lending, and criminal justice.

The current concern of human rights is primarily with concrete physical and material needs. But the

digital age and AI (artificial intelligence) introduce new hazards that are not addressed by ancient human-rights laws. Artificial intelligence systems are already making decisions that people live by in healthcare, education, law enforcement, employment, etc., hence the need to redefine human rights to incorporate digital rights. Algorithms require accountability, and digital privacy, as well as the right to explanation, should be incorporated into human-rights frameworks. Based on automated profiling and predictive analytics, decisions can be made about personal outcomes, and individuals have a limited ability to determine or counter these decisions. They must understand how their personal information is utilized and be capable of challenging automated procedures that affect them, particularly in credit scoring, recruitment, and policing. The Universal Declaration of Human Rights and international law have a loophole that makes citizens vulnerable to decisions of AI systems. Such legal tools will have to be modified or augmented with clauses specific to AI to protect digital rights and hold such engines liable in case they cause damage. Then we will be sure that the AI technology will not be detrimental to fundamental human rights, but will be in their support (Abrusci et al., 2018).

Existing AI regulations are fragmented. In some areas, such as the European Union, governments have been working to control AI, with the EU AI Act being the most common, but there is no unified global consensus. Different countries have come up with their own ways of regulating AI, and their approaches differ in terms of how much emphasis they place on human rights and ethics. "As AI work is transnational, these different regulations create serious complications when an AI system is deployed across multiple jurisdictions. For this reason, I believe it is the role of organizations like the United Nations (UN) and the Organization for Economic Co-operation and Development (OECD) to step in and democratically work to enshrine values and clear principles that guide AI development, with a primary focus on human rights, non-discrimination, and algorithmic accountability and data privacy. These goals need to be operationalized into concrete, actionable objectives, backed by international standards for the use of AI and enforced by strict and enforceable regulations. This will only be possible through cooperation between industry and government. This would give companies an incentive to build AI systems that incorporate safeguards for human rights and would ensure that governments are well-positioned to regulate AI and hold companies accountable.

While AI systems work and perform efficiently, they often fail to properly address ethical concerns. From predictive policing and hiring to other areas of AI, bias and discrimination (whether racial, gender, or otherwise) are ingrained in many tools. Designers must develop strong ethical standards and keep fairness, non-discrimination, and human dignity at the core of AI development right from the start. One of the best ways to accomplish this would be to ensure all AI projects include Human Rights Impact Assessments (HRIA). Such reviews would examine the impact that a system can have on the rights of people before its implementation. HRIA resembles Environmental Impact Assessments (EIA), which examine the potential adverse effects that a project may have on the environment. HRIA would look at the potential harm an AI system can inflict on human rights, highlight the risks, e.g., discriminatory bias, privacy violations, and provide solutions on how to address them before the system is implemented. This review should always be a part of high-risk AI applications in the healthcare, criminal justice, and finance sectors. Using HRIA, the development of AI can remain ethical and yet provide its benefits by not violating human rights. The expert groups should conduct independent audits to ensure that all systems are not biased and conform to human rights standards.

Responsibility is one of the key issues in the artificial intelligence context since in the case of damage, the party to blame is unclear. The responsibility of attributing culpability becomes more complicated as AI systems become more autonomous. In cases where an AI system makes a biased hiring choice or causes harm by predictive policing, the most important question is, is the developer, the hiring company, or the regulator that approved the implementation liable? One of the solutions is a remedial one, which is the introduction of AI accountability laws. These laws should define who or what should be responsible in case of harm caused by AI and provide the parties concerned with simple avenues of redress. Individuals whose decisions are made by AI should be told the rationale behind such decisions, especially when making high-stakes decisions such

as employment, health care, and the right to counsel. They should be empowered to appeal such decisions. Moreover, governments should create special oversight agencies that will control the design and implementation of AI systems. These agencies would make sure that the AI is employed in a responsible, transparent, and ethical manner, apply the principles of human rights, and become the primary adjudicator of violations and complaints management.

Acknowledgment

This article is derived from the thesis of Muhammad Aatif, titled "Potential Human Rights Risk Associated with Emerging Artificial Intelligence Technologies: Analysis of Data Protection," submitted to Abdul Wali Khan University, Mardan, under the supervision of Dr. Ashraf Ali and with further assistance from Aftab Haider.

REFERENCES

Jain, V., & Verma, D. R. (2025). Governing the Artificial Intelligence of Things: Navigating Techno-Legal Challenges in a Connected World. *Available at SSRN 5254579*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5254579

Bharati, D. R. (2025). *Bias and Fairness in AI Algorithms: Legal Standards and Ethical Guidelines*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5378211

Goswami, A. (2025). AI Governance for Risk Modelling in European Banks: A Compliance-First Approach. *Available at SSRN 5360444*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5360444

Ferreira, D. B., & Gromova, E. A. (2025). The Bossware Era and the e-Panopticon: Current Technologies and Legal Challenges. *Industrial Law Journal*, dwaf006. https://academic.oup.com/ilj/advance-article-abstract/doi/10.1093/indlaw/dwaf006/8071938

Manheim, K., & Kaplan, L. (2019). Artificial intelligence: Risks to privacy and democracy. *Yale JL & Tech.*, *21*, 106. https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/yjolt21&section=4

Shahriar, S., Allana, S., Hazratifard, S. M., & Dara, R. (2023). A survey of privacy risks and mitigation strategies in the artificial intelligence life cycle. *IEEE Access*, *11*, 61829–61854. https://ieeexplore.ieee.org/abstract/document/10155147/

Yanamala, A. K. Y., & Suryadevara, S. (2024). Navigating data protection challenges in the era of artificial intelligence: A comprehensive review. *Revista de Inteligencia Artificial En Medicina*, *15*(1), 113–146. https://www.academia.edu/download/119087510/113_146_redc_2024.pdf

Meurisch, C., & Mühlhäuser, M. (2022). Data Protection in AI Services: A Survey. *ACM Computing Surveys*, *54*(2), 1–38. https://doi.org/10.1145/3440754

Ikwuanusi, U. F., Adepoju, P. A., & Odionu, C. S. (2023). Advancing ethical AI practices to solve data privacy issues in library systems. *International Journal of Multidisciplinary Research Updates*, *6*(1), 033–044. https://www.researchgate.net/profile/Ugochukwu-Ikwuanusi/publication/387313189_Advancing_ethical_AI_practices_to_solve_data_privacy_issues_in_library_systems/links/67aa92c38311ce680c5c959e/Advancing-ethical-AI-practices-to-solve-data-privacy-issues-in-library-systems.pdf

Paul, J. (2024). Privacy and data security concerns in AI. *ResearchGate, November*. https://www.researchgate.net/profile/Joel-Paul-10/publication/385781993_Privacy_and_data_security_concerns_in_AI/links/6734ffe2f255d5728669d3a3/Privacy-and-data-security-concerns-in-AI.pdf

Perla, L., & Di Grassi, A. (2025). 6 Transparency and Accountability in AI Decision-Making Processes. *AI-Powered Pedagogy and Curriculum Design: Practical Insights for Educators*. https://books.google.com/books?hl=en&lr=&id=9B12EQAAQBAJ&oi=fnd&pg=PT12&dq=Transparency+and+Accountability+in+AI+Decision-Making&ots=6wAU_mdIUB&sig=P5Gl3oHKKPNr0L0imBESh4Ul600

Gabriel, I. (2022). Toward a theory of justice for artificial intelligence. *Daedalus*, *151*(2), 218–231. https://direct.mit.edu/daed/article-abstract/151/2/218/110610

Gordon, T. F. (2013). *The pleadings game: An artificial intelligence model of procedural justice*. Springer Science & Business Media. https://books.google.com/books?hl=en&lr=&id=-PapCAAAQBAJ&oi=fnd&pg=PR9&dq=Theoretical+Framework:+Theories+of+Procedural+Justice+in+AI++&ots=7obUF5CWUM&sig=x8YW9YX6Pm_w7Nx8o1I7RvqPLYA

Guler, A., Kula, S., & Boke, K. (2025). Examining public support for AI in policing: The role of perceived procedural justice. *Police Practice and Research*, 1–23. https://doi.org/10.1080/15614263.2025.2516535

Doshi-Velez, F., Kortz, M., Budish, R., Bavitz, C., Gershman, S., O'Brien, D., Scott, K., Schieber, S., Waldo, J., Weinberger, D., Weller, A., & Wood, A. (2019). *Accountability of AI Under the Law: The Role of Explanation* (No. arXiv:1711.01134). arXiv. https://doi.org/10.48550/arXiv.1711.01134

Tatipamula, S. (2025). The ethics of AI decision-making: When should machines be accountable. *World Journal of Advanced Engineering Technology and Sciences*, *15*(1), 878–895. https://eprint.scholarsrepository.com/id/eprint/2839/*The Future of Jobs Report*. (2023). World Economic Forum. https://www.weforum.org/publications/the-future-of-jobs-report-2023/

Kashefi, P., Kashefi, Y., & Ghafouri Mirsaraei, A. (2024). Shaping the future of AI: Balancing innovation and ethics in global regulation. *Uniform Law Review*, *29*(3), 524–548. https://academic.oup.com/ulr/article-abstract/29/3/524/7904690

Buolamwini, J., & Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. Proceedings of the 1st Conference on Fairness, Accountability, and Transparency.

Zeng, Y., Lourentzou, I., Deng, X., & Jin, R. (2025). *FAIR: Facilitating Artificial Intelligence Resilience in Manufacturing Industrial Internet* (No. arXiv:2503.01086). arXiv. https://doi.org/10.48550/arXiv.2503.01086

Wordpress, 2U. (2021). How Artificial Intelligence Bias Affects Women and People of Color. *UCB-UMT*. https://ischoolonline.berkeley.edu/blog/artificial-intelligence-bias/

Raso, F. A., Hilligoss, H., Krishnamurthy, V., Bavitz, C., & Kim, L. (2018). Artificial intelligence & human rights: Opportunities & risks. *Berkman Klein Center Research Publication*, *2018–6*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3259344

Burnay, M. (2019). Privacy and surveillance in a digital era: Transnational implications of China's Surveillance State. *EUCROSS. Https://Ghum. Kuleuven. Be/Ggs/Research/Eucross/Eucross-Wp-Burnay-Oct2019. Pdf*. https://ghum.kuleuven.be/ggs/research/eucross/eucross-wp-burnay-oct2019.pdf

Mahmoudi, M. (2021). Ban dangerous facial recognition technology that amplifies racist policing. *Amnesty Intl (Jan. 26, 2021 8: 22AM) Https://Www. Amnesty. Org/En/Latest/Press-Release/2021/01/Ban-Dangerous-Facial-Recognitiontechnology-That-Amplifies-Racist-Policing*.

Obermeyer, Z., Powers, B., Vogeli, C., & Mullainathan, S. (2019). Dissecting racial bias in an algorithm used to manage the health of populations. *Science*. https://doi.org/10.1126/science.aax2342

Li, H., Moon, J. T., Shankar, V., Newsome, J., Gichoya, J., & Bercu, Z. (2024). Health inequities, bias, and artificial intelligence. *Techniques in Vascular and Interventional Radiology*, *27*(3), 100990. https://www.sciencedirect.com/science/article/pii/S1089251624000465

Kossow, N., Windwehr, S., & Jenkins, M. (2022). *Algorithmic transparency and accountability*. JSTOR. https://www.jstor.org/stable/pdf/resrep30838.pdf?refreqid=fastly-default%3A293411f4525078b1389aed0f71064f61&ab_segments=0%2Fbasic_search_gsv2%2Fcontrol&initiator=&acceptTC=1

Diakopoulos, N. (2020). Accountability, Transparency. *The Oxford Handbook of Ethics*

of AI, *17*(4), 197. https://books.google.com/books?hl=en&lr=&id=8PQTEAAAQBAJ&oi=fnd&pg=PA197&dq=Transparency+and+Accountability+in+AI+analysis+&ots=uDcDom14Zx&sig=5oFqK_Y52kmNcbMrRbClJSeEMx8

Maas, M. M. (2021). AI, Governance Displacement, and the (De) Fragmentation of International Law. *Available at SSRN 3806624*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3806624

Zaidan, E., & Ibrahim, I. A. (2024). AI governance in a complex and rapidly changing regulatory landscape: A global perspective. *Humanities and Social Sciences Communications*, *11*(1). https://www.nature.com/articles/s41599-024-03560-x

Lescrauwaet, L., Wagner, H., Yoon, C., & Shukla, S. (2022). Adaptive legal frameworks and economic dynamics in emerging technologies: Navigating the intersection for responsible innovation. *Law and Economics*, *16*(3), 202–220. https://journals.ristek.or.id/index.php/LE/article/view/61

Latonero, M. (2018). Governing artificial intelligence: Upholding human rights & dignity. *Data & Society*, *38*, 25. https://uatdoctorado.wordpress.com/wp-content/uploads/2025/02/datasociety_governing_artificial_intelligence_upholding_human_rights.pdf

Hogan, L., & Lasek-Markey, M. (2024). Towards a Human Rights-Based Approach to Ethical AI Governance in Europe. *Philosophies*, *9*(6), 181. https://www.mdpi.com/2409-9287/9/6/181

Scherer, M. U. (2015). Regulating artificial intelligence systems: Risks, challenges, competencies, and strategies. *Harv. JL & Tech.*, *29*, 353. https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/hjlt29&section=15

Nations, U. (2000). *Universal Declaration of Human Rights*. United Nations; United Nations. https://www.un.org/en/about-us/universal-declaration-of-human-rights

McKenzie, B. (2023). International: Can a global framework regulate AI Ethics. *Insight Plus*, *8*.

Zhou, J., Luo, F., Han, Y., Long, X., & Lyu, Y. (2025). Bibliometric Analysis on Ethic Consideration in Academic Publishing Based on WoS Core Collection. *Journal of Scholarly Communication*. https://ojs.inforvidor.com/index.php/jsc/article/view/31

Schmidt, J.-H., Bartsch, S. C., Adam, M., & Benlian, A. (2025). Elevating Developers' Accountability Awareness in AI Systems Development: The Role of Process and Outcome Accountability Arguments. *Business & Information Systems Engineering*, *67*(1), 109–135. https://doi.org/10.1007/s12599-024-00914-2

Meduri, K., Podicheti, S., Satish, S., & Whig, P. (2025). Accountability and transparency ensuring responsible AI development. In *Ethical Dimensions of AI Development* (pp. 83–102). IGI Global. https://www.igi-global.com/chapter/accountability-and-transparency-ensuring-responsible-ai-development/359639

Güven, Ç., Alishahi, A., Brighton, H., Nápoles, G., Olier, J. S., Šafář, M., Postma, E., Shterionov, D., Sisto, M. D., & Vanmassenhove, E. (2025). *AI in Support of Diversity and Inclusion* (No. arXiv:2501.09534). arXiv. https://doi.org/10.48550/arXiv.2501.09534

Shams, R. A., Zowghi, D., & Bano, M. (2025). AI and the quest for diversity and inclusion: A systematic literature review. *AI and Ethics*, *5*(1), 411–438. https://doi.org/10.1007/s43681-023-00362-w

Emma, L. (2024). The Ethical Implications of Artificial Intelligence: A Deep Dive into Bias, Fairness, and Transparency. *Retrieved from Emma, L.(2024). The Ethical Implications of Artificial Intelligence: A Deep Dive into Bias, Fairness, and Transparency*. https://www.researchgate.net/profile/Lawrence-

Li, H. (2025). *AI governance and human rights protection* [PhD Thesis]. https://repositories.lib.utexas.edu/items/6a34b5a0-1896-4284-a49d-1d993cd32ad1

Ahmad, R., Saleem, S., & Hussain, S. (2025). Ethical and Legal Challenges of Artificial

Intelligence: Implications for Human Right. *Journal of Law, Society and Policy Review*, *2*(01), 10–25. https://jlspr.uskt.edu.pk/index.php/Journal/article/view/29

Nyst, C., & Falchetta, T. (2017). The right to privacy in the digital age. *Journal of Human Rights Practice*, *9*(1), 104–118. https://academic.oup.com/jhrp/article-pdf/doi/10.1093/jhuman/huw026/16638245/huw026.pdf

Juliussen, B. A. (2025). The Right to an Explanation Under the GDPR and the AI Act. In I. Ide, I. Kompatsiaris, C. Xu, K. Yanai, W.-T. Chu, N. Nitta, M. Riegler, & T. Yamasaki (Eds.), *MultiMedia Modeling* (Vol. 15523, pp. 184–197). Springer Nature Singapore. https://doi.org/10.1007/978-981-96-2071-5_14

Abrusci, E., McGregor, L., Shaheed, A., Ng, V., Williams, C., Murray, D., & Kent, C. (2018). *The Universal Declaration of Human Rights at 70: Putting Human Rights at the heart of the design, development and deployment of artificial intelligence*. https://bura.brunel.ac.uk/bitstream/2438/23262/1/FullText.pdf

Aftab Haider, & Ayesha Sadiq. (2025). *CAN PAKISTAN REPLICATE CHINA'S ECONOMIC SUCCESS? KEY LESSONS FOR LONG-TERM GROWTH*.

Ahmad, I., Haider, A., & Afzal, J. (2024). The Geopolitical and Economic Impact of BRICS on the Middle East. *FWU Journal of Social Sciences*, *18*(4), 80–95. https://www.researchgate.net/profile/Aftab-Haider-3/publication/387663966_The_Geopolitical_and_Economic_Impact_of_BRICS_on_the_Middle_East/links/6776b2d0117f340ec3ee4829/The-Geopolitical-and-Economic-Impact-of-BRICS-on-the-Middle-East.pdf

Ahmad, J., & Haider, A. (2025). Firewall Technology Testing in Pakistan: The Fine Line Between National Security and Freedom of Expression. *Journal of Engineering, Science and Technological Trends*, *2*(1). https://journals.scopua.com/index.php/JESTT/article/view/11

Haider, A. (2024). Application of the United Nation Convention against Transnational Organized Crime: An Analysis. *Available at SSRN 4686710*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4686710

Haider, A., & Afzal, J. (2025). Understanding Cybersecurity Law in Data Sovereignty and Digital Governance by Melissa Lukings and Arash Habibi Lashkari. *International Journal of Law and Legal Advancement*, *1*(1). https://journals.scopua.com/index.php/IJLLA/article/view/41

Haider, A., Ahmad, I., & Gohar, M. (2023). Analyzing International Human Rights Law: Global Enforcement and Treaties. *INTERNATIONAL JOURNAL OF HUMAN AND SOCIETY*, *3*, 229–236. https://scholar.google.com/scholar?cluster=17065946018534265802&hl=en&oi=scholarr

Haider, A., Ali, A., & Zeb, B. (2024). *Broken laws, broken lives: When organized crime shreds human rights*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4751333

Haider, A., Ali, A., & Zubair, M. (2023). Chasing Dragons in the Dragon's Land: A Convoluted Struggle with Drugs and Deviance in Modern China. *Asketik J. Agama Dan Perubahan Sos*, *7*(2), 322–343. https://www.researchgate.net/profile/Aftab-Haider-3/publication/378365788_Chasing_Dragons_in_the_Dragon's_Land_A_Convoluted_Struggle_with_Drugs_and_Deviance_in_Modern_China/links/65d64a51adf2362b634b161d/Chasing-Dragons-in-the-Dragons-Land-A-Convoluted-Struggle-with-Drugs-and-Deviance-in-Modern-China.pdf

Haider, A., Al-Shibli, F. S., & Ahmad, I. (2026). Policy and Regulatory Landscape: A Legal Framework for the Regulation of Advanced Nano Biomaterials: Responsibility, Risk, Reflexivity. In *Sustainable Corrosion Inhibition: Nanobiotechnological Solutions and Challenges* (pp. 251–276). IGI Global Scientific Publishing. https://www.igi-global.com/chapter/policy-and-regulatory-landscape/397891

Haider, A., Fatima, A., & Batool, A. (2025). *The Human Rights Implications of Scientific Progress: A Case Study on Gene Editing and Disability Rights*.

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5267253

Haider, A., Raza, S., & Khan, B. Z. (2023). Organized Crime and the Objectives of the Islamic Penal System. *Al-Qamar*, 6(2), 63–82. https://www.alqamarjournal.net/index.php/alqamar/article/view/1269

Haider, A., Yousaf, U., Shah, N. H., & Azeem, W. (2024). UNTOC's Role in Combating Transnational Organized Crime: An International Response. *Pakistan JL Analysis & Wisdom*, *3*, 178. https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/pknjlolw3&section=183

Hui, Z., Haider, A., & Khan, A. (2025). International trade and plastic waste in oceans: Legal and policy challenges. *Frontiers in Marine Science*, *12*, 1627829. https://www.frontiersin.org/journals/marine-science/articles/10.3389/fmars.2025.1627829/full

Mathlouthi, N., Haider, A., Khan, A., & Ahmad, N. (2025). The role of Hainan Free Trade Port in shaping China's WTO commitments and international trade policies. *China and WTO Review*, *11*(1), 71–82. http://cwto.net/index.php/CWR/article/view/269

Strzępek, K. (2025). Convergence or Divergence? Balancing Regulatory Approaches in the Council of Europe AI Convention and the EU AI Act. *Rocznik Administracji Publicznej*, *11*(2), 351–368. https://www.ceeol.com/search/article-detail?id=1394840