ARTIFICIAL INTELLIGENCE, HUMAN RIGHTS AND THE WAY FORWARD

Abubakar Balarabe Kura*

Abstract

The rapid development of technology and the emergence of artificial intelligence have a significant impact on several aspects of human life. The impact permeates social interactions, healthcare, education, businesses and defence systems, among others. Fundamental human rights are inalienable rights that must be protected in all situations. Artificial intelligence systems, as machine decision-making entities, interact with humans, which poses a threat to the protection of their fundamental rights. This paper examines the complex and often contentious intersection between AI advancement and the protection of human dignity and liberties. Using the doctrinal research method, this paper explored the means by which a balance can be struck and appropriate measures taken to reduce human rights risks preemptively, and to develop effective mitigation measures. The key findings in the paper are that AI systems are inevitable in today's human life, and the system should be designed and regulated to prevent human rights abuse.

Keywords: Artificial Intelligence, Human rights, protection measures

* PhD, Faculty of Law, Northwest University, Kano. Email: Abkura@yumsuk.edu.ng

1. INTRODUCTION

Artificial intelligence (AI) has emerged as one of the most transformative technologies of the 21st century, permeating nearly every facet of human existence, from economic production and healthcare to governance and social interaction.[1] Its capacity for data analysis, pattern recognition, and autonomous decision-making offers immense potential to address some of humanity's most pressing challenges, promising advancements in medical diagnostics, resource management, and scientific discovery.[2] However, the same capabilities that drive this potential also introduce significant risks to the global human rights framework, a system of norms and laws established to protect the inherent dignity and fundamental freedoms of all individuals. The integration of AI into the societal fabric has created a critical juncture where the trajectory of technological innovation intersects, and often collides, with long-standing principles of justice, equality, and liberty.[3]

AI systems can be leveraged to enhance human rights, for instance, by analyzing satellite imagery to detect human rights abuses or by creating accessibility tools for persons with disabilities. On the other hand, the design and deployment of these systems present formidable challenges that

* A lecturer at Faculty of Law, Northwest University, Kano. Email: abkura@yumsuk.edu.ng

[1] Cataleta, M.S. and Anna, C. Artificial Intelligence and Human Rights: An Unequal Struggle. CIFILE Journal of International Law Journal Vol. 1, No. 2 (2020) 40-63.

[2] Moon, Li H, Purkayastha, J. T S., Celi, L. A., Trivedi, H., & Gichoya, J. W. Ethics of large language models in medicine and medical research. The Lancet Digital Health, 5(6), (22023)333–335.

[3] Bakeer, H., Alzamily, J., Almadhoun, H., & Abu-Nasser B. S, AI and Human Rights. *International journal of Academic Engineering Research* (2024)www.ijeais.org last visited on 17 September 2025

can undermine these very rights[4] Key areas of concern have rapidly come to the forefront of academic and policy discourse. The reliance of machine learning models on vast datasets often perpetuates and amplifies historical biases, leading to discriminatory outcomes in critical domains such as employment, criminal justice, and credit scoring, thereby infringing upon the fundamental right to non-discrimination. The expansion of AI-powered surveillance, including facial recognition and predictive policing, poses a direct threat to the right to privacy and can create a threat on freedom of expression and assembly.[5] Furthermore, the complexity of many advanced AI systems—often referred to as the "black box" problem—challenge the principles of transparency and accountability, making it difficult for individuals to understand, question, or seek redress for decisions that profoundly affect their lives.[6]

[4] Ahmad, R., Saleem, S., & Hussain, S. (2025) Ethical and Legal Challenges of Artificial Intelligence: Implications for Human Right. https://jlspr.uskt.edu.pk/index.php/Journal/article/view/29 last visited on 18 September 2025

[5] Sabah, A., Abu-Nasser, B., & Abu-Naser, S (2025). The Intersection of AI and Human Rights: Challenges and Opportunities (2025). https://philpapers.org/rec/SABTIO-9 last visited on 18 September 2025

[6] Black box AI models arrive at conclusions or decisions without providing any explanations as to how they were reached. As AI technology has evolved, two main types of AI systems have emerged: *black box AI* and *explainable* (or *white box*) *AI*. The term *black box* refers to systems that are not transparent to users. Simply put, AI systems whose internal workings, decision-making workflows, and contributing factors are not visible or remain unknown to human users are known as black box AI systems. The lack of transparency makes it hard for humans to understand or explain how the system's underlying model arrives at its conclusions. Black box AI models might also create problems related to flexibility (updating the model as needs change), bias (incorrect results that may offend or damage some groups of humans), accuracy validation (hard to validate or trust the results), and security (unknown flaws make the model susceptible to cyberattacks).

These challenges are not merely technical; they are deeply intertwined with social, ethical, and legal dimensions. The rapid and often unregulated deployment of AI technologies risks entrenching existing power imbalances and creating new forms of inequality, including a digital divide where access to the benefits of AI is unevenly distributed. The allocation of responsibility when an autonomous system causes harm remains a significant legal gray area, complicating efforts to ensure justice for victims.

This paper seeks to contribute to this vital discourse by providing a comprehensive examination of the intersection between AI and human rights. It navigates the multifaceted challenges posed by AI technologies and critically evaluates the emerging legal and policy responses designed to address them. Foundational regulatory efforts, such as the European Union's General Data Protection Regulation (GDPR)[7] have laid crucial groundwork for data protection in the AI era. Similarly, The Nigeria Data Protection Act (NDPA) (2023)[8] almost replicate the provisions of GDPR on data protection at the national level, while more recent, targeted legislation like the European Union AI Act signals a global shift towards risk-based regulation.[9] This paper will analyze and advocate for the adoption of a proactive, human-centric governance model. Such a model requires embedding human rights considerations directly into the design and development phases of AI systems, fostering robust multi-stakeholder

[7] Celso, Cancelo, Outeda, et al "The EU's AI Act: A Framework for Collaborative Governance", Internet of Things (2024) 2 Doi https://doi.org/10.1016/j.iot.2024.101291
[8] Nigeria Data Protection Act, 2023 https://ndpc.gov.org last visited on 6th May, 2025.
[9] Mauritz Kop, 'EU Artificial Intelligence Act: The European Approach to AI', Stanford-Vienna Transatlantic Technology Law Forum, issue No. 2 (2021) https://law.stanford.edu/publication last visited on 10th May, 2025.

collaboration, and implementing clear policy directives that prioritize human dignity and democratic values. This paper aims to inform the development of an AI ecosystem that is not only technologically innovative but also ethically sound, legally accountable, and fundamentally aligned with the protection and promotion of human rights for all.

2. CONCEPTUALIZATION OF ARTIFICIA INTELLIGENCE (AI) AND HUMAN RIGHTS

AI, like many other terms, lacks a universally accepted definition. UNESCO defines AI as "a system capable of processing data and information in a way that resembles human intelligence. These systems utilise algorithms and models to perform cognitive tasks, learn from data, make informed decisions and predictions, and plan effective actions. They include learning, reasoning, perception, and control.[10] AI was first credited to a scientist named John McCarthy in 1955, who defined it as, 'The science and engineering of making intelligent machines,[11] It has also been defined as the science of training machines to perform tasks that humans can do.[12] The European Union Artificial Intelligence Act has given a broader definition to AI, thus;

> A machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that for explicit or implicit objectives, infers, from the input it

[10] Shurooq Mnawer Ibrahim, et al, Artificial Intelligence Ethics: Ethical Consideration and Regulations from Theory to Practice," IAES International Journal of Artificial Intelligence, Vol 13, No 3 (2024) 3704

[11] Stanford University Human Centre Artificial Intelligence Definitions. htpps://hai.standard.edu/sites/defaults/files/2020/-09/AI-Definitions-//AI.pdf last visited on 25th April, 2025.

[12] F Marengo, Privacy and AI: Protecting Individuals in the Age of AI (Federico, Morengo 2023) 5

> receives, how to generate, outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.[13]

The Special Rapporteur on the Provision and Protection of the Right to Freedom of Opinion and Expression defines AI as;

> AI is often used as shorthand for the increasing independence, speed and scale connected to automated, computational decision–making. It is not one thing only, but rather refers to a "constellation" of processes and technologies enabling computers to complement or replace specific tasks otherwise performed by humans, such as making decisions and solving problems.[14]

The EU Act definition for AI is almost similar to the definition given by the Organization for Economic Cooperation and Development (OECD) and the Council of Europe Framework on AI and Human Rights, Democracy and Rule of Law.[15]

AI can be classified into different types depending on the criteria used for the classification. There is strong and weak AI. Weak AI is also called

[13] Art 3(1) EU AI Act
[14] Office of the High Commissioner on Human Rights, 'Report on the AI Technologies and implications for Freedoms and Information Environment' 73 session UN Doc/AI73/348 (29 Aug, 2018) para 3
[15] Art 1 OECD Recommendation of the Council on AI (2024) and Council of Europe, Framework Convention on Artificial Intelligence and Human Rights, Democracy and Rule of Law (2024)

narrow AI, which is trained to perform specific tasks.[16] Narrow AI limited its capability within the boundaries of the task given to it.[17]

Strong AI consists of Artificial General Intelligence (AGI) and Artificial Super Intelligence (ASI). The former is an AI with human-level intelligence, including self-awareness and the ability to solve issues, learn and plan for the future. An ASI would surpass human intelligence and the ability of the human brain.

Human rights can broadly be defined as the basic rights of human beings that is centered on equality, fairness, freedom, and respect for all. Human rights were succinctly defined by Kayode Eso J.S.C. (as he then was) in the case of *Ransome Kuti & ORS v. A.G Federation & ORS*[18] as thus:

> [Human rights] are rights that have always existed, even before orderliness prescribed rules for the manner they are to be sought. It is a primary condition to a civilized existence which stands above the ordinary laws of the land.

Human rights are the freedoms, liberties, immunities or benefits which, according to natural law, modern values and international law, all human beings are entitled to enjoy as a matter of right in the country or society in which they live.[19] Human rights are very fundamental to every human; a person cannot live without them. Human rights are what enable a person to

---

[17] Examples of the narrow AI include Apple Siri, Amazon Alexa and several other AI systems used to interact with people for specific tasks like customer service AI, legal research platforms, document review engine, etc.

[18] 1985) 2 NWLR

[19] Ese Malemi. The Nigerian Constitutional Law with Fundamental Rights (Enforcement Procedure) – Rules 2009. (Princeton Publishing Company, Lagos, 3rd Edition, 2017)

continue his humanity. Without human rights, life is meaningless, worthless and a mere shadow. To wit, human rights are too precious to be infringed upon without sufficient and convincing justification. In every country, there is a usual mandatory inclusion of human rights in the law of that land. For example, the 1999 Constitution of the Federal Republic of Nigeria (as amended), which is the grundnorm of Nigeria, has the fundamental human rights of her citizens embedded in it. [20]These rights are recognized as fundamental human rights, and are expected to be treated with utmost regard and serve as a basis of every policy of the government.

Several international laws make human rights sacrosanct, and their protection is inevitable for world peace and stability. For example, the Universal Declaration of Human Rights (UDHR) is one of the important documents that declared fundamental rights for humans and requested all states to protect these rights.[21] The Declaration was proclaimed by the United Nations General Assembly in Paris on 10 December 1948 as a common standard of achievements for all peoples and all nations,[22] International Covenant on Civil & Political Rights. The International Covenant on Civil and Political Rights (ICCPR) has its foundation in the Universal Declaration of Human Rights. The rights guaranteed by this covenant are the basic rights which are generally enforceable by instituting a judicial action in the legal system of democratic countries. At the regional

[20] Chapter 4 of the Constitution of the Federal Republic of Nigeria, 1999 as amended
[21] Ebad, R., Leila, R.D. & Mahmoud, J.K, 'Protection of Prisoner's Human Rights in Prisons through the Guidelines of Rule of Law', *Journal of Politics and Law,* Vol. 10, No. 1 (2017), <https://www.researchgate.net/publication/311972901_Protection_of_Prisoner%27s_Human_Rights_in_Prisons_through_the_Guidelines_of_Rule_of_Law> accessed 17 October 2021.
[22] Ibid.

level, the African Charter on Human & Peoples Rights. The African charter was adopted on the 27th June, 1981 and entered into force on the 21st October, 1986 and virtually all countries in Africa have ratified and domesticated the treaty into their own municipal laws.[23] The African Charter on Human and Peoples Rights, also called the Banjul Charter, was developed to promote the rights of individuals and peoples of Africa.[24]

3. INTERSECTION BETWEEN ARTIFICIAL INTELLIGENCE AND HUMAN RIGHTS

The rapid integration of artificial intelligence into the fabric of modern society presents a profound duality: while it offers unprecedented opportunities for progress and the enhancement of human well-being, it simultaneously introduces significant and complex threats to the enjoyment of fundamental human rights. This duality stems from the core functionalities of AI—its capacity to process vast datasets, identify patterns, and automate decisions at a scale and speed previously unimaginable. The deployment of these technologies across critical sectors such as justice, finance, healthcare, and security has created new vectors through which long-standing rights can be both promoted and undermined. The multifaceted impact of AI on fundamental human rights, focusing on three core areas of tension: the challenge of algorithmic bias to the right of non-discrimination; the erosion of privacy and civil liberties through advanced surveillance capabilities; and the systemic obstacles to transparency and accountability that opaque AI systems create. By dissecting these issues, we can better understand the nature of the risks involved and lay the

[23] Yusuf, D. 2011. The African Charter on Human and Peoples Rights: An Exposition Of Its Peculiarities And Dynamism. *Human Rights Review: An International Human Rights Journal*, Vol. 2, No.2, July, 2011. p.457.
[24] Ibid.

groundwork for developing robust, rights-preserving governance frameworks.

3.1 Right to non-Discrimination and AI

The principle of non-discrimination is a cornerstone of international human rights law, enshrined in foundational documents.[25] It guarantees that all individuals are to be treated with equal concern and respect, without distinction based on race, gender, religion, or other protected characteristics. However, the proliferation of AI systems in decision-making processes poses a systemic threat to this principle through the mechanism of algorithmic bias. AI algorithms, particularly those based on machine learning, can perpetuate and even amplify existing societal biases, leading to discriminatory outcomes that are often difficult to detect and contest.[26] This phenomenon arises not from malicious intent but from the very nature of how these systems are developed and the data upon which they are trained.

The primary source of algorithmic bias is the data used to train AI models. Machine learning systems learn to make predictions and classifications by identifying patterns in historical data. If this data reflects past discriminatory practices or societal inequalities, the AI model will

[25] Article 2(1), the International Covenant on Civil and Political Rights, Article 1, 2 and 7 Universal Declaration of Human Rights, Article 2 and 3 African Charter on Human and People's Rights, Section 42 Constitution of the Federal Republic of Nigeria, 1999 as amended.

[26] Polok, B., El Taj H., Rana A. A., (2023). Balancing Potential and Peril: the Ethical Implications of Artificial Intelligence on Human rights. https://www.academia.edu/download/107208670/11.pdf last visited on 21/9/2025

inevitably learn and reproduce these biases.[27] For instance, if an AI system for screening job applications is trained on a company's past hiring data, which may reflect a historical preference for male candidates in technical roles, the algorithm may learn to penalize applications from women, regardless of their qualifications. Similarly, AI models used in the criminal justice system for predicting recidivism have been shown to be biased against minority populations, often because the historical arrest and conviction data used for training is itself skewed by decades of biased policing and judicial practices. The result is a technological reinforcement of systemic discrimination, creating a feedback loop where biased predictions lead to actions that generate more biased data, further entrenching inequality.

Beyond biased data, the design choices made during an AI system's development can also introduce or exacerbate bias. The selection of features, the definition of success metrics, and the underlying assumptions encoded into the model's architecture can all contribute to inequitable outcomes. An algorithm designed to predict creditworthiness, for example, might use proxies for protected characteristics, such as postal codes, which can correlate with race or socioeconomic status, leading to discriminatory lending practices.[28] These technical decisions, often made without

[27] Hoxhaj, O., Halilaj, B., & Harizi, A (2023). Ethical Implications and Human Rights Violations in the Age of Artificial Intelligence, "*Balkan Social Science Review*." https://www.ceeol.com/search/article-detail?id=1207107 last visited on 21 September 2025

[28] Rayhan, R. & Rayhan, S. (2023). AI and Human Rights: Balancing Innovation and Privacy in the digital age. Comput. Sci. Eng. https://www.researchgate.net/profile/Rajan-Rayhan/publication/372743882_AI_and_Human_Rights_Balancing_Innovation_and_Privacy_in_the_Digital_Age/links/64c525b6cda2775c03d23cd4/AI-and-Human-Rights-Balancing-Innovation-and-Privacy-in-the-Digital-Age.pdf

sufficient consideration for their human rights implications, can translate abstract biases into concrete harms, denying individuals fair access to employment, housing, credit, and other essential opportunities.

The challenge of algorithmic bias is compounded by its scale and opacity. Unlike human decision-makers, whose biases can be questioned and challenged on an individual basis, a single biased algorithm can make millions of discriminatory decisions automatically and consistently. This automates discrimination at an unprecedented scale, making it a systemic rather than an individual problem. Furthermore, the complexity of many advanced AI models, often referred to as "black boxes," makes it exceedingly difficult to audit their internal logic and identify the precise source of a biased outcome.[29] This lack of transparency creates significant barriers for victims seeking to prove discrimination and for regulators attempting to enforce non-discrimination law, thus undermining the right to an effective remedy. Addressing this challenge requires a fundamental shift towards ethical AI development practices that prioritize fairness and equity from the outset.

3.2 Right to privacy, Civil Liberties and AI

The right to privacy is a fundamental human right, essential for protecting human dignity and the free development of personality. It has been

[29] Abiade, S. (2025). Artificial Intelligence Surveillance in Counterterrorism: Assessing Democratic Accountability and Civil Liberties Trade-offs. https://www.researchgate.net/profile/Sheriffdeen-Abiade/publication/393465948_Artificial_Intelligence_surveillance_in_counterterrorism_Assessing_democratic_accountability_and_civil_liberties_trade-offs/links/686bfe90e4632b045dca69e4/Artificial-Intelligence-surveillance-in-counterterrorism-Assessing-democratic-accountability-and-civil-liberties-trade-offs.pdf last visted on 21/9/2025

determined to be the right to be left alone; freedom from interruption, intrusion, embarrassment or accountability; control of the disclosure of personal information; protection of the individual's independence, dignity and integrity; secrecy, anonymity and solitude; the right to protection from intrusion into your personal life.[30] The right to privacy involves rules governing the collection and handling of personal data, the protection of physical autonomy, the right to limit access to oneself and the right to control one's identity. The international and national laws have safeguarded this right.[31] It underpins other civil liberties, including the freedoms of expression, association, and peaceful assembly. The advent of AI has, however, supercharged surveillance capabilities, creating new and pervasive threats to privacy and these associated freedoms.[32]

AI-powered technologies enable the collection, aggregation, and analysis of personal data on a massive scale, transforming previously disparate pieces of information into detailed profiles of individuals' lives, beliefs, and behaviours. This has profound implications for the balance of power between states, corporations, and individuals, potentially fostering an environment of control that chills democratic participation and dissent. The right to a private life is threatened by the constant tracking and surveillance that AI systems use for data collection. The lack of transparency about how AI systems operate creates uncertainty for individuals, whose data can reveal not only their interests but also their vulnerabilities. Consequently, an imbalance of power emerges. Companies possess extensive knowledge

[30] Law Teacher, 'The Right to Privacy' <https://www.lawteacher.net/free-law-essays/human-rights/right-to-privacy.php> last visited on 20 September, 2025.
[31] Article 17 the International Covenant on Civil and Political Rights, Section 37 of the Constitution of the Federal Republic of Nigeria, 1999 as amended.
[32] Op. cit Ahmad

about users, while users remain uncertain about how their data is used and whose interests it serves.[33]

One of the most prominent examples of AI-driven surveillance is the deployment of facial recognition technology in public spaces. These systems can identify and track individuals in real time, effectively eliminating anonymity in the public sphere. While proponents argue for their utility in law enforcement and national security, their use raises significant human rights concerns.[34] The constant monitoring of citizens can have a chilling effect on freedom of expression and assembly, as people may become hesitant to participate in protests, attend political meetings, or express dissenting views for fear of being identified and catalogued by the state. The potential for error and bias in these systems further exacerbates the risk, potentially leading to false identifications and wrongful accusations, disproportionately affecting marginalized communities.

Beyond facial recognition, AI enables subtler but equally invasive forms of surveillance. Predictive policing algorithms analyze historical crime data to forecast where and when future crimes are likely to occur, leading to heightened police presence in certain neighbourhoods, often those predominantly inhabited by minority groups. This can result in over-policing and reinforce existing biases within the justice system. Similarly, governments and corporations use AI to monitor online communications and social media for sentiment analysis, identifying potential threats or

[33] European Network for National Human Right Infiltaration Key human rights challenges of AI - ENNHRI last visited on 21/9/2025
[34] Op. cit Abiade

dissent.[35] While sometimes framed as necessary for counterterrorism or public safety, such practices constitute a significant intrusion into the private lives of individuals and can be used to suppress legitimate political opposition. The capacity of AI to analyze vast datasets means that even seemingly innocuous information, when aggregated, can reveal sensitive personal details, from political affiliations and religious beliefs to health conditions and sexual orientation.

The collection of massive datasets required to power these AI surveillance systems—often referred to as "big data"—is itself a major privacy concern. [36] Much of this data is collected without individuals' meaningful consent or full understanding of how it will be used. The business models of many technology companies are predicated on the extraction and monetization of personal data, creating a powerful economic incentive for ever-expanding data collection. This "surveillance capitalism" erodes individual autonomy and control over personal information, a key component of the right to privacy. The lack of robust data protection frameworks in many jurisdictions leaves individuals vulnerable to exploitation and manipulation. As AI's analytical capabilities continue to advance, the potential for these technologies to be used for social scoring, manipulation of public opinion, and widespread social control poses a direct threat to the foundations of democratic societies and the civil liberties they are meant to protect.

[35] Bajraktari, H. & Qatani, V. (2025). Artificial Intelligence a''Right''or''Violation''of Human Rights and Freedoms in the 21st Century. https://www.igi-global.com/chapter/artificial-intelligence-a-right-or-violation-of-human-rights-and-freedoms-in-the-21st-century/365942 last visited on 21/9/2025

[36] Op. cit, Polok

4. AI REGULATORY FRAMEWORKS TO CURB HUMAN RIGHTS ABUSE

The rapid integration of Artificial Intelligence into the fabric of society has presented one of the most significant governance challenges of the modern era, compelling nations and international bodies to develop new legal and regulatory frameworks.[37] As AI systems increasingly mediate access to essential services and opportunities, their potential to undermine fundamental human rights has spurred a global dialogue on the necessity of robust oversight.[38] This has catalyzed a shift from abstract ethical principles to concrete regulatory proposals, with a growing consensus that any effective governance model must be built upon a solid foundation of human rights and the rule of law. In this complex and evolving landscape, policymakers are grappling with how to foster innovation while simultaneously erecting safeguards against the harms of algorithmic bias, pervasive surveillance, and opaque decision-making. The ensuing efforts have produced a diverse array of national strategies and international initiatives, reflecting different legal traditions, economic priorities, and societal values. At the forefront of this regulatory push, the European Union

[37] Maras, Marie-Helen, and Alex Alexandrou. (2019) "Determining Authenticity of Video Evidence
in the Age of Artificial Intelligence and in the Wake of Deepfake Videos." *International Journal
of Evidence & Proof 23, no. 3: 255–62 https://doi.org/10.1177/1365712718807226 last visited on 22/9/2025*

[38] Miazi, M., (2023) Interplay of legal frameworks and artificial intelligence (AI): A global perspective. Law and Policy Review. https://www.researchgate.net/profile/Md-Abu-Nayem-Miazi/publication/379955489_Interplay_of_Legal_Frameworks_and_Artificial_Intelligence_AI_A_Global_Perspective/links/662345aaf7d3fc28747035d8/Interplay-of-Legal-Frameworks-and-Artificial-Intelligence-AI-A-Global-Perspective.pdf

has emerged as a key standard-setter, first through its landmark data protection regulation and more recently with its ambitious, sector-spanning legislation specifically targeting AI. Examining these pioneering frameworks and comparing them with other global approaches provides crucial insights into the future direction of AI governance and the ongoing struggle to align technological advancement with human dignity.

Long before AI-specific legislation became a primary focus of global regulatory efforts, the European Union's General Data Protection Regulation (GDPR), enacted in 2018, established a foundational framework that has profoundly shaped the governance of data-driven technologies, including artificial intelligence. While not an AI regulation per se, the GDPR's comprehensive approach to data protection created a set of principles and obligations that directly address many of the human rights risks inherent in AI systems. Its influence extends far beyond the EU, setting a de facto global standard and providing a blueprint for subsequent AI-specific policies.[39] The core of the GDPR's relevance to AI lies in its principles-based approach to the processing of personal data, which is the lifeblood of most modern AI applications. Principles such as data minimization, purpose limitation, and storage limitation impose crucial constraints on the indiscriminate collection and use of data for training algorithms. More significantly, the regulation grants individuals a suite of enforceable rights that serve as a critical check on automated power. The right to access, the right to rectification, and the right to erasure empower individuals to exert a degree of control over their data, while the right to object to certain types of processing provides a mechanism to challenge its

[39] About 144 countries across the world have passed data protection laws. www.iapp.org/news/data-protection-laws last visited on 3rd May, 2025.

use. Article 22 establishes a qualified right for individuals not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.[40] This provision directly confronts the challenge of autonomous AI decision-making in high-stakes domains such as credit scoring, employment, and social benefit allocation. While subject to exceptions, it enshrines the principle of human oversight and provides individuals with the right to obtain human intervention, express their point of view, and contest the decision. This right is complemented by obligations of transparency, requiring data controllers to provide meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. These requirements were pivotal in advancing the conversation around AI governance, pushing developers and deployers of AI systems to consider issues of explainability and fairness from the outset.[41]

Furthermore, the GDPR's robust definition of personal data, including its extension to online identifiers and inferred data, brings many AI-driven analytical processes within its scope.[42] Its stringent requirements for processing "special categories" of personal data—such as data revealing racial or ethnic origin, political opinions, or health information—are

[40] EU General Data Protection Regulations https://gdpr-info.eu last visited on 22/9/2025. Similarly, Sections 27(1) g and 37 of the Nigeria Data Protection Act (NDPA) 2023 provide and mandate a data controller to inform a data subject of the existence of automated decision making and profiling. It further stated that automated decision making or profiling includes an automated decision necessary for entering into or the performance of a contract between a data subject and a data controller.
[41] Fessenko, D. & Jasperse, A. 2025). Ethics at the Heart of AI Regulation. AI and Ethics. https://link.springer.com/article/10.1007/s43681-024-00562-y last visted on 22/9/2025
[42] Article 4 GDPR

particularly salient given that AI systems trained on such data pose heightened risks of discrimination and other rights violations. By mandating a higher standard of protection for sensitive data, often requiring explicit consent, the GDPR provides a legal bulwark against some of the most pernicious applications of AI.

The regulation also introduced the concept of "Data Protection by Design and by Default,"[43] obligating organizations to build data protection measures into their processing activities and business practices from the design stage. Similarly, the requirement for Data Protection Impact Assessments (DPIAs)[44] for high-risk processing activities forces organizations to systematically identify, assess, and mitigate data protection risks before a system is deployed. This risk-based methodology has proven to be a highly influential model for subsequent AI-specific regulations, which often adopt a similar approach to managing AI-related harms. The significant impact of the GDPR on AI is undeniable; it has forced organizations worldwide to re-evaluate their data handling practices and has provided a robust legal framework for challenging AI-driven harms related to data privacy.[45]

Building on the foundation laid by the GDPR, the European Union has continued its pioneering role in technology regulation with the introduction of the Artificial Intelligence Act (AI Act).[46] This proposal represents one of

[43] Ibid Article 25
[44] Ibid Article 35
[45] Mukherjee, B. (2025). Navigating AI Governance: National and International Legal and Regulatory Frameworks. https://www.igi-global.com/chapter/navigating-ai-governance/382021. Last visted on 22/9/2025
[46] Tambiama Madiega, 'Artificial Intelligence Act: Overview,' European Parliamentary Research Service (2024)

the world's first and most comprehensive attempts to create a horizontal legal framework specifically for AI. Moving beyond data protection, the AI Act aims to establish a harmonized set of rules for the development, placement on the market, and use of AI systems within the Union. Its central organizing principle is a risk-based approach, which categorizes AI applications based on their potential to cause harm to health, safety, and fundamental human rights. This methodology seeks to strike a balance between fostering innovation and ensuring that AI development remains aligned with democratic values, human rights and the rule of law.[47]

The AI Act's framework stratifies AI systems into four distinct risk categories: unacceptable risk, high risk, limited risk, and minimal risk. This classification determines the level of regulatory scrutiny and the specific obligations imposed on developers and users. At the highest level, the Act proposes an outright ban on AI systems deemed to present an "unacceptable risk"[48] to human rights. This category includes applications that have a high potential for manipulation or exploitation of vulnerable groups, such as social scoring systems used by public authorities and AI that deploys subliminal techniques to distort behavior in a manner likely to cause physical or psychological harm. The prohibition of these systems signals a strong normative stance that certain uses of AI are fundamentally incompatible with the EU's core values.

The most extensive and detailed regulations are reserved for "high-risk" AI systems. Article 6 describes and identifies the number of cases in which AI

[47] Lund, B., Orhan, Z., Mannuru, N., Bevara, R., & Porter, B. (2025). Standards, Frameworks, and Legislation for Artificial Intelligence (AI) Transparency. AI and Ethics. https://link.springer.com/article/10.1007/s43681-025-00661-4
[48] Article 5 EU AI Act

systems are to be considered high risk because they can potentially create an adverse impact on people's health, safety or their fundamental rights. Before the AI systems are put into use or placed in areas considered to be high risk, a conformity assessment procedure must be run to ensure the system is free from danger.[49] This category encompasses AI intended for use in critical areas where significant rights are at stake. The Act identifies several such domains, including biometric identification, the management of critical infrastructure, education and vocational training, employment and workers management, access to essential public and private services (such as credit scoring and welfare), law enforcement, migration and border control, and the administration of justice. Providers of these high-risk systems are subject to a stringent set of ex-ante compliance obligations. These requirements include establishing robust risk management systems, using high-quality data sets to minimize risks of bias and discrimination, maintaining detailed technical documentation, ensuring human oversight is possible, and meeting high standards of accuracy, robustness, and cybersecurity.

For AI systems classified as "limited risk," the Act focuses primarily on transparency obligations. This category includes systems that interact with humans, such as chatbots, and AI used to generate or manipulate content, like deepfakes. Users must be clearly informed that they are interacting with an AI system or that the content they are viewing is artificially generated, enabling them to make informed decisions and exercise critical judgment. Finally, for the vast majority of AI applications deemed to pose "minimal

[49] Mauritz Kop, 'EU Artificial Intelligence Act: The European Approach to AI', Stanford-Vienna Transatlantic Technology Law Forum, issue No. 2 (2021) https://law.stanford.edu/publication last visited on 10th May, 2025.

or no risk,"[50] such as AI-enabled video games or spam filters, the Act imposes no new legal obligations, allowing innovation in these areas to proceed unhindered. This risk-based structure is designed to avoid over-regulation while concentrating compliance efforts where the potential for societal harm is greatest.

The EU AI Act represents a significant evolution in AI governance, moving from the data-centric focus of the GDPR to a broader consideration of AI as a cross-sectoral technology with diverse impacts. It explicitly aims to create an ecosystem of trust where citizens can be confident that AI technology is used safely and in compliance with fundamental rights.[51]

5. THE DIVIDING LINE AND CROSSROAD

The challenges posed by the rapid advancement of artificial intelligence to the foundational principles of human rights are significant and multifaceted. As detailed in the preceding sections, issues of algorithmic bias, pervasive surveillance, and decision-making systems threaten to erode fundamental rights like the right to non-discrimination, the right to privacy, and due process. However, these challenges are not insurmountable. The path forward requires a deliberate and proactive shift in protecting human rights without jeopardizing AI and technological development. This approach is not about stifling innovation but about steering it in a direction that is aligned with democratic values, ethical principles, and the rule of law.[52] A

[50] Article 53 and 54 AI Act

[51] Cole, M (2024). AI Regulation and Governance on a Global Scale: An Overview of International, Regional and National Instruments. Journal of AI Law and Regulation. https://scholar.archive.org/work/gwbfan6uovdfze364zqqn42ksu/access/wayback/https://aire.lexxion.eu/data/article/19406/pdf/aire_2024_01-017.pdf last visited on 22/9/2025

[52] Cole, M. (2024) AI Regulation and Governance on a Global Scale: An Overview of International, Regional and National Instruments. Journal of AI Law and Regulation.

human-centric model is employed, which is predicated on the idea that technology must serve humanity, enhancing dignity and protecting human rights rather than diminishing them. It requires a comprehensive strategy that integrates human rights considerations into every stage of the AI lifecycle, fosters robust collaboration among all societal actors, and establishes clear, enforceable policies that balance technological progress with fundamental human protections. The balance could be achieved through: integrating human rights by design and implementing specific policy recommendations to ensure AI development is both responsible and equitable.

The principle of "Human Rights by Design" represents a fundamental paradigm shift in the development and deployment of AI systems. It moves beyond compliance checks to a proactive methodology where the protection of human rights is an integral component of the entire AI lifecycle, from initial conception and data collection to model training, deployment, and ongoing monitoring. This approach mandates that developers, engineers, and organizations consider the potential human rights impacts of their technologies as a core design requirement, equivalent in importance to functionality, efficiency, and marketability. By embedding ethical considerations and human rights principles into the very architecture of AI systems, this model aims to prevent harms before they occur, rather than merely attempting to remedy them after the occurrence.[53]

https://scholar.archive.org/work/gwbfan6uovdfze364zqqn42ksu/access/wayback/https://aire.lexxion.eu/data/article/19406/pdf/aire_2024_01-017.pdf last visited on 29/9/2025

[53] Almeida, P. D., Santos, C. D., & Farias, J. (2021) Artificial Intelligence Regulation: a Framework for Governance. https://link.springer.com/article/10.1007/s10676-021-09593-z last visited on 29/9/2025

A critical first step in implementing Human Rights by Design is the mandatory execution of Human Rights Impact Assessments (HRIAs) before the development of any high-risk AI system. Similar to environmental impact assessments, HRIAs would provide a structured process for systematically identifying, predicting, and evaluating the potential effects of an AI application on human rights. This process would require developers to explicitly map the system's intended functions and potential unintended consequences against established international human rights frameworks. For instance, a predictive policing algorithm would need to be assessed for its potential to infringe on the right to non-discrimination, freedom of movement, and the presumption of innocence. The assessment should be a transparent and participatory process, involving input from affected communities, civil society organizations, and human rights experts to ensure a comprehensive evaluation of risks. The findings of the HRIA should then directly inform the design, development, and deployment decisions, including the implementation of specific mitigation measures or, in cases of unacceptable risk, the decision to halt the project altogether.

Finally, meaningful human oversight must be architected into AI systems from the outset, ensuring that autonomous technologies remain under ultimate human control. This principle rejects technological determinism and asserts that final accountability for critical decisions must rest with human agents. In practice, "human-in-the-loop" systems ensure that a person is directly involved in the decision-making process, such as a doctor reviewing an AI's diagnostic suggestion before confirming a diagnosis. "Human-on-the-loop" systems allow AI to operate autonomously but with

human supervision and the ability to intervene and override the system if necessary, which is critical for safety-critical applications like autonomous vehicles. "Human-in-command" approaches, particularly relevant for lethal autonomous weapons systems, maintain that the ultimate decision to apply force must always be made by a human. Integrating these levels of oversight by design ensures that AI systems function as tools to augment human capabilities rather than replace human judgment and moral responsibility in contexts where fundamental rights are at stake.

6. FINDINGS

From the totality of the research, it's crystally clear that technological advancement and artificial intelligence development are inevitable in today's life. World has moved several miles ahead with such developments. However, innovation and development should not be at the expense of human rights. Protecting human rights is core in depending democratic values so that a balance could be created.

Several AI systems affected human rights protection such as right to non-discrimination and right to privacy and family life.

7. CONCLUSION

The integration of artificial intelligence into the fabric of society represents a pivotal moment in human history, offering unprecedented opportunities for progress while simultaneously presenting profound challenges to the universal principles of human rights. The tension between the drive for technological advancement and the imperative to protect human dignity is not a zero-sum game, but rather a complex dynamic that demands careful and continuous navigation. This paper has examined the impact of AI on fundamental rights, highlighting how algorithmic bias, pervasive

surveillance, and a lack of transparency can undermine non-discrimination, privacy, and accountability. It has also surveyed the evolving landscape of global governance, recognizing the foundational role of frameworks like the GDPR and the EU AI Act in establishing a risk-based and rights-conscious approach to regulation. The analysis underscores a clear consensus: unchecked AI development poses a direct threat to the legal and ethical pillars of democratic societies, necessitating a coordinated and principled response.

The path forward requires a decisive shift towards a human-centric governance model, one that embeds human rights considerations into the very DNA of technological innovation. This is not a call to halt progress but a call to steer it with purpose and foresight. The model sets the principle of "Human Rights by Design" and standard practice, mandating that developers proactively assess and mitigate rights-based risks throughout the entire AI lifecycle.