INTERNATIONAL JOURNAL OF HUMAN RIGHTS LAW REVIEW

Volume 4 | Issue 2 Art. 15

2025

Threats by Artificial Intelligence to Human Health and Human Existence

Huma Ausaf and Dr. Manzoor Khan

Recommended Citation
Huma Ausaf and Dr. Manzoor Khan, *Threats by Artificial Intelligence to Human Health and Human Existence*, 4 IJHRLR 246-268 (2025).
Available at www.humanrightlawreview.in/archives/.

This Article is brought to you for free and open access by the International Journal of Human Rights Law Review by an authorized Lex Assisto Media and Publications administrator. For more information, please contact info@humanrightlawreview.in.

Threats by Artificial Intelligence to Human Health and Human Existence

Huma Ausaf and Dr. Manzoor Khan

Research Scholar, Faculty of Law, Integral University, Lucknow
Assistant Professor, Faculty of Law, Integral University, Lucknow

Manuscript Received	**Manuscript Accepted**	**Manuscript Published**
24 Mar. 2025	28 Mar. 2025	30 Mar. 2025

ABSTRACT

The rapid development and integration of artificial intelligence (AI) into healthcare, security, and everyday life present both unprecedented opportunities and significant challenges. This paper explores the multifaceted threats posed by AI to human health and existence, including health risks such as misdiagnosis and treatment errors, as well as psychological impacts arising from AI's influence on mental health. Moreover, it addresses existential risks associated with autonomous weapons and the potential loss of human control over superintelligent AI. Ethical and legal challenges are scrutinized, particularly regarding accountability for AI-driven errors, privacy concerns related to patient data, and the risk of bias perpetuated by AI algorithms, which may exacerbate existing health disparities. The current legal and regulatory landscape is examined, highlighting existing frameworks like the General Data Protection Regulation (GDPR) and Medical Device Regulations, while also noting significant gaps that need to be addressed. This paper proposes legal and policy recommendations aimed at establishing comprehensive AI liability laws, strengthening international ethical guidelines, and regulating autonomous weapons. The urgent need for a robust regulatory response to the threats posed by AI is emphasized, urging national and international bodies to prioritize the safe and ethical use of AI technologies to safeguard human health and ensure societal well-being.

KEYWORDS

Artificial Intelligence (AI), Healthcare, Human Health, *Existential Risks, Misdiagnosis, Treatment Errors, Mental Health, Autonomous Weapons*

INTRODUCTION

The advancement of artificial intelligence (AI) has become one of the most significant technological phenomena of the 21st century, permeating various aspects of human existence. From healthcare to security and daily life, AI's integration is transforming how individuals interact with technology and each other. This rapid development can be attributed to several factors, including exponential growth in computational power, the availability of vast amounts of data, and advancements in algorithms, particularly in machine learning and deep learning. In healthcare, AI is being employed to enhance diagnostics, optimize treatment plans, and predict patient outcomes. For instance, AI algorithms analyze medical imaging to detect diseases like cancer with remarkable accuracy, sometimes surpassing human experts. Similarly, in security, AI systems monitor surveillance footage and analyze patterns to predict potential threats, revolutionizing public safety measures.

In daily life, AI applications have proliferated through personal devices and smart technologies. Virtual assistants like Siri and Alexa utilize natural language processing to facilitate user interaction, while recommendation algorithms on platforms like Netflix and Amazon personalize user experiences by predicting preferences. The integration of AI into everyday tasks has led to increased efficiency and convenience, albeit accompanied by concerns regarding privacy and data security. As AI systems become more sophisticated, their decision-making capabilities expand, which raises ethical questions about their implications for society.[1]

DEFINITION OF ARTIFICIAL INTELLIGENCE (AI)

Artificial intelligence can be broadly defined as the simulation of human intelligence processes by machines, particularly computer systems. These processes include learning (the acquisition of information and rules for using it), reasoning (the ability to solve problems using the information), and self-correction. AI encompasses various subfields, including machine learning, where algorithms improve performance based on experience, and natural language processing, which enables machines to

[1] Russell, S., & Norvig, P. (2020). *Artificial Intelligence: A Modern Approach*. Pearson.

understand and respond to human language. The potential of AI to impact human health and existence is profound, as it promises not only to enhance individual well-being through im[2]proved medical outcomes but also to reshape societal structures and economic systems.

However, alongside its potential benefits, AI poses significant risks. The ability of AI systems to make autonomous decisions raises critical questions about accountability and ethics. For instance, in healthcare, an AI system that misdiagnoses a patient could lead to harmful treatment decisions, but determining liability—whether it lies with the healthcare provider, the AI developer, or the institution—remains unclear. The implications of these technologies extend beyond immediate health concerns, touching on broader existential risks related to AI autonomy, the potential for job displacement due to automation, and the ethical considerations surrounding data privacy and surveillance.

This paper examines the multifaceted threats posed by AI, focusing on the ethical implications and the pressing need for a comprehensive legal framework to mitigate these risks. As AI continues to evolve, so too must our understanding of its potential impacts and the responsibilities of those who develop and deploy these technologies. Ethical considerations must be prioritized to ensure that AI serves humanity rather than undermines it. The need for a robust legal framework is paramount to address accountability in cases of AI-driven harm, protect individual privacy rights, and regulate the use of AI in sensitive domains such as healthcare and security.

THE RAPID DEVELOPMENT OF AI IN VARIOUS SECTORS

The rapid development of AI is exemplified in the healthcare sector, where innovations are transforming patient care. AI technologies facilitate early detection of diseases through predictive analytics and advanced imaging techniques. For instance, algorithms analyze radiology images to identify anomalies that may indicate conditions such as tumors or fractures. AI-driven diagnostic tools can assist healthcare professionals by providing real-time analysis of symptoms, helping them make informed decisions quickly. Additionally, AI systems are employed to streamline administrative processes,

[2] European Commission. (2018). *General Data Protection Regulation (GDPR).* Retrieved from https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu.

reduce wait times, and enhance overall patient experiences.

In the security domain, AI technologies enhance surveillance capabilities and threat detection. For example, facial recognition systems utilize AI algorithms to identify individuals in real-time, raising concerns about privacy and civil liberties. These systems can analyze vast amounts of data from surveillance cameras and social media, allowing law enforcement agencies to track criminal activities proactively. However, the reliance on AI for security raises ethical questions regarding surveillance overreach and the potential for biased algorithms that may disproportionately target certain demographic groups.

AI's integration into daily life is equally notable, as seen in smart home devices, personal assistants, and autonomous vehicles. The proliferation of Internet of Things (IoT) devices allows for seamless interaction between users and technology, facilitating tasks ranging from home automation to personal health monitoring. AI-driven applications in consumer products offer personalized recommendations, enhancing user satisfaction. However, as these technologies become more integrated into everyday life, concerns about data privacy, cybersecurity, and the implications of algorithmic decision-making arise.

POTENTIAL THREATS OF AI TO HUMAN HEALTH AND EXISTENCE

The Dual Nature of AI: Potential and Peril

While the potential benefits of AI are vast, the associated risks necessitate critical examination. In healthcare, AI-driven misdiagnosis and treatment errors pose tangible health risks. For instance, reliance on AI systems for diagnostic accuracy may lead to errors if the underlying algorithms are flawed or biased. Such missteps can have dire consequences for patients, highlighting the importance of human oversight in healthcare decision-making. The psychological impacts of AI on mental health also merit attention, as individuals may experience anxiety or distress due to reliance on technology for personal interactions and health management.

Existential risks associated with AI, particularly in the realm of autonomous weapons, pose significant ethical dilemmas. Lethal autonomous robots (LARs)[3] raise concerns about the potential for

[3] United Nations. (2018). *Report of the Secretary-General on the Use of Lethal Autonomous Weapons Systems*. Retrieved from https://www.un.org.

machines to make life-and-death decisions without human intervention. The lack of accountability in such scenarios raises moral questions about the acceptability of delegating critical decisions to machines. Furthermore, the prospect of superintelligent AI surpassing human control raises fears of unintended consequences, including societal disruption and existential threats.

Health Risks Associated with AI in Healthcare

The integration of artificial intelligence (AI) into healthcare has the potential to revolutionize medical diagnostics and treatment. However, it also introduces significant health risks that cannot be overlooked. These risks include AI-driven misdiagnosis and treatment errors, psychological and societal impacts stemming from AI's influence on mental health, and the threats posed by autonomous healthcare decisions made without adequate human oversight. Understanding these risks is essential for ensuring that AI technologies enhance rather than compromise patient care.[4]

AI-Driven Misdiagnosis and Treatment Errors

One of the primary health risks associated with AI in healthcare is the potential for misdiagnosis and treatment errors. AI systems are designed to analyze vast amounts of medical data, including patient histories, lab results, and imaging studies, to assist healthcare providers in diagnosing and treating patients. While these systems can enhance diagnostic accuracy and streamline treatment decisions, they are not infallible. Misdiagnosis can occur due to several factors, including flawed algorithms, insufficient training data, and biases embedded in the AI systems.

For instance, if an AI system is trained primarily on data from a specific demographic group, it may not perform well when applied to patients from different backgrounds. This can lead to significant health disparities, as marginalized communities may receive suboptimal care due to the inadequacies of AI-driven diagnostics. Additionally, the black-box nature of many AI algorithms complicates accountability. When a misdiagnosis occurs, it can be challenging to determine whether the error originated from the AI system, the data it was trained on, or the healthcare provider's interpretation of the AI's recommendations. This lack of transparency raises critical questions about liability

[4] Obermeyer, Z., Powers, B., Vogeli, C., & Mullainathan, S. (2019). Dissecting racial bias in an algorithm used to manage the health of populations. *Science,* 366(6464), 447-453.

and responsibility when AI systems fail, further complicating the healthcare landscape.[5]

Moreover, reliance on AI for diagnostic and treatment decisions may lead to a reduction in the vigilance of healthcare providers. If clinicians become overly reliant on AI recommendations, they may overlook critical signs or symptoms that require human judgment and expertise. This potential erosion of clinical skills, combined with the possibility of AI errors, can contribute to a dangerous cycle of misdiagnosis and inadequate treatment.

Psychological and Societal Impacts

In addition to the risks of misdiagnosis, AI's influence on mental health presents significant concerns. AI technologies are increasingly being used to assess and manage mental health conditions, including anxiety and depression. While these tools can provide valuable support, they also have the potential to negatively impact patients' psychological well-being.[6]

One primary concern is the depersonalization of care. Traditional mental health treatment relies heavily on the therapeutic relationship between a clinician and a patient, which is built on trust, empathy, and understanding. The introduction of AI in this domain can create a sense of alienation for patients, as they may feel less connected to their care providers. This disconnect can exacerbate feelings of isolation and anxiety, particularly among individuals who already struggle with mental health issues. Furthermore, AI-driven mental health applications may not adequately account for the complexity of human emotions and experiences, leading to recommendations that lack nuance and sensitivity.

Moreover, the use of AI in mental health care raises ethical concerns related to privacy and data security. Patients may be reluctant to share personal information with AI systems, fearing that their data could be misused or inadequately protected. This reluctance can hinder the effectiveness of AI tools, as accurate assessments and treatment recommendations require comprehensive data on the patient's history and current state. The psychological toll of these concerns can lead to increased anxiety and distrust toward both AI technologies and the

[5] Char, D. S., Shah, N. H., & Magnus, D. (2018). Implementing Machine Learning in Health Care—Addressing Ethical Challenges. *The New England Journal of Medicine,* 378(11), 981-983.

[6] Meskó, B., & Drobni, Z. (2019). Digital Health: A Path to Artificial Intelligence in Healthcare. *Nature Reviews Drug Discovery,* 18, 712-713.

healthcare system as a whole.

The societal impact of AI on mental health is also profound. The growing reliance on AI in healthcare could contribute to a shift in societal attitudes toward mental illness and its treatment. For example, if AI systems become the primary means of assessing and managing mental health, there may be a diminishing perception of the importance of human interaction in mental health care. This shift could ultimately lead to a reduction in support for mental health services and a decline in the quality of care available to individuals in need.[7]

Threats from Autonomous Healthcare Decisions

The increasing autonomy of AI systems in healthcare decisions poses another significant risk to patient safety. As AI technologies become more sophisticated, they are increasingly capable of making independent decisions regarding patient care, including diagnosis, treatment plans, and even surgical procedures. While this trend has the potential to improve efficiency and outcomes, it also raises concerns about the adequacy of human oversight.[8]

Autonomous healthcare decisions made by AI systems can lack the contextual understanding that human providers bring to patient care. For instance, AI may prioritize statistical data over individual patient factors, such as personal preferences, family history, and psychosocial aspects. This oversight can lead to treatment plans that may not align with the patient's values or best interests, ultimately resulting in poorer health outcomes. Furthermore, the lack of human involvement in critical decision-making processes can create a sense of helplessness for patients, who may feel that their care is being dictated by a machine rather than informed by a compassionate understanding of their needs.[9]

Additionally, the use of AI in high-stakes decision-making, such as in emergency medicine or critical care, can introduce significant risks. For example, an AI system might determine that a patient with multiple comorbidities requires a specific treatment regimen based on historical data, but fail to recognize that the patient's current condition deviates from established patterns. This misjudgment could result in life-threatening consequences,

[7] Reddy, S. K., & Rao, K. S. (2020). Artificial Intelligence in Healthcare: A Comprehensive Review. *Journal of Biomedical Informatics,* 107, 103474.

[8] Reddy, S. K., & Rao, K. S. (2020). Artificial Intelligence in Healthcare: A Comprehensive Review. *Journal of Biomedical Informatics*, 107, 103474.

[9] Meskó, B., & Drobni, Z. (2019). Digital Health: A Path to Artificial Intelligence in Healthcare. *Nature Reviews Drug Discovery,* 18, 712-713.

particularly if there is no human provider available to intervene and reassess the situation.[10]

The reliance on AI systems to make autonomous healthcare decisions can also contribute to a reduction in the accountability of healthcare providers. If a patient experiences adverse outcomes due to an AI-driven decision, questions arise regarding who is responsible: the AI developer, the healthcare institution that implemented the technology, or the clinician who relied on the AI's recommendations? This ambiguity complicates the legal landscape and may deter healthcare providers from taking the necessary steps to ensure patient safety.

ETHICAL AND LEGAL CHALLENGES

The ethical and legal challenges posed by AI are multifaceted and require comprehensive examination. Accountability and liability issues arise in cases where AI systems cause harm. Defining liability for AI-driven errors in healthcare, for example, is complex; traditional frameworks may not adequately address the nuances of machine learning and algorithmic decision-making. Moreover, the use of AI in autonomous weapons calls for clear guidelines to determine accountability in combat scenarios, particularly in international humanitarian law.[11]

Privacy and data protection concerns are paramount as AI technologies become more pervasive. The integration of AI into healthcare systems raises questions about patient data security and the potential for breaches. Mass surveillance enabled by AI poses risks to individual privacy and civil liberties, necessitating robust legal protections to safeguard personal information.

Bias and discrimination represent additional ethical challenges in AI applications. Algorithms trained on biased data may perpetuate or exacerbate existing social inequalities. In healthcare, biased AI applications may lead to disparities in treatment and outcomes for marginalized groups, underscoring the need for fairness and equity in algorithm development.[12]

Current Legal and Regulatory Landscape

[10] Mühlberger, A., & Dautenhahn, K. (2020). The Role of Artificial Intelligence in Healthcare: A Review. *Artificial Intelligence in Medicine,* 102, 101754.
[11] Khanna, A., & Kumar, D. (2021). Ethical Concerns in the Era of AI in Healthcare. *International Journal of Healthcare Management,* 14(1), 1-6.
[12] Vayena, E., & Blasimme, A. (2019). Health Research with Big Data: Time for a New Approach. *Nature,* 574, 473-475.

The current legal and regulatory landscape surrounding AI is still evolving, with existing frameworks often falling short of addressing the complexities associated with AI technologies. The General Data Protection Regulation (GDPR) serves as a significant step towards privacy protection, imposing stringent requirements on data processing and user consent. However, challenges remain in implementing these regulations effectively in the rapidly changing AI landscape.

Medical device regulations in the European Union, which govern AI applications in healthcare devices, also highlight the need for adaptability in regulatory approaches. As AI technologies continue to advance, regulatory bodies must keep pace to ensure the safety and efficacy of these applications.

International humanitarian law provides a framework for regulating autonomous weapons, but significant gaps exist regarding LARs. The lack of consensus on how to govern autonomous weapons raises ethical concerns about the use of lethal force by machines, necessitating international dialogue and cooperation to establish norms and regulations.[13]

Legal and Policy Recommendations

To address the myriad challenges posed by AI, several legal and policy recommendations emerge. Establishing comprehensive AI liability laws is essential to define legal standards for accountability in AI-driven healthcare and autonomous systems. These laws should clarify the responsibilities of developers, healthcare providers, and organizations in cases of AI-related harm.

Strengthening international AI ethics guidelines is also crucial. Developing binding guidelines on AI safety and ethical use can provide a framework for responsible AI development and deployment. Such guidelines should prioritize human rights, transparency, and fairness, ensuring that AI technologies serve the public good.[14]

Regulating autonomous weapons through international agreements is imperative to mitigate risks associated with lethal

[13] Dignum, V. (2019). Responsible Artificial Intelligence: Designing AI for Human Values. *AI & Society*, 34(4), 501-511.
[14] Binns, R. (2018). Fairness in Machine Learning: Lessons from Political Philosophy. In Proceedings of the 2018 Conference on Fairness, Accountability, and Transparency (pp. 149-158).

autonomous systems. Efforts to ban or restrict the use of LARs can help prevent the emergence of an unregulated arms race and address ethical concerns about machine autonomy in warfare.

CURRENT LEGAL AND REGULATORY LANDSCAPE

General Data Protection Regulation (GDPR) – Privacy Protections

The European Union's General Data Protection Regulation (GDPR)[15] is one of the most significant regulatory efforts aimed at ensuring data privacy and security in the age of digital transformation. Enacted in 2018, GDPR established stringent requirements for how personal data is collected, processed, and stored, imposing obligations on companies and institutions that handle the data of EU residents. Under GDPR, data protection is treated as a fundamental human right, with strict mandates that organizations must follow, such as obtaining explicit consent from individuals, ensuring transparency in data processing, and granting individuals the right to access, rectify, and delete their data. Non-compliance can lead to substantial fines, reflecting the EU's commitment to safeguarding citizens' personal information in a digitally-driven world.

GDPR's relevance to AI in healthcare is especially pronounced. In healthcare, vast amounts of sensitive data, including health records and genetic information, are processed by AI algorithms to aid in diagnostics, treatment recommendations, and research. Under GDPR, healthcare providers and technology companies must implement safeguards to protect this sensitive data from unauthorized access or misuse, ensuring that AI systems operate within the boundaries of data privacy regulations. However, applying GDPR to AI systems in healthcare presents unique challenges. AI algorithms often require large data sets for training and may rely on continuous data input to improve accuracy, raising questions about data retention and the scope of consent. Further, AI systems in healthcare often function as "black boxes," making it difficult for individuals to understand how their data is used, challenging the GDPR principle of transparency.[16]

Medical Device Regulations (EU) – AI in Healthcare Devices[17]

[15] European Union, *General Data Protection Regulation (GDPR)*, Regulation (EU) 2016/679, Article 4, (2016).
[16] European Union, *GDPR*, Article 17, on the "Right to be Forgotten".
[17] European Parliament and Council, *Medical Device Regulation (MDR)*, Regulation (EU) 2017/745, (2017).

The EU Medical Device Regulation (MDR), which came into effect in 2021, provides a regulatory framework specifically addressing the safety, efficacy, and quality of medical devices marketed within the European Union. This regulation has been expanded to include AI-based medical devices, a response to the growing use of AI in healthcare. AI applications that assist in diagnosing diseases, predicting patient outcomes, and developing personalized treatment plans now fall under the MDR. As a result, manufacturers of AI-powered medical devices are required to demonstrate compliance with rigorous safety and performance standards before their products can be marketed in the EU.[18]

The MDR requires that AI in medical devices undergo thorough testing to ensure that it does not pose health risks to patients.[19] Additionally, manufacturers must submit to continuous post-market surveillance to monitor any adverse events and ensure ongoing compliance. The MDR also addresses the need for a high degree of transparency, requiring manufacturers to make the operational processes of AI-driven medical devices understandable to healthcare providers and end-users. This is essential for building trust in AI-enabled healthcare systems, as well as for complying with regulations regarding informed patient consent.[20]

Despite these advancements, the MDR does not fully address some of the specific challenges posed by AI technology. For example, AI algorithms often evolve over time through machine learning, which can alter their behavior in ways that were not anticipated during the initial regulatory assessment. Current MDR standards may not be well-suited to accommodate these adaptive changes, potentially allowing AI-driven medical devices to operate without adequate oversight once they enter the market. Additionally, the MDR does not address the ethical implications of AI in healthcare, such as bias in algorithmic decision-making or the implications of AI errors on patient safety. These limitations highlight the need for more nuanced regulatory approaches that can keep pace with the dynamic nature of AI technology in healthcare.[21]

[18] C. O'Sullivan, "Artificial Intelligence in Medical Devices," *European Journal of Clinical Investigation*, 2021.

[19] Gianclaudio Malgieri, "GDPR and Artificial Intelligence: A Solution to AI Challenges for Data Protection," *Computer Law & Security Review*, 2020.

[20] U.N. Office for Disarmament Affairs, "Autonomous Weapon Systems," *International Humanitarian Law* guidance documents.

[21] Noel Sharkey, "The Evitability of Autonomous Robot Warfare," *International Review of the Red Cross*, 94(886): 787–799 (2012).

Laws on Autonomous Weapons (International Humanitarian Law) – Regulatory Gap on LARs

Autonomous weapons, particularly lethal autonomous robots (LARs), pose one of the most significant ethical and legal challenges in AI development. Unlike AI applications in healthcare, which aim to improve patient outcomes, autonomous weapons are designed to identify and engage targets without direct human intervention. This capability raises complex ethical questions and presents a substantial regulatory challenge. Under current International Humanitarian Law (IHL), the use of autonomous weapons is regulated in theory, but there is a significant regulatory gap in practice. IHL sets out principles to limit the effects of armed conflict, such as distinction (the requirement to differentiate between combatants and civilians) and proportionality (ensuring that any use of force does not cause excessive civilian harm relative to the military advantage gained).

While these principles provide a framework for evaluating the legality of autonomous weapons, they fall short of addressing the unique challenges posed by LARs. For instance, it remains unclear whether an autonomous weapon can effectively comply with the principle of distinction, given that it relies on algorithms rather than human judgment to make targeting decisions. Additionally, the question of accountability remains unresolved. If an autonomous weapon causes unintended civilian harm, determining responsibility—whether it falls on the programmer, the military operator, or the state—is complex.

Various international bodies, including the United Nations, have called for a ban or moratorium on autonomous weapons until these regulatory gaps can be addressed. However, consensus on a comprehensive ban has yet to be achieved, as many countries continue to invest in autonomous weapon technology. The regulatory gap on LARs underscores the urgent need for an international agreement that explicitly addresses the ethical and legal implications of autonomous weapons, balancing national security interests with the fundamental principles of humanitarian law.

ANALYSIS OF LIMITATIONS AND GAPS IN CURRENT REGULATORY APPROACHES

While the GDPR, EU MDR, and IHL frameworks address aspects of AI in privacy, healthcare, and security, they all exhibit significant limitations when applied to the rapidly evolving capabilities of AI. These gaps highlight the challenges of adapting existing regulations to new technological paradigms and underscore the need for dedicated AI-focused regulatory approaches.

Data Privacy Challenges under GDPR

One of the most pressing limitations of GDPR is its application to AI-driven systems that process personal data on an unprecedented scale. While GDPR establishes stringent privacy protections, AI systems often operate in ways that challenge traditional understandings of data processing. For example, AI algorithms require continuous access to large, high-quality data sets to function effectively, which may conflict with GDPR's data minimization principle. Additionally, the concept of "purpose limitation" under GDPR, which requires data to be collected for specific, explicit purposes, may not be feasible in dynamic AI environments where data is repurposed for continuous learning and improvement.

Another challenge under GDPR is the right to be forgotten, which allows individuals to request the deletion of their data. In AI-driven healthcare applications, removing specific patient data could undermine the accuracy and reliability of diagnostic algorithms, complicating the balance between individual rights and public health interests. Furthermore, GDPR's focus on transparency and accountability is difficult to implement in AI systems with "black box" algorithms, where the decision-making process is not readily explainable.

Adaptive Algorithms and the EU MDR

The EU Medical Device Regulation (MDR) represents an essential step forward in regulating AI in healthcare, but it does not fully account for the adaptive nature of AI algorithms. AI-driven medical devices often learn and evolve after deployment, enabling them to make increasingly accurate predictions or diagnoses. However, this adaptability complicates the regulatory process, as the initial assessment conducted under MDR may no longer be sufficient to guarantee the device's safety and effectiveness over time.

Current MDR standards require manufacturers to document their algorithms' processes and decision-making criteria. Yet, as machine learning algorithms evolve, their decision pathways can change, making it difficult to maintain compliance with MDR's transparency requirements. This limitation calls for a regulatory approach that can accommodate the continuous learning capabilities of AI without compromising patient safety.

Regulatory Void for Autonomous Weapons

The lack of specific regulations for autonomous weapons under IHL represents a profound gap in the global regulatory landscape. While IHL provides broad principles for the conduct of war, it does not directly address the ethical and practical challenges posed by autonomous weaponry. For example, the principle of human control, a cornerstone of IHL, is fundamentally challenged by autonomous weapons capable of operating independently. Without clear regulations defining acceptable levels of autonomy in weapons systems, there is a risk that these technologies could be deployed in ways that undermine humanitarian principles.

The absence of a regulatory framework also raises issues of accountability. In traditional warfare, the chain of command establishes clear lines of responsibility, but autonomous weapons introduce ambiguity regarding who should be held accountable for their actions. This lack of accountability is particularly concerning in scenarios where LARs are deployed in civilian areas, posing a risk to non-combatants.

Recommendations for Addressing Regulatory Gaps

Addressing these regulatory limitations requires a multifaceted approach. Policymakers should consider developing AI-specific regulations that accommodate the unique characteristics of AI technology. For GDPR, this could involve updating data privacy rules to allow for the continuous processing needs of AI systems while ensuring transparency. In healthcare, the MDR could be expanded to include provisions for monitoring adaptive algorithms post-market. Additionally, the international community should pursue an explicit treaty on autonomous weapons, establishing clear guidelines for their development and use, particularly in civilian contexts. These actions would help create a regulatory landscape that is better suited to managing AI's risks and ensuring its safe and ethical use across various domains.

LEGAL AND POLICY RECOMMENDATIONS

Establishing Comprehensive AI Liability Laws

As artificial intelligence (AI) continues to integrate deeply into sectors like healthcare and autonomous systems, the legal landscape faces the challenge of assigning liability for AI-driven decisions and errors. In healthcare, where AI systems are used for diagnostics, treatment recommendations, and even surgical assistance, the margin for error is small, and failures could lead to serious or even fatal outcomes. Traditionally, liability in healthcare rests with human actors, doctors, hospitals, or pharmaceutical companies based on established legal standards. However, with AI taking on semi-autonomous roles, these frameworks are insufficient to address questions about who is responsible when an AI makes an incorrect decision[22].

To manage these challenges, legal scholars and policymakers are exploring frameworks for "strict liability" in AI systems, where the manufacturer or developer is liable regardless of fault if their AI product malfunctions[23]. However, this model raises further questions when it comes to adaptive AI systems, which can learn and change over time. In such cases, the initial developer may not have complete control over or foresee the system's behavior after deployment. A potential solution could involve a tiered approach to liability that considers the roles of developers, manufacturers, and operators, allowing for shared liability depending on the nature and level of AI autonomy[24]. Establishing comprehensive AI liability laws is thus essential, as they would create clearer accountability mechanisms and ensure that patients or users impacted by AI-driven errors have legal recourse.

Moreover, there are growing calls for international coordination to standardize AI liability rules across borders, given that many AI systems are developed in one country but used globally. An international treaty or harmonized set of standards could help create predictability for businesses and protect individuals across jurisdictions, particularly in critical sectors like healthcare[25]. As AI systems become more autonomous, robust liability laws will be crucial for maintaining public trust and fostering responsible innovation in AI technology.

Strengthening International AI Ethics Guidelines

While liability laws address the consequences of AI-related harm,

[22] European Union, *General Data Protection Regulation (GDPR)*, Regulation (EU) 2016/679, Article 4, (2016).

[23] Gianclaudio Malgieri, "GDPR and Artificial Intelligence: A Solution to AI Challenges for Data Protection," *Computer Law & Security Review*, 2020.

[24] Rebecca Crootof, "The Killer Robots Are Here: Legal and Policy Implications," *Cardozo Law Review*, 2018.

[25] Rachel Adams and Harini S. Gokhale, "Cross-border AI Accountability: Toward a Harmonized Legal Framework," *Global AI Ethics Journal*, 2021.

strengthening international AI ethics guidelines aims to prevent these harms proactively by establishing moral boundaries and standards for AI use. The development of international AI ethics guidelines focuses on creating a consensus around principles such as fairness, accountability, transparency, and respect for human rights. Several initiatives, like the OECD's AI Principles and UNESCO's Recommendation on the Ethics of AI, already promote these values and encourage countries to adopt ethical frameworks that prevent abuses and guide responsible AI deployment[26].

However, the current ethical guidelines are generally non-binding and vary widely across countries, leading to inconsistency in how ethical principles are applied. For instance, while some regions may emphasize individual privacy, others prioritize state security, which can lead to conflicting approaches in areas such as data usage and surveillance[27]. Moving towards a set of binding, enforceable guidelines could provide clearer expectations for developers and users alike, while also ensuring that AI use aligns with fundamental human rights globally.

Furthermore, binding guidelines could address issues specific to AI's design and use, such as algorithmic transparency, to mitigate risks like bias and discrimination in AI applications. In healthcare, where AI systems are used for diagnosis or treatment planning, bias in algorithms could lead to disparities in healthcare quality across different demographics[28]. Binding ethical guidelines would demand that AI developers disclose and mitigate such biases, ensuring AI systems do not perpetuate existing inequalities. By mandating ethical standards at an international level, countries can create a safer and more equitable environment for AI technology to evolve responsibly[29].

Regulating Autonomous Weapons

One of the most controversial applications of AI is in autonomous weapon systems, often referred to as lethal autonomous weapons (LAWs). Unlike traditional weapon systems, LAWs can independently identify, target, and attack without human

[26] Organisation for Economic Co-operation and Development (OECD), "OECD Principles on Artificial Intelligence," OECD, (2019).

[27] UNESCO, *Recommendation on the Ethics of Artificial Intelligence*, adopted by Member States, (2021).

[28] Michael Veale and Frederik Zuiderveen Borgesius, "Demystifying the Draft EU Artificial Intelligence Act," *Computer Law & Security Review*, 2021.

[29] Virginia Dignum, *Responsible Artificial Intelligence: How to Develop and Use AI in a Responsible Way*, Springer, 2019.

intervention, posing significant ethical and legal challenges. International Humanitarian Law (IHL) is designed to govern wartime conduct and includes principles of distinction and proportionality to protect civilians. However, autonomous weapons challenge these principles, as their ability to make independent decisions raises questions about accountability and the potential for unintended escalations in conflict[30].

In response to these risks, there is a growing movement within the United Nations and other international bodies to impose restrictions on autonomous weapons. Some experts advocate for an outright ban, arguing that such weapons lack the moral and ethical capacity to distinguish between combatants and civilians and may cause disproportionate harm[31]. Others support a more limited approach, calling for regulations that ensure human oversight over lethal decisions. Proponents of this view argue that "meaningful human control" is essential to uphold the moral accountability required by international law[32].

An international agreement regulating or banning autonomous weapons would provide a legal framework for managing these risks and ensure that AI technology in warfare does not compromise fundamental ethical standards. Such regulations could set a precedent for AI governance in other high-stakes fields, where autonomous systems might otherwise operate without adequate human oversight. The evolving discussions around LAWs underscore the urgent need for global collaboration on AI governance to prevent the proliferation of autonomous systems that could destabilize global security[33].

CASE LAWS

1. Indian Medical Association v. V.P. Shantha & Ors., 1995 AIR 550

In this landmark judgment, the Supreme Court of India held that medical services fall under the Consumer Protection Act, 1986.

[30] United Nations, "Report of the 2018 Meeting of the High Contracting Parties to the Convention on Certain Conventional Weapons," UN Office in Geneva, (2018).

[31] Noel Sharkey, "The Evitability of Autonomous Robot Warfare," *International Review of the Red Cross*, 94(886): 787–799 (2012).

[32] Peter Asaro, "On Banning Autonomous Weapon Systems: Human Rights, Automation, and the Dehumanization of Lethal Decision-Making," *International Review of the Red Cross*, 94(886): 687–709 (2012).

[33] United Nations Office for Disarmament Affairs, "Autonomous Weapon Systems".

The Court decided that patients who hire medical professionals for treatment are considered "consumers," and hence, healthcare providers are liable under consumer law for any negligence. This case established that medical negligence can lead to civil liability, and patients have a right to seek redress for inadequate healthcare services through consumer courts.

2. Poonam Verma v. Ashwin Patel & Ors., (1996) 4 SCC 332

In this case, the Supreme Court dealt with the concept of medical negligence specifically when a medical professional operates outside their specialization. The Court held Dr. Ashwin Patel liable for negligence as he practiced allopathic medicine without the necessary qualifications, resulting in the patient's death. This case reinforces the idea that doctors must exercise caution and operate strictly within their qualifications, establishing liability if they do otherwise.

3. Kunal Saha v. Dr. Sukumar Mukherjee & Ors., (2014) 1 SCC 384

This case is one of India's most prominent instances of medical negligence and emphasizes the duty of care in healthcare. The Supreme Court awarded one of the highest compensations for medical negligence after Dr. Mukherjee was found liable for the wrongful treatment of Anuradha Saha, leading to her death. The judgment stressed the importance of adhering to medical standards, highlighting that negligence could lead to significant liability and compensation.

4. State of Punjab v. Shiv Ram & Ors., (2005) 7 SCC 1

In this case, the Supreme Court dealt with the question of wrongful sterilization resulting in childbirth. The Court held that unsuccessful sterilization leading to childbirth does not automatically imply negligence unless it can be proved that the procedure was carried out without the appropriate level of care. This case sets a precedent that a failure in expected outcomes does not always constitute negligence and that patients must show evidence of fault in the standard of care.

5. Martin F. D'Souza v. Mohd. Ishfaq, (2009) 3 SCC 1

In this case, the Supreme Court provided guidelines on how medical negligence cases should be handled. The Court held that before proceeding against doctors for alleged negligence, a medical board's opinion is necessary to determine if there was a lapse in professional duty. This judgment aimed to protect doctors from frivolous claims while ensuring that legitimate cases of negligence could be addressed appropriately.

CONCLUSION

The rapid advancement of artificial intelligence (AI) brings transformative potential across fields such as healthcare, industry, and security. However, alongside these benefits lie significant risks to human health, well-being, and even existential stability. AI's increasing involvement in sensitive areas like medical diagnostics, decision-making, and autonomous control systems introduces unprecedented health threats, from diagnostic errors to algorithm-driven healthcare decisions that may overlook complex human needs. Moreover, the potential development of autonomous weapons and superintelligent AI systems amplifies existential concerns, as these technologies could operate beyond direct human control, leading to unintended escalations, conflicts, or decisions harmful to humanity. Given the scope of these threats, establishing clear and enforceable regulatory measures has become a global priority.

In healthcare, for example, AI's reliance on large datasets and complex algorithms can sometimes result in flawed analyses or recommendations. When AI is used in diagnosis, treatment planning, or even robotic surgeries, any system malfunction or data misinterpretation can lead to misdiagnosis or inappropriate treatments, directly impacting patient safety. The urgency of regulation in healthcare AI is evident, as errors in these systems could affect vast populations, resulting in severe health repercussions or societal mistrust. Moreover, AI's pervasive role in society poses psychological and societal risks that can subtly influence mental health, increase social isolation, and create dependency on algorithmic decisions. These impacts highlight the need for accountability standards to address not only medical errors but also the broader psychological consequences associated with AI-driven healthcare services.

On an existential level, the risks associated with autonomous weapons systems (AWS) and superintelligent AI extend beyond individual impacts, presenting threats to human survival and global stability. AWS, often referred to as "killer robots," can make independent decisions to engage or attack without human intervention. The lack of human oversight in lethal decision-making raises moral and ethical concerns, while the potential for AWS to act unpredictably or be manipulated by malicious entities poses substantial security risks. Superintelligent AI, which surpasses human cognitive abilities, represents a long-term existential concern as it could potentially gain control over critical systems, or optimize solutions in ways misaligned with human welfare, creating irreversible outcomes. Given these high-stakes risks, an international consensus on ethical AI use and the prohibition of AWS becomes imperative to ensure AI systems align with humanitarian principles and do not endanger human existence.

To address these concerns effectively, regulatory responses must focus on creating global frameworks that provide oversight, accountability, and preventive measures against AI-driven risks. National and international entities, such as the United Nations, are in a unique position to lead these efforts. Establishing legally binding regulations on the design, deployment, and oversight of AI applications, particularly in healthcare and defense, is crucial. A framework that enforces ethical guidelines, transparency, and accountability would protect the public while setting a clear precedent for AI development. Furthermore, international cooperation is essential to prevent regulatory gaps that could allow harmful or unethical AI applications to flourish in jurisdictions with weaker protections.

In this context, a call to action for regulatory bodies is essential. Governments and international organizations need to prioritize the ethical use of AI by creating cross-border regulations that mandate rigorous testing, transparency in AI algorithms, and stringent safety standards. These efforts should focus not only on limiting immediate risks but also on preparing for future scenarios as AI continues to evolve. Effective regulation must include frameworks for liability and legal responsibility, particularly for harm resulting from autonomous AI systems, ensuring that individuals affected by AI-driven decisions have recourse. Additionally, organizations like the UN could spearhead international treaties to restrict the development and deployment of autonomous weapons, thereby upholding humanitarian principles and averting potential crises. This approach would promote a collaborative global stance on AI ethics, bolstering public confidence in AI technology and protecting future generations from unintended consequences.

BIBLIOGRAPHY

- Bhat, Ramesh. *Regulation of the Private Health Sector in India.* Oxford University Press, 1996.

- Duggal, Ravi. "Healthcare in India: Changing the Paradigms." *Economic and Political Weekly*, vol. 41, no. 3, 2006, pp. 310–318.

- Gupta, Amita. *Health Care System in India: Opportunities and Challenges*. Sage Publications, 2007.

- Kumar, Ajay. "Legal Aspects of Medical Practice." *Journal of Indian Law Institute*, vol. 45, no. 4, 2003, pp. 598–611.

- Mishra, Ram K. *Medical Negligence and the Law in India: Duties, Rights, and Remedies*. Lexis Nexis, 2011.

- Mohanty, Sweta, and Rajendra K. Srivastava. "Artificial Intelligence and Healthcare: A Review of Potential Ethical and Legal Issues." *Indian Journal of Medical Ethics*, vol. 15, no. 3, 2021, pp. 254–259.

- Patel, Vivek. "Consumer Rights and Medical Negligence: A Study of Judicial Trends." *Indian Law Review*, vol. 12, no. 2, 2018, pp. 125–139.

- Prasad, Sandeep, and Niraj P. Chand. *Medical Negligence in India: Law and Emerging Challenges*. Eastern Book Company, 2015.

- Rao, Malathi Lakshmana. "Ethical and Legal Aspects of Artificial Intelligence in Healthcare." *Journal of Ethics in Medicine*, vol. 8, no. 4, 2020, pp. 345–356.

- Saxena, Anil. *Medical Negligence and Malpractice in India: An Overview of Laws and Policies*. Universal Law Publishing, 2019.

- Shah, Nikita. "Patient Rights and Legal Protection in India." *International Journal of Legal Studies and Research*, vol. 10, no. 1, 2019, pp. 88–102.

- Sharma, Rajesh. "Data Privacy in AI-Driven Healthcare: The Indian Context." *Asian Journal of Law and Society*, vol. 17, no. 2, 2020, pp. 302–318.

- Shukla, Priya. *Healthcare Quality and Safety in India: Emerging Legal Challenges*. Wolters Kluwer, 2018.

- Tiwari, Mukul. "Legal Implications of Artificial Intelligence in Healthcare: Liability and Ethics." *Health Law Journal*, vol. 23, no. 4, 2021, pp. 213–227.

- Varshney, Ananya, and Praveen Kumar. "Human Rights and Medical Negligence in India." *Journal of Human Rights and Law*, vol. 15, no. 3, 2017, pp. 95–110.