Page 563 - 570 **DOI:** *https://doij.org/10.10000/IJLMH.115423*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 6 | Issue 4

2023

AI's Impact on Law and Human Rights: Gaps, Challenges, and Vulnerabilities

AKRITI SANJAY GUPTA[1]

ABSTRACT

This article addresses the gaps and obstacles in the legal and human rights issues surrounding machine learning (AI), as well as how these issues have an impact on basic human rights concepts. These problems include: algorithmic openness, cybersecurity weaknesses, unfairness, bias, and prejudice, lack of contestability, problems with legal personhood, problems with intellectual property, negative effects on workers, problems with privacy and data protection, liability for harm, and lack of responsibility. The article uses the concept of 'vulnerability' to help readers understand significant areas of concern and to direct risk and impact mitigation actions to safeguard people's well-being. This article advances the discussion, which is crucial, while appreciating the good work done in the field of AI legislation and the fact that it requires continual examination and agility in approach.

Keywords: *Artificial intellect (AI)Legal concerns vulnerability Rights of humanity.*

I. INTRODUCTION

According to Boden (2016), machine learning (AI)1 is present everywhere, and its use, research, and deployment are all progressing quickly and boosting the world economy. Increases in creativity, services, safety, and lifestyles are only a few of the many benefits of AI, but it also generates a lot of worries and concerns due to its possible adverse impacts on individual liberty, anonymity, and basic liberties (OECD 2019).

The legal debate on the ethical and human rights implications of artificial intelligence (AI) is well-established, and many specific concerns have undergone in-depth legal study (as described in this article's Sections 3 and 4). Although this industry is a changing target in terms of regulation, there is a need for an investigative, aerial perspective, and selective look at the range of challenges. A more thorough examination and mapping of sensitivity to such problems is also seriously lacking. Based on investigation done for the EU-funded SIENNA project under Horizon 2020, this article fills this gap.

The primary research inquiries for this essay are: What are the ethical and legal concerns with

[1] Author is a student at Symbiosis Law School, Pune, India.

 [ISSN 2581-5369]

AI? How are they being dealt with? What are the problems and gaps?

(A) Structure, strategy, approach, and scope

Following a brief summary of the protection of legal and ethical issues (Section 3), this article outlines specific legal issues related to AI that are currently under discussion (Section 4), solutions that have been proposed or how they are being implemented, deficiencies and difficulties, and affected human rights principles (Section 5). It connects the legal concerns to basic rights worldwide and offers illustrations of related human rights concepts that may be impacted on a global and regional scale. More importantly, it examines legal problems through the lens of 'vulnerability' (Section 6) to help better unify the identification of what are essential areas of concern and help direct AI dangers and effects mitigation efforts to safeguard individual and society well-being. Considering AI's growing installation and use, the seriousness of its effects on people and their fundamental rights, and the excellent work that is already being done in the AI law time (as evident in the research identified in this article), this strengthened examination of the issues anticipates to further provide insights and add to the essential demand for more and experienced debates on this topic.

Issues were only included if they had been discussed, were frequently raised, had an impact on cultural norms and daily life, and were contentious. This study's time constraints and reliance on English-language sources of research were two of its limitations. Additionally, while each of these topics may be examined more thoroughly separately (e.g., by looking into the applicable legal requirements), this is outside the purview of this study and in numerous instances has been or is being done by other scholars.

We searched the main global rights-related documents for treatment of such concerns in order to connect legal concerns to principles in those treaties. The General Declaration of Human Rights (UDHR), the Charter of the UN, the UN Covenant on Civil and Political Rights (ICCPR), the Worldwide Covenant on the Rights of the Economy, Society, and Culture (ICESCR), the Convention on the Prohibition or Limits on the Use of certain Conventional Weapons which may be regarded as to be Overly detrimental or to Have Indiscriminate Impacts (and Protocols), and the European Convention for the safeguarding of People Rights were among them.

We used a law-in-context method to map the recognised AI legal challenges to the most susceptible populations and the elements that determine and/or enable susceptibility. By reading the material that was examined in the matter identification process and reinforced with an online search for more examples, the susceptible categories and elements that affect vulnerability were discovered and determined. The table is not thorough and will alter when examined in various

 [ISSN 2581-5369]

situations.

Economic and rights-related problems are covered.

The European Parliament (2017, 2018a, 2018b, 2019, 2020a, 2020b, 2020c), the European Commission (2018a, 2018b, 2020), the European Order for the improvement of justice (CEPEJ) (2018), and the European Data Protection Supervisor (2016) all have policy papers that address legal and rights-related gives on a global scale.

The covering of legal problems relating to AI by academia and civil society (Access Now 2018; Privacy International and Article 19 2018) can be extensive and encompass a range of hazards and difficulties. Sometimes they address very particular topics. Domain-specific analyses exist.

Aspects including liability (Mitchell 2019), fairness in decision-making (Niiler 2019), bias (Marr 2019), privacy (Lindsey 2018), and responsibility (Coldewey 2018) have all been covered in further detail in the media coverage of AI legal concerns. Particularly, concerns about bias (Dave 2018) and privacy/data protection (Meyer 2018; Williams 2019; Forbes Insights Team 2019; Lohr 2019) have drawn a lot of attention.

II. AI LEGAL AND HUMAN RIGHTS CONCERNS

The relevance of each issue, proposed remedies (or how it is being tackled), gaps and obstacles that surround it are all briefly discussed in this section. This is a brief study; other studies have critically examined and analysed each of these concerns in depth; the goal here is to give a comprehensive, current summary and make it useful for future studies.

The 10 challenges listed below are divided into two categories: those related to the implementation and usage of AI, albeit frequently, implementation and use issues are caused by or made easier by the design of AI itself, which is covered first. The problems can occasionally arise in more than one sector or area of application, or they may be cross-domain. Many of these problems—such as privacy and data protection—are shared by all forms of technology; many are interconnected and might not be dealt with separately.

But it is significant to keep in mind that AI has the interest to worsen and/or helps their unfavourable impacts. Lack of openness in the algorithms The issues and its importance A essential issues that is at the top of legal conversation on AI (EDPS2016; Pasquale 2015) is the lack of candour in computations (Bodo et al. 2018, Coglianese & Lehr 2018, Lepri et al 2018). Given the prevalent use of AI in high-risk areas, Cath (2018) highlights that "the stress is expanding on those who build and control AI to be responsible, fair, and open."

 [ISSN 2581-5369]

(A) How it is being addressed/solutions suggested

An EU Parliamentary STOA research (2019) provided three parliamentary options to regulate algorithmic accountability and accessibility, each of which tackles a different aspect of computer openness and obligation, based on an understanding of the interpersonal, scientific, and legal issues: 4. International cooperation for algorithm control. 1. gaining insight through research, agents of oversight, and informants. 2. responsible application of algorithms in the public sector. 3. judicial responsibility and oversight of regulators.

(B) Lacks and difficulties

Visibility has its drawbacks and is frequently thought to be insufficient and constrained (Ananny and Crawford 2018). For instance, according to Vaccaro and Karahalios (undated), "Decision-subjects may not agree with the outcome even when algorithmic choices can be explained." Although very helpful, some of the solutions mentioned above, including algorithmic impact evaluations, are still in the early stages of development and cannot yet be completely assessed for their efficacy. Future investigation and assessment are most certainly needed in this area.

III. SHORTCOMINGS IN COMPUTER SECURITY

(A) The problem and its importance

A viewpoint paper by RAND The use of AI weapons without human mediation, issues related to AI vulnerabilities in cyber security, how the application of AI to observation or cyber security for the country's safety opens a new attack vector based on "data diet vulnerability," the use of online tactics for intervention by foreign-deployed AI, and other security-related issues are highlighted by Osoba and Welser (2017).

The study by Osoba and Welser (2017) also cites problems with internal security, such as the (increasing) use of artificial agents by authorities to monitor people (such predictive policing algorithms). These have come under fire for having the potential to impair core civil liberties Couchman (2019). Such problems are important because they expose essential facilities to threats that have a negative impact on society and people as a whole, threatening human life, human security, and resource access. Cyber flaws are a serious issue as well because they are frequently concealed and only come to light after the damage has been done.

(B) How it is being addressed/solutions suggested

To deal with this issue, several methods and tools are being employed or suggested. Implementing effective protection and recovery methods, thinking about and addressing weaknesses during the design process, involving human analysts in crucial decision-making,

 [ISSN 2581-5369]

utilising risk control courses, and updating software are a few examples. Farrell (2019).

(C) Cracks and difficulties

For developers and users to employ cybersecurity rules, methods, and tools effectively, they must do so at all stages of development, implementation, and use. But in reality, this is frequently not the case, which presents a significant obstacle. According to the SHERPA report, "When creating systems that use machine learning theories, scientists ought to carefully evaluate their choice of a particular design, based on knowledge of possible threats and on clear, thought trade-offs among the complexity of the model, explainability, and robustness" (Patel et al, 2019).

IV. INJUSTICE, PREJUDICE, AND DISCRIMINATION

(A) The problem and its importance

Fairness (Smith 2017), bias (Courtland 2018), and discrimination (Smith 2017) are persistent problems that have been named as a significant challenge (Hacker 2018) in relation to the use of methods and machine-learning systems, such as those used to make decisions about insurance, employment, credit, and criminal justice (Danks & London 2017), among other things.

The adoption of a contentious exam algorithm used to award scores to GCSE students in England sparked protests in August 2020, and legal challenges are anticipated (Ferguson & Savage 2020). The potential for algorithm-based discrimination against people is discussed in a focus paper from the EU Agency for Fundamental Rights (FRA 2018), which also notes that "the notion of equality, as established in Article 21 of the The Charter of Fundamental Freedoms of the European Union, demands to be taken into account when implementing algorithms to everyday life" (FRA 2018).

One IEEE ethics-related norm, the IEEE P7003 Standard for Algorithmic Bias Considerations, is being developed as part of the IEEE Worldwide Initiative on Ethics of Autonomous and Creative Systems. Its purpose is to give those who are developing systems based on algorithms an environment for development to help them avoid producing unforeseen, irrational or improperly differential results for users. Throughout the lifecycle of an AI usage, users can investigate, report, and mitigate bias and prejudice in machine learning models with the aid of open source toolkits, such as the AI Equality 360 Open Source Toolkit. It makes use of 10 cutting-edge bias mitigation algorithms and 70 fairness measures that have been invented by the research industry.

 [ISSN 2581-5369]

(B) Gaps and difficulties

It is stated that the legislation falls short even while it explicitly controls and guards against discriminatory action. The legislation has gaps when it does not cover what is specifically safeguarded against prejudice by law or where new classes of distinction are formed and have biased and unfair impacts, according to a Council of Europe research published in 2018. There may be disagreements about when and where to use human-in-the-loop approaches (sometimes it may be better or even impossible to do so, for example, when there is a chance that an individual's error or stupidity could have serious or permanent consequences).

V. NOT BEING CONTESTABLE

(A) The problem and its importance

Individuals have the right to object to and request a review of artificially made decisions that materially impairs their rights or legitimate pursuits under the European Union data protection law (GDPR 2016/679). recipients have the right to object at any time to the use of their personal data that is based on tasks done in the public benefit or legitimate reasons, on grounds specific to their circumstances. Additionally, in accordance with Article 22(3) of the GDPR, data controllers are required to take appropriate steps to protect a data the subject's rights, freedoms, and legitimate interests, including at the very least the right to request human involvement on the part of the party in charge, the right to voice their opinion, and the right to challenge the decision.

(B) How it is being addressed/solutions suggested

In order to better protect the rights of choices made purely by automated processing, contestability by design has been suggested as a need at every stage of the lifetime of an artificial intelligence system. In 2019, Almada.

(C) Gaps and difficulties

The general protections, according to Roig (2017), "may not apply in the case of data analysis-based automated procedures, including the right to specific information to the data topic, the right to obtain human oversight, the right to express one's point of view, the precisely to obtain a clarification of how the choice was reached, and the right to object to the decision." Furthermore, it will be challenging to challenge an automatic decision in the absence of a detailed explanation of how the decision was made.

Weakness in the setting of AI depends on a variety of issues, including:

 [ISSN 2581-5369]

- Physical/Technical, such as inadequate security/protection; inadequate security/ development of algorithms and/or AI systems;
- Social issues include (lack of) knowledge and understanding among the general public about AI and its effects, steps taken to ensure/protect the wellbeing of people, communities, and the community, literacy, education, skill development, the presence of stability and peace, access to fundamental human rights, social equity, good morals, health, and unity in society.
- Political, such as inadequate official acknowledgment of or plan to handle AI risks, readiness measures, appropriate governance systems, and incentives, such as those to encourage the deployment of risk mitigation measures
- Regulations, such as laws, oversight, enforcement, and harm-relieving measures,
- Economic factors include income levels, insurance, investments in safe and morally acceptable systems, resources to deal with negative outcomes, affluence, and poverty.

VI. CONCLUSION

especially, it associated the subject of AI legal problems with vulnerability—a inquiry that is much needed on many levels—and provided a comprehensive overview of the myriad legal concerns, gaps, challenges, and affected human rights principles that are connected to AI. This article will serve as a particularly useful reference and stepping-stone for investigators doing more research on the topic. Additionally, it offered three crucial measures that have to be taken into account to safeguard society's most vulnerable citizens.

Numerous the topics under investigation have broad societal and human rights ramifications. They have an impact on a variety of human rights concepts, including security of information, fairness, rights, human independence and choice, human dignity, human safety, informed approval, honesty and legal services, and justice.

Given the circumstances, usage, and use of AI, as demonstrated in section 6, the groups and communities that will be most impacted by such challenges will change. The root causes of the weaknesses must be addressed in order to reduce the negative effects, build resilience, and effectively combat the vulnerability-causing elements.

As AI technology develops, there will be further (and perhaps more significant) legal concerns, vulnerabilities, and effects on human rights that require greater investigation and monitoring. Through data-driven innovation and intelligent devices that either augment or replace humans and their abilities, technological advancements will accelerate.

 [ISSN 2581-5369]

VII. REFERENCES

- https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf
- To build disputed structures, the role of humans in machine learning is being explored. (2019), 10.2139/ssrn.3264189, 17th International Conference on Artificial Intelligence and Law
- You are being observed by smart machines at work. Regulations, personnel tracking, and online surveillance in the EU context. Automation, artificial intelligence, and labour safety in: Stefano VD (ed.2019's special edition of the Comparative Labour Law & Policy Journal)
- Understanding the open-door ideal's shortcomings and how they relate to computational accountability 10.1177/1461444816676645, New Media & Society, 20 (3) (2018), pp. 973-989
- Is human rights' basis vulnerability? The vulnerable inherent worth in the age of rights, (2016), Springer, Cham, pp. 257-272

*****

 [ISSN 2581-5369]