Journal of Advances and Scholarly Researches in Allied Education
Vol. 19, Issue No. 4, July-2022, ISSN 2230-7540

A Study the Human Rights Facing AI And Legal issues of AI: Gaps, Challenges

Astha Garg[1]*, Dr. Vipin Kumar[2]

[1] Research Scholar, Shri Venkateshwara University

[2] Associate Professor, School of Law & Jurisprudence, Shri Venkateshwara University

Abstract- ***AI can improve society if used wisely. Furthermore, there is a genuine possibility that commercial and governmental use will have a negative influence on human rights, as is the case with most developing technologies. The objective of this study focuses on how gaps & challenges in AI will be addressed, as well as how these issues may affect fundamental human rights concepts. These problems include algorithmic openness, cyber security flaws, unfairness, bias, &perception, lack of contestability, problems with legal personhood, problems with intellectual property, negative effects on workers, problems with privacy & data protection, liability for harm, & lack of accountability. In order to better understand key areas of concern &direct risk & impact mitigation measures to safeguard human well-being, the analysis will use the concept of "vulnerability."***

Keywords - Human Rights, Artificial Intelligence, Legal Issues, Cyber Security

----------X----------

INTRODUCTION

We must ensure sufficient accountability in defending human rights as we hand over increasing authority to computers in terms of autonomous decision-making. Human surveillance is one instance of using AI for a purported good that might also violate human rights. Many countries are currently putting new technology into practice to stop illegal & threatening behavior, including terrorist acts, such as video surveillance & biometric tracking. Our lives are safer thanks to these government initiatives, which also serve to deter criminal activity.Moreover, these same technologies actively track & monitor regular people, that is a violation of their privacy and may lead to future discrimination based on their political views, health issues, or even their religious beliefs. Additionally, the industry's evolution presents new problems. The idea of a legal person is challenged in the light of advancements in science & technology, for *"the scientific and technological world, artificial in conceptual nature, come to encroach upon the already defined legal dimension of a person, an artificial concept in itself".*

Dignity, the guiding principle for all human rights & idea of the inherent equality of all people, is challenged by this technological advancement. Particularly in the preamble & paragraphs 1 and 2, the 1948 UDHR & UN Charter both clearly demonstrate concern for dignity. All people have unalienable rights, which guarantee natural equality & shield us from all forms of discrimination, because of the acknowledgement of our inherent worth. Technology has the capability to endanger equality.

EUROPEAN (EU) HUMAN RIGHTS PROTECTION AND AI

The EU Ethical Charter regarding the utilization of AI in the judicial system, endorsed by the Commission for the Efficacyof Justice, was based on a studies on the human rights aspect of automatic data processing techniques & potential regulatory implications issued in 2018 under the title "Algorithms & Human Rights-Study" (CEPEJ).The issue was that, given the use of sensitive data in predictive judgments of responsibility, including race or ethnicity origin, political preferences, religious or political beliefs, social economic conditions, or data regarding health, the usage of AI in this field would not only violate the right to a judge & right to a fair trial via presumption of innocence, equality of arms, & respect for the contradictory. According to Article 5 of the EU Convention on Human Rights, the right to a judge thus refers to the right to a judge's bodily presence, and as a result, it cannot be replaced by an algorithm.

PROTECTING PERSONAL DATA ONLINE THROUGH AI & DIGITAL SECURITY

Massive volumes of personal data are sent via social networks every second by billions of Internet users, providing huge digital operators with an annual market value of $1 trillion. This supports Metcalfe's Law, which states that a network's value rises exponential as its user base increases. In this situation, the legislation also relates to the value that each user, for instance, of a social network like Facebook, adds to AI. The major digital players

develop the world of AI from this vast social, economic, and emotional history. But how are this digital patrimony & underlying rights safeguarded?

We are focusing on personal data in particular because it is one of the industries that is daily affected by the development of AI technologies. These systems' operation is in fact based on the development, analysis, & treatment of large amounts of information, particularly personal data that are transmitted via the internet. However in this same area, there are numerous concerns.

Risks to our digital security, which is intertwined with a number of rights, include data theft, phishing, malware, & online mass checks. The right to privacy comes first and foremost, and it also affects other rights like the freedom of expression or the right to peaceful assembly & association. Online, several rights are consequently questioned. Our right to privacy is at jeopardy when we use a mobile phone to transmit data about our whereabouts or habitudes. We exercise our right to free speech when we engage in public online conversations & voice our opinions. We exercise our right to informational access when we look for a topic online that interests us.Finally, we utilize our right to peaceful assembly when we submit an application to consent to take part in a public protest. Human rights are in jeopardy in each of these situations because they are interrelated, non-hierarchically ordered, & dependent on one another, placing others' enjoyment of them in jeopardy when one is violated. These rights are protected in the online environment thanks to appropriate & strong digital security.

HUMAN RIGHTS & LEGAL CONCERNS WITH AI

The relevance of each issue, suggested remedies (or how it is being tackled), gaps & obstacles that surround it are all briefly discussed in this section. This is a superficial analysis (Other studies has thoroughly examined & critically debated each of these topics; the goal here is to present a comprehensive, up-to-date review that will be valuable for future investigation). Ten issues are listed below, some of which are related to the implementation & usage of AI, others to the design & nature of AI itself (these are treated first) (Despite this, the architecture of AI frequently contributes to or facilitates implementation and use challenges).The vulnerabilities are occasionally cross-domain, in the sense that they may obvious in one or more sectors/fields of application. Several of these concerns are universal to all technology (e.g., privacy/data protection); many are interconnected (e.g., transparency, fairness, accountability) and may not exist in isolation. However, the power of AI to compound and/or assist these negative impacts should never be underestimated.

Lack of algorithmic transparency

The lack of algorithm transparencies (Bodo et al 2018) is a crucial issue that has risen to the top of legal discussions around AI (EDPS 2016 ; Pasquale 2015). Cath (2018) emphasizes that "demand is rising to design & control AI to be accountable, fair, and transparent" given the expansion of AI in high-risk domains. The lack of algorithm transparencies is significant; Desai (2017) explain why by citing cases of people who were denied jobs, loans, were placed on no-fly lists, or were denied services without knowing "why it occurred other that the decision was executed through some program."

Solutions being address

Founded on an analysis of the social, technical, & regulatory problems, an EU Parliament STOA research (2019) offered multiple legislative solutions to manage algorithmic transparency & accountability; each proposal addresses a distinct component of algorithmic transparency & accountability:

1. Raising awareness through education, watchdogs, & whistleblowers;

2. Accountability in the usage of algorithmic decision-making in the public sector;

3. Regulatory oversight & legal culpability; and

4. Worldwide coordination for algorithmic governance.

Algorithmic influencevaluations (Reisman et al 2018; Govt. of Canada, undated), an algorithmic transparency standard (IEEE P7001:Transparency of Autonomous Systems), counterfactual explanations, local interpretable model-agnostic explanations (LIME) (Ribeiro, Singh, Guestrin 2016), or other solutions have been proposed to promote algorithmic transparency.

Gaps & challenges

Transparency has constraints and is sometimes perceived as insufficient and limiting (Ananny 2018). According to Vaccaro and Karahalios (undated), "even when machine learning conclusions could be elucidated, decision-subjects may not agree with the outcome." Although several of the solutions mentioned above, such as algorithmic impact evaluations, are incredibly helpful, they are still in their early stages and cannot be completely tested for their effectiveness at this time. This is undoubtedly a topic for future investigation& review.

Adverse effects on workers

The IBA Global Employment Institute report (2017) emphasizes the impact of AI & robotics in the workplace (seen a global concern). Among the issues raised contain: variations in the requirements for future employees, a decrease in demand for workers, labor relations, the creation of new job structures and new types of jobs, employee

dismissal, inequality in the 'new' job market, integration of untrained workers in the 'new' job market, labor relations (and its implications for union activities & collective bargaining aspects, challenges for employee representatives, and structural changes).

Solutions is being address

Many strategies or remedies are being considered or have been offered to address this problem. Involving retraining workers & refocusing and adjusting the education system (UK House of Lords 2018). According to the EU Commission's Communication on AI for Europe (2018), governments should prioritize the modernization of education at all levels, & Europeans should have every chance to acquire the skills they require. To accomplish the AI revolution, the Communication urges for employees whose employment change or disappear to be supported; it suggests that "national initiatives will be important for providing such up-skilling & training" . Social security systems will also need to be reviewed & modified.

Gaps & challenges

One study released for the Royal Society (2018) identifies evidence gaps, especially with regard to the existence of "*limited evidence on how AI is being used now and on how workers' tasks have changed where this has happened* ", "*relatively little discussion of how existing institutions, policies, social responses are shaping and are likely to shape the evolution of AI and its adoption* "and "*little consideration of how international trade, mobility of capital and of AI researchers are shaping the development of AI and therefore its potential impact on work* "Frontier Economics (2018) . While there is acknowledgement of the widespread disruption that AI is and may cause in the workplace, not enough has been done at the policy &regulatory levels to address concerns and implement necessary economic and educational policies & regulations.

Privacy & data protection issues

Legal researchers & data protection enforcement authorities (CNIL 2017; ICO 2017) feel that AI provides significant privacy & data protection challenges Gardner (2016). Included informed consent, monitoring Brundage (2018), and violations of individuals' data protection rights, such as the right of access to personal data, the right to prevent processing that is likely to cause harm or distress, the right not to be subject to a decision based solely on automatic processing, and so on.

Solutions being address

Privacy & data protection law (especially in the European Union) offers adequate security & protections for data subjects' rights, at least in the notelet of the law. For example, GDPR data subjects' rights to transparency, information, and access (Article 15), rectification (Article 16) & erasure (Article 17), right to object to autonomous individual decision-making (Article 21), and so on. Transparency of potential hazards associated with AI use is strongly endorsed in terms of informed consent (Rigby 2019); designersmust "*pay close attention to ethical & regulatory restrictions at each stage of data processing. "Data provenance & consent for usage, reuse are regarded as particularly essential" (Vayena, 2018).*

Gaps &challenges

The law governing privacy & data protection does not touch all aspects of AI. As already stated, "*Identifying & resolving the extent of data protection law & principles in the rapidly evolving context of AI is a difficult task, but it is essential to prevent overloading AI with excessive regulatory obligations or doubt about whether regulatory standards apply.*"(CIPL 2018).Measures to protect privacy & data are only effective if they are utilized, appropriately applied, monitored, and/or enforced. As the EU Data Protection Supervisor's Opinion 5/2018 Earliest Opinion on privacy through design highlights, "*there is a incomplete uptake of commercial products and services fully embracing the concept of privacy by design &default* ". The challenge in some cases is that the efficiency of measures including privacy/data protection impact studies & privacy by design may fall flat (such as concluding the gate after the horse has bolted) because the main objective of the AI system or technology may directly conflict with societal values & fundamental rights.

Liability for damage

AI technology implementation & use can result in harm to people and property. For example, Gluyas & Day (2018) present various examples, such as driverless autos driving over pedestrians, crashing and damaging caused by a partly piloted drone, and incorrect medical treatment diagnosed by an AI software program. They elaborate more, "*Because there are so many countries involved in an AI system (data source, designer, producer, developer, coder, user, & AI system itself), establishing liability when anything goes wrong is challenging, due to the numerous aspects to consider.…*"Gluyas & Day (2018) .

Solutions is being address

Civil or criminal liability could be used to solve AI liability issues. Kingston (2016) discusses AI and legal liability, as well as whether criminal liability may ever be implemented, to whom it might apply, and whether an AI program is a product subject to product design legislation (product liability, for example, in cases of design or manufacturing failures) or a service subject to the tort of negligence.

Lack of accountability for harms

Accountability, as described by the Evaluation List for Trustworthy AI (ALTAI), necessitates the establishment of mechanisms to guarantee accountability for the innovation, deployment, and/or use of AI systems - risk management, identifying and mitigating risks in a democratic manner that can be explained & analyzed by third parties (AI HLEG 2020). According to Dignum (2018), "*Accountability in AI necessitates both the role of guiding action (by forming beliefs & making judgments) & function of explanation (by situating decisions in a broader context & categorizing them according to moral norms) "*. Some observers argue that the "accountability gap" is a bigger problem than it appears, generating issues in three areas: causality, justice, & recompense. Bartlett, 2019 According to a Privacy International & Article 19 (2018) report,"Even when a potential harm is found, it can be difficult to ensure accountability for violations of those responsible. "

Solutions is being address

According to Wachter, (2017), "American & European policies appear to be disagreeing on how to bridge current accountability gaps in AI." Legal accountability mechanisms for AI abuses could include a "right to explanation" Edwards, Veale (2017), data protection & information & transparency safeguards, auditing, or other reporting standards. Doshi-Velez et al. (2017) examine the scenarios in which explanation is necessarily required by law & explain technological aspects that must be explored if AI systems that can deliver the kinds of explanations that humans are currently compelled to provide are required.

Gaps &challenges

According to Bartlett (2019), *"There is no one-size-fits-all solution to AI accountability. One of the most serious concerns of holding researchers accountable is a chilling impact on AI development. After all, AI developers are frequently individuals or small businesses. Whether or not they are the most responsible when their creations cause injury, the pragmatic nightmare of facing litigation every time their AI causes harm may make AI developers extremely hesitant to release their creations into the world (hedge fund shareholders may pause before achieving for their cheques issued) "*Bartlett (2019) .As an accountability mechanism, the right to explanation has some difficulties. Wallace (2017) emphasizes, "it is often not practical or even possible, to explain all decisions made by algorithms". Further, "the challenge of explaining an algorithmic decision comes not from the complexity of the algorithm, but the difficulty of giving meaning to the data it draws on "Wallace (2017)

CYBER SECURITY VULNERABILITIES

Osoba & Welser (2017) illustrate various AI security issues, such as fully automated decision-making leading to costly errors & fatalities; the utilization of AI weapons without human mediation; issues associated to AI vulnerabilities in cyber security; how the usage of artificial intelligence to scrutiny or cyber security for national security opens a new attack vector based on 'data diet vulnerability'; & usage of network intervention methods. The study Osoba & Welser (2017) also addresses domestic security-related issues, such as governments' (increasing) use of artificial agents for civilian monitoring (e.g., predictive policing algorithms).Couchman (2019) has identified these as having the potential to negatively impair fundamental citizens' rights. These challenges are crucial because they expose vital infrastructures to harm, with serious consequences for society & individuals, posing a threat to life & human security, with access to resources. Cyber security flaws are also a serious hazard because they are frequently disguised and found only after it is too late (after the damage is caused).

Solutions is being address

To solve this issue, several approaches & tools are being utilized or proposed. For example, putting in place appropriate protection & recovery methods; evaluating & addressing vulnerabilities during the design phase; utilizing human analysts in important decision-making; utilizing risk management programs; & upgrading software. Fralick (2019).

Gaps & challenges

To efficiently address such concerns, developers & users must be proactive & responsive in their utilization of cybersecurity policies, methods, & tools at all phases of design, implementation, and use. However, this is frequently not the case in practice, which poses a significant issue. Outlines of a SHERPA report, "*Engineers should evaluate their choice of architecture when creating systems that incorporate machine learning models, depending on an awareness of potential threats and clear, reasoned trade-off judgments between computational cost, explainability, & robustness.*"(Patel et al, 2019).

Unfairness, bias & discrimination

Unfairness (Smith 2017), bias (Courtland 2018), and discrimination (Smith 2017) were recognized as issues & major challenge (Hacker 2018) referring to the utilization of algorithms & automated decision-making systems, such as those used to make health (Danks & London 2017), employment, credit, criminal justice (Berk 2019), & insurance decisions. Protests & legal challenges are likely in August 2020 over the usage of a contentious assessment methodology utilized to assign scores to GCSE students in England (Ferguson& Savage 2020).

According to an EU Agency for Fundamental Rights (FRA 2018) focus paper, "the concept of non-discrimination, as enshrined in Article 21 of the Charter of Fundamental Rights of the EU, must be

considered into account when implementing algorithms to daily life" (FRA 2018). It includes examples of prejudice, such as computerized choice of candidates for job interviews & use of risk assessments in creditworthiness or trials. The European Parliament (2017) stated in a study on the fundamental rights aspects of big data: privacy, data protection, non-discrimination, security, & law enforcement that "*because of the data sets and algorithmic systems used when making assessments and predictions at the different stages of data processing, big data may result not only in infringements of the fundamental rights of individuals, but also in differential treatment of and in- direct discrimination against groups of people with similar characteristics, particularly with regard to fairness and equality of opportunities for access to education and employment, when recruiting or assessing individuals or when determining the new consumer habits of social media users* "European Parliament (2017) .

Solutions is being address

Several proposals have been presented to overcome such concerns. For example, European Parliament (2017), discussing regular assessments into the sampling of data sets & whether they are influenced by biased elements, making technological or algorithmic adjustments to reimburse for problematic bias (Danks & London 2017), humans-in-the-loop (Berendt, Preibusch 2017), & making algorithms open. Schemes are also being developed to ensure that algorithmic decision systems do not show unjustifiable bias. The IEEE P7003 Standard for Algorithmic Bias Deliberations is one of the IEEE ethics-related standards (under advance as part of the IEEE Global Initiative on Ethics of Autonomous & Intelligent Systems) aimed at providing individuals or organizations developing algorithmic systems with a framework to prevent undesirable, unjustified, & inadequately differential consequences for users.There are other open source toolkits available, such as the AI Fairness 360 Open Source Toolkit, which assists users in examining, reporting, & mitigating discrimination & bias in machine learning models across the AI application life cycle. It makes use of 70 fairness criteria & 10 cutting-edge bias reduction algorithms established by the research field.

Gaps & challenges.

While the legislation explicitly regulates & protects against discrimination, it is argued that it falls short. Affording to a studiesshowed by the Council of Europe (2018), the law falls short if it does not extended to address what is not explicitly protected against discrimination by law, or where new classes of differentiation are formed, resulting in biased & discriminatory impacts. Human-in-the-loop techniques may confront disagreements over where and when they should be used (Sometimes it may be preferable or impossible to have humans in the loop, such as when there is a risk of human error or stupidity leading to significant or irreversible repercussions).Other gaps involve whether the usage of human-in-the-loop technology is properly represented in the technologies that employ it. Making algorithms accessible does not imply that they will become more accessible to people; there is also the question of the exposing or discoverability of private data, which raises its own set of difficulties. Parliament's House of Commons (2018). To be efficient, algorithmic auditing must be holistic, interdisciplinary, scientifically founded, & ethically informed. While the technical solutions presented thus far are positive steps forward, many have called for increased regulatory, policy, & ethical attention to fairness, particularly in terms of protecting vulnerable & marginalized people. Buolamwini & Raji (2019).

Lack of contestability

Individuals have the ability under European Union data privacy law to challenge & request a study of automated decision-making that materially impacts their rights or legitimate interests (GDPR 2016/679). Data subjects have the right to object at any time, on reasons pertaining to their specific situation, to the use of personal information relating to them that is based on works carried out in the public interest or legitimate interests. Furthermore, according to Article 22(3) GDPR, data controllers must adopt appropriate measures to protect a data subject's rights, freedoms, or legitimate interests, including the right to obtain human intervention from the controller, express their point of view, or challenge the decision.Hildebrandt (2016), the other perspective, emphasizes how "the opacity of ML systems may undermine both the accountability of their 'owners' & contestability of their choices." Edwards & Veale (2017) emphasize the absence of contestability in algorithmic systems i.e., the "absence of a clear way to challenge them when they create unexpected, harmful, unfair, or discriminating outcomes".

Solutions is being addressed

Almada (2019) advocated contestability by construction as a way to better protect the rights of choices based exclusively on automated processing as a necessity at each level of AI system's lifecycle.

Gaps & challenges

According to Roig (2017), "*General safeguards - specific information to the data subject; the right to human intervention; the right to express one's point of view; the right to an explanation of the decision reached; & right to challenge the decision -may not apply in the case of data analysis-based automated processing*". Further, that it "*will be difficult to contest an automatic decision without a clear elucidation of the decision reached. To challenge such an automatic data-based decision, only a multi-disciplinary team with data analysts will be able to detect false positives and discriminations* "Roig (2017) . As a result, this is an issue that must be

handled at multiple levels (design, development & utilize).

Legal personhood issues

There is continuous discussion regarding whether AI (and/or robotics systems) "fit within existing legal categories or whether a new category with its own distinctive features and implications should be developed." (Resolution of the European Parliament, 16 February 2017) This is a politically fraught matter, not just a legal one. Burri (2017) .erka et al. (2017) investigate whether AI systems could be considered legal subjects. The High-Level Expert Group on AI (AI HLEG) has particularly persuaded "policymakers to refrain from establishing personality for AI systems or robots," arguing that doing so is "intrinsically inconsistent with the concept of human agency, accountability, & responsibility" and poses a "significant moral hazard" (AI HLEG 2019).Others, however, argue that "legal personality for AI could be justifiable as an elegant answer to pragmatic problems deriving from the challenges of allocating responsibility for AI and/or, in order to promote AI's moral rights, if any."

Solutions is being addressed

At the international, EU, or national levels, there has been no major progress in addressing legal personality issues for AI. Since this issue has been elevated (and will proceed to be at the frontline of legal debates in the near future), international or even regional-level agreement Delcker (2018) on this (i.e., whether legal personhood must be granted to AI systems/robots and in what form) may be challenging or impossible to achieve (showed the political nature & sensitivity of the issue). Furthermore, such matters are generally governed at the national level.

Gaps & challenges

Bro z & Jakubiec (2017) addressed the question of autonomous machines' legal responsibility & concluded that "autonomous machines cannot be awarded the status of legal actors." According to Bryson, Diamantis, & Grant (2017), bestowing legal personhood on wholly synthetic entities is a very real legal option, but such "legislative action will be morally unwarranted and legally difficult." "As AI legal personality also has emotional or economic appeal, so do several seemingly desirable perils against which we are protected by the law," they argue in their review of the utility & history of legal fictions of personhood, and after describing the salient precedents where fictions resulted in abuse or incoherence. Grant, Bryson, & Diamantis (2017)

Intellectual property issues

UDHR, Article 27, the International Covenant on Economic, Social, & Cultural Rights (ICESCR, Article 15), the International Covenant on Civil & Political Rights (ICCPR, Article 19), &Vienna Declaration and Programme of Action (VDPA) 1993 all include IP rights. Such rights have a "human rights dimension" & "have become contextualised in a variety of policy areas," according to WIPO (1998). AI introduces a number of IP concerns, such as who owns AI-generated/produced works or inventions. Should the inventions of artificial intelligence be considered previous art? Who owns the dataset from which an AI is expected to learn? Who should be held accountable for AI-generated creativity & invention that infringe on the rights or other legal provisions of others? CEIPI, undated

Solutions is being addressed

Rodrigues (2019) suggests that the law may provide a number of answers to the difficulties presented. In the United Kingdom, for example, computer-generated literary, theatrical, musical, or creative creations are protected by law. There is no explicit legislative provision regarding the patentability of computer-generated works. The inventor of the AI design holds such rights unless the work was commissioned or developed during the course of employment. In the latter case, the rights are retained by the employer or entity that commission the AI work UK Copyright Service (2004). Since a registered trade mark is personal property, this right may not pertain or be available to an AI system unless the AI system can hold/have personal property.

Gaps & challenges

Many IP rights issues remain unresolved, and current laws are viewed as "woefully insufficient to deal with the expanding employment of more and more perceptive AI systems in the production of such works." Davies, D. (2011). More inquiry & exploration are required, especially as AI improves and it becomes more difficult to recognize the inventor. Talking Tech was released in 2017.

This paper gave ainclusivesummary of the numerous legal issues, gaps & challenges, and influenced human rights principles associated with AI, and will serve as an extremely effective reference & stepping-stone for researchers to conduct additional studies on the topic in some countries, lack of judicial knowledge & training, and greyness in the legal status of automation systems.

CONCLUSION

AI is a kind of intelligence that was born in the 1950s &essential part of the digital revolution. Progress made by AI has permitted the birth of systems capable of rivaling human capacities or, in some cases, surpassing them. This analysis is focus on the legal & human rights issues raised by AI, how they are addressed, gaps & challenges, and how they influence human rights concepts. These

include: algorithmic transparency, cybersecurity vulnerabilities, unfairness, bias, & discrimination, lack of contestability, legal personhood issues, IP issues, negative effects on workers, privacy & data protection issues, liability for damage, & lack of accountability. The framework of 'vulnerability' is used in the study to consolidate awareness of major areas of concern and to drive risk & impact mitigation actions to protect human well-being.

REFERENCES

1. Cath, C (2018). Governing artificial intelligence: Ethical, legal and technical opportu- nities and challenges. *Philosophical Transactions of the Royal Society A: Mathemati- cal, Physical and Engineering Sciences* . https://royalsocietypublishing.org/doi/full/10.1098/rsta.2018.0080 .
2. Čerka, P , Grigien ė, J , & Sirbikyt ė, G (2017). Is it possible to grant legal personality to artificial intelligence software systems.*Computer Law & Security Review, 33* (5), 685–699 .
3. Christiaan, V., & Corinne, C. (2018). Artificial intelligence: What's human right got to do with it? *Data & society points*. Retrieved August 28, 2019, from https://points.datasociety.net/artificial-intelligence-whats-human-rights-go-to-do-with-it-4622ec1566d5
4. Christiaan, V., & Corinne, C. (2018). Artificial intelligence: What's human right got to do with it? *Data & society points*. Retrieved August 28, 2019, from https://points.datasociety.net/artificial-intelligence-whats-human-rights-go-to-do-with-it-4622ec1566d5
5. Davies, CR (2011). An evolutionary step in intellectual property rights–Artificial intelligence and intellectual property. *Computer Law & Security Review, 27* (6), 601–619 .
6. Davison, N. (2016). "A legal perspective: Autonomous weapon systems under international humanitarian law, Perspectives on Lethal Autonomous weapon systems", Legal Division International Committee of the Red Cross, UNODA. Occasional Papers, No. 30. PP 5-18. Retrieved from:
7. Heinrichs, B. (2022). Discrimination in the age of artificial intelligence. AI & society, 37(1), 143-154. https://doi.org/10.1007/s00146-021-01192-2
8. Huong, L.T.T., & Giao, V.C. (2019). The impact of artificial intelligence on human rights: A number of theoretical and practical issues. In N.T.Q. Anh, V.C.Giao, M.V. Thang (Eds.), *Artificial Intelligence with* Law *and Human Rights*. Hanoi: The Judiciary Publishing House.
9. Jaynes T, L (2020). Legal personhood for artificial intelligence: citizenship as the exception to the rule. *AI & SOCIETY, 35* (2), 343 35 .
10. Kingston, JKC (2016). Artificial intelligence and legal liability. In *International conference on innovative techniques and applications of artificial intelligence* (pp. 269–279).

Corresponding Author

Astha Garg*

Research Scholar, Shri Venkateshwara University