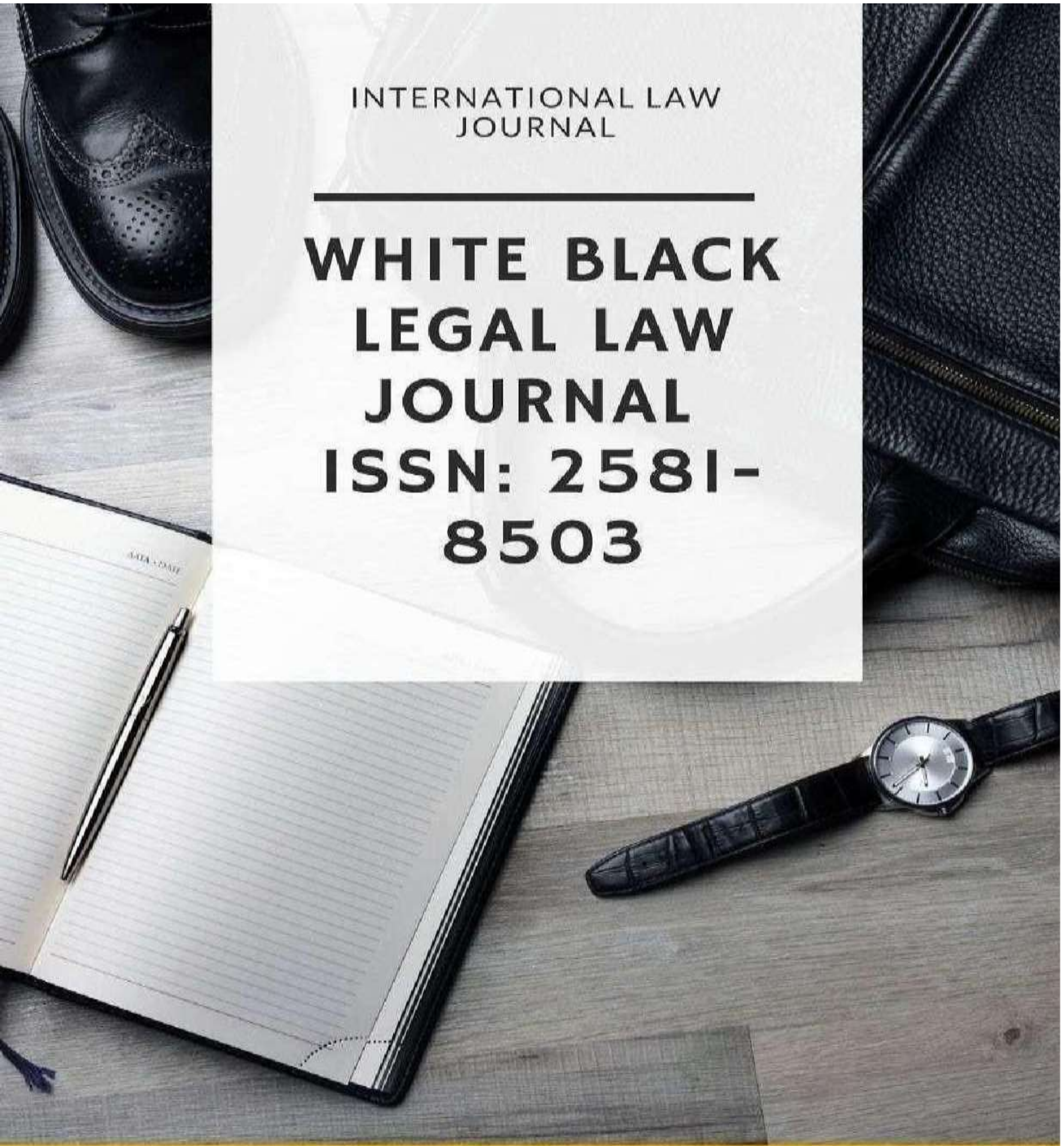

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of White Black Legal – The Law Journal. The Editorial Team of White Black Legal holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of White Black Legal. Though all efforts are made to ensure the accuracy and correctness of the information published, White Black Legal shall not be responsible for any errors caused due to oversight or otherwise.

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

www.whiteblacklegal.co.in
Volume 3 Issue 1 | April 2025 ISSN: 2581-8503

BALANCING INNOVATION AND RIGHTS: THE ROLE OF LAW IN GOVERNING AI TECHNOLOGIES

AUTHORED BY - YASH SINGHAL

Abstract

In this regard, accountability getting the centre stage when it comes to the deployment of AI technologies to make sure they uphold principles of human rights as well as ethical issues. Today’s frameworks, including GDPR, define the protection and responsibility of individuals who are about to be exposed to automated decisions. Data processors’ transparency and accountability laws are part of the GDPR that was devised by the European Union. Article 22 of the GDPR, for example, provides the right not to be made a subject to a decision solely based on automated processing where such decision has a legal or significant effect on the person, for example when it comes to employment or credit rating. Such legal warranty proves that several human interventions and appeal procedures are still necessary to protect people from adverse consequences of embracing AI.

Another is the right to explanation which while its operationality is contentious makes it mandatory that the data subject can always ask for an explanation of the decision of the automated system. The purpose of this provision is to enable people to gain confidence and be able to comprehend why things are done adversely affecting him or her. Recital 71 of the GDPR builds on this by noting that reasonable steps should be taken to avoid such adverse effects, this speaks of fairness and transparency.

International human rights also form another framework of instruments of accountability. According to Under the International Covenant on Civil and Political Rights (ICCPR), Article 17 prohibits forced or unlawful interference with the privacy of others which has impact on collection and surveillance by artificial intelligence systems. The United Nations Guiding Principles on Business and Human Rights takes this a step further and argue that business entities are required to protect human rights and this entails dealing with possible human rights abuses arising out of the technologies the businesses have developed. To this end, the above-mentioned principles call for risk assessment practices that consider the outcomes of applying AI and the utilization of enabling measures for mitigation.

Introduction

AI system technologies are seen to have more applications in various fields such as health care, finance, law enforcement, and education among others since the benefits of the systems range from more efficient and effective decisions making. Still, this fast integration of AI raises pertinent issues on issues to do with human rights. Due to the increasing adoption of AI in different sectors it impacts on the core rights and freedoms such as the right to privacy, anti-discrimination and freedom of speech. Human rights are increasingly a consideration in both the development and application of AI, according to the United Nations, which states that human rights must be brought to bear on the management of artificial intelligence to prevent the technologies from devolving from their ideals of societal justice. AI can facilitate the delivery of critical services to the needy, at the same time, perpetrate bias in algorithm choices and implementation of intrusive measurement tools. For example, some recently released AI works like facial recognition result in cases of wrongful arrest and racial profiling while there is a lack of elaborate law protecting the rights of citizens in their development. Larger concerns are summed up with regard to privacy as the majority of these systems are founded on amassing copious amounts of highly personal information. Lack of highly developed Data Protection laws makes it possible for the tech-giants to extract users' data without sufficient control. Also, there is the problem of algorithmic bias; most AI systems are taught on biased data and as such uphold prejudices in areas like employment and police work. Additionally, the already existing issues with human rights are worsened by the potential abusive use of AI systems as seen in authoritarian regimes for surveillance purposes. This research seeks to thus examine the relationship between AI and human rights by analysing the already existent legal frameworks to thus establish the existing legal deficiencies that act as barriers to the protection of human rights. The study will consider how existing legislation that is today being developed, such as the EU AI act, can be strengthened for the prevention of risk factors related to artificial intelligence technologies.

2. Human Rights Implications of AI

2.1 Privacy Rights

AI technologies are a step up, and they have an effect on the privacy rights worldwide, primarily since there are real-life examples of how these technologies can be misused. Among others the latest example is the case of Cambridge Analytica[1] that used AI to process people's data, including the personal one, from Facebook to influence politics. This particular occurrence not only revealed the capability of AI in data profiling numbers but also challenges of data protection law at the time. The result led to legislative discussions and changes, for example, under GDPR[2], making privacy conditions stricter, and new repudiation of data manipulating procedures all over the world.

Other controversies laid in this oversimplification of politics of surveillance as tech giants were dragged into legal battles. Carpenter v. Carp v. United States (2018)[3] was a US supreme court case on warrant less wiretapping, in particular the warrant less collection of location data. The ruling was that such actions amounted to a search under the Fourth Amendment and that decision helped serve to strengthen privacy rights against weaknesses or attempts at erosion by the government relative to applications of AI based data collection. This case points to how judicial courts are gradually starting illustrate concerns on technological capability. Again, extending the concept of predictive algorithms into privacy, there are deeper encroachment into one's life as the fields of machine learning open up new opportunities for behavioural prediction. Berk and Edwardsm studying cities such as Los Angeles and Chicago have identified concerns regarding usage of tools in predictive policing on individual's privacy. These systems, frequently implemented with non- transparent governance, utilize big data to anticipate future offenses and sometimes use data that may comprise sensitive personal information gathered without subject consent. Human Rights Watch has observed such practices cause a form of surveillance that denies individual's right of privacy and freedom of physical movement with a particular impact on vulnerable persons.

Even when it comes to culture and laws defining the domain of privacy, one gets lost in differences. In EU, right to privacy is recognized as a human right under Article 8 of ECHR and so the regulation of AI is even stricter than this protection. On the other hand, in the countries that do not have strong defending rights like in China, AI technologies are being used more vehemently for surveillance, and normally, such violations compromise the privacy of

[1] "See Carole Cadwalladr & Emma Graham-Harrison, Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach, *The Guardian* (Mar. 17, 2018), https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election."

[2] "See General Data Protection Regulation, Regulation (EU) 2016/679, OJ L119 (2016), available at https://eur-lex.europa.eu/eli/reg/2016/679/oj."

[3] "Carpenter v. United States, 138 S. Ct. 2206 (2018)."

the individual. Facial recognition application in objects and data accumulation process under the Supervision of SCS reveal that how otherwise benevolent technology of AI might be abused by states to infringe the basic notion of privacy and consent.

2.2 Non-discrimination and Equality

The problem of non- discrimination and equal opportunities regarding the AI has recently turned into a burning actuality, particularly as more and more cases demonstrate the prejudice of algorithmic systems. Algorithms for hiring employed by leading companies have been criticized for being discriminative by gender and color. A notable example is an Amazon's AI-powered recruitment tool that almost always rejected applicants with characteristics that are typical of females, such as care and nursing experience, as well as words related to these skills. This failure was as a result of training data which contained features likely hireable based on history where male candidates were the majority. Modelling these real-life situations explain information of algorithms an organization's prejudice even when an algorithm is optimized for efficiency.

The analysis of target vectors conducted in technical papers, including the one by Bolukbasi et al. (2016), shows that prejudice can be innate in the source data into which machine learning models are trained. It becomes evident in a situation where Data contains historical prejudice, for example, when recursion results in old prejudices in inequalities or stereotyping. A study in the Journal of Artificial Intelligence Research shows how word embeddings, commonly applied in natural language processing, are sexist: they associated the word 'doctor' with maleness and the word 'nurse' with femaleness. Such findings further emphasize in the need for active monitoring of AI model and multiple data feeds to avoid bias in the model.

It is also important to notice that discrimination is not restrained only for corporate environments. Biometric techniques like Facial recognition earlier had manifested variance in performance between different groups of population. The study by the US National Institute of Standards and Technology (NIST) released in 2019 unveiled that many facial recognition systems are as much as 100% more likely to identify women and people with darker skin tones as other people than white men. These disparities raises when such technologies are applied in tender areas such as policing SYSTEM, which results in wrong accusations and other violations of the law. For this reason, the fact that an African American man, Robert Williams was wrongfully arrested in Detroit due to a misidentification of facial recognition, AI is a perfect illustration of the effect of bias on people’s lives. This case led to the demands of enhanced measures in the deployment of AI in relation to public security and also the need for legislation that requires organizations to be fair in this space.

These concerns have in turn spurred creation of fairness principles and what is referred to as algorithmic auditing. However, the issue of real non-discrimination in case of AI is not an easy thing to manage. European legal scholars like Sandra Wachter have stated formally that while acts like the EU AI Act bring in major measures against bias in algorithms, more needs to be done. It must be noted that explainability and transparency are critical tenets to Wachter in arguing that without being able to explore why an AI system has made a particular decision, disentangling discrimination is almost impossible.

Thus, the impact of AI on issues of privacy, as well as non-discrimination, defines the extent to which such technologies shape the idea of human rights. Despite such progress being evidenced in the topic and these provided key points, real-life experiences and case and/ or empirical studies indicate that the process of achieving fair, transparent and accountable AI governance is not easy. Algorithms as the key component of AI should be audited, diverse people should be involved in AI development, and researchers should continue their work, with the help of proper legal frames.

2.3 Accountability Mechanisms

To highlight why AI Accountability matters, we got to pinpoint the scene. It's all about sticking to human rights and ethics when we use these techy things. These days, rules like GDPR are all about keeping people safe when computers make choices for them. The GDPR cooked up by the European Union, has these laws that make sure the folks handling data do it clean and straight. Take Article 22[4], yeah? It gives you the right to dodge decisions made by a computer when it's big stuff like jobs or your credit score. This legal backup drives home the point: we got to have real people checking on AI and setting up ways to fix any mess it might cause. Rights around the world also make up another accountability system. The International Covenant on Civil and Political Rights (ICCPR) Article 17[5], bans forced or illegal intrusions into someone's privacy. This has an influence on how AI systems gather data and keep an eye

[4] Council Regulation 2016/679, General Data Protection Regulation, art. 22, 2016 O.J. (L 119) 1 (EU).

[5] International Covenant on Civil and Political Rights art. 17, Dec. 19, 1966, 999 U.N.T.S. 171.

on stuff. The United Nations Guiding Principles on Business and Human Rights go even further insisting that companies must safeguard human rights. They got to handle any bad stuff that might happen because of the tech they create. So, these guidelines are all about checking for risks that could come from using AI and finding ways to reduce any problems.

Court battles are paying more attention to who's accountable with AI showing off both the wins and tough parts. In the UK Supreme Court, the Lloyd v. Google LLC (2021)[6] case tackled the question if people could get money for data wrongs without showing actual harm or upset. Even though in the end claiming money got harder, it highlighted how courts are starting to notice when a bunch of folks say hey, our data got mishandled. That's super important because AI systems are handling a ton of personal details.

Court decisions and expert reviews stress the need for accountability in automated choices to extend past simple rule-following. They suggest active checks and evaluations of dangers. Experts, including Ryan Calo, maintain that "algorithmic accountability" requires checks from the outside, like independent reviews, to judge prejudice and functional effects prior to using AI systems with high stakes. This method makes sure that not just the makers check the AI models, but also neutral parties boosting openness and confidence among the public.

Dealing with accountability keeps being a headache, and it gets knotty when we dive into the murky waters of AI's "black box." You know, that's where the brainy but hush-hush AI systems hide how they make choices. Pasquale's (2015) talked about this "black box society" thing, which says these murky AI setups dodge being checked out messing with holding them responsible. Then you've got the regulations squad, like the data watchdogs that GDPR put on the beat, and they're on a mission to make sure everyone plays by the rules. But here's the kicker: these watchdogs are trying to make do with what they've got, which isn't a lot making it tough for them to keep an eye on all the AI shenanigans that keep changing and spreading everywhere.

Lawmakers are rolling out new rules to tackle these tough spots. The "EU AI Act"[7] says high-

[6] Lloyd v. Google LLC [2021] UKSC 50

[7] John Ruggie, *Report of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises: Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework*, U.N. Doc. A/HRC/17/31 (Mar. 21, 2011).

risk AI stuff has got to have more checks, like making sure how they handle data, what they're doing, and keeping accurate records is all on point. Plus, this rule says people who make and use AI systems got to be able to explain how their tech works and what it does making them own up to their actions within the law books.

Wrapping things up even though stuff like the "GDPR" and global human rights laws started the job for AI answering-to-people stuff using them shows holes we've got to patch up. You can make AI more answerable by setting up tight records of what it does making it clearer how the algo-whatchamacallits decide things, and getting some big-shot groups to keep an eye on them. The next rules we make need to weigh cool new tech stuff against folks' trust in AI. We got to keep the human touch by putting rights and making sure we're doing the right thing first.

3. Balancing Innovation with Human Rights

3.1 Regulatory Challenges

In Europe various pilot programs are testing out ways to put these clear rules into action. Take Denmark's Data Ethics Council for example; they're running experiments to check if current AI setups respect these clear guidelines from the Act. What they're seeing at first glance is that even though the rules are pretty solid in theory real-world issues like not enough folks understanding data and not enough watchdogs to keep an eye on things could make these rules less potent.

Putting in place redress mechanisms that promise quick and just results turns out to be a sticky problem. Some smart folks point out that if we don't give enough cash and know-how to the people watching over things, the whole system for fighting back against AI choices might turn super slow and clunky. This could make people who got the short end of the stick think twice about going after what's fair. Plus, the whole deal depends a lot on each country's big shots to keep things in line. This could lead to a bit of a mess across the EU, cuz not all members are on the same page about how much effort and resources they're willing to pony up for these protections.

In a nutshell, the EU AI Act's human rights shields, like the need to be clear and ways to fix stuff, are huge leaps forward in AI rules. They show they're trying hard to fit human rights into the rules for AI tech. But to make this work, we need strong rule-enforcing stuff, we got to keep teaching folks how to understand data, and everyone, like folks who make laws big shot business peeps, and everyday people need to work together. If the EU can deal with these tough bits well, it might drop some wisdom on other places that want to set up the same kind of safeguards in their AI rule books.

Advancing AI super-fast makes it hard to set rules trying to make laws match up across countries and making sure rules can keep up with new tech. A big problem is trying to make different legal and cultural ways of controlling AI agree with each other. Like, the European Union (EU) insists on tough safety measures with its GDPR and the upcoming EU AI Act, but other places such as the United States like a more laid-back sectoral vibe that's all about boosting innovation. This mismatch is a headache for big tech companies that work in many places. It makes following the rules a pricey and tricky game.

One big problem is how fast AI tech changes. Old school rules take forever to make and use, and they can't keep up with the fresh AI stuff popping up super quick. People call this trouble "regulatory lag" cause the law's update speed isn't even close to how fast tech is moving. Folks who make the laws and rules get tangled up trying to make stuff that bends with new AI tricks but still works as rules. Plus, they're kind of scared to be too tough with rules because they don't want to kill the cool new ideas. They worry that if they're too strict, all the high-tech action might go to places where nobody cares about rules making everyone care even less about playing fair and safe.

People can't agree whether we need more rules or more new stuff. Some folks who like rules say that if we don't watch AI super, it's going to make unfairness way worse and step on our basic rights. They talk about times when computers made decisions that were not fair or messed with people's private lives. Now, Shoshana Zuboff talks a bunch about how if nobody keeps tech in line, it can get scary saying we got to have tough rules so people can stay in charge of their own lives and keep democracy safe.

Instead, supporters of policies that are nice to new ideas say that too many rules might slow down tech updates losing out on good stuff for the economy and people. They point out how AI could help in health checking out the environment, and learning stuff. They say if you make the rules too tight, it'll kill off the good changes. Big-brain folks like Andrew Ng reckon there's a sweet spot calling for smart rules that change depending on how risky an AI thing is. Stuff with high risk should have tougher checks, but things that aren't that dangerous could have an easier time with fewer rules. This would help new things happen while making sure they don't cause trouble.

3.2 Opportunities for Ethical Governance

Despite these hurdles, we have big chances to create rules that protect human rights while still allowing new ideas to flourish. One good way to do this is to weave ethical principles right into how AI is made making sure these technologies keep human rights in mind from the start. Canada has taken the lead here with its Directive on Automated Decision-Making. This rule says government departments using AI must check how their algorithms might affect people and make sure humans are always involved in making decisions. This shows how we can bake ethics and responsibility into the system without holding back progress.

Successful ethical governance also shows up in standards led by industry. The Partnership on AI, a group that includes big tech companies, NGOs, and research institutions, has created guidelines to promote fairness, openness, and responsibility. These optional frameworks, though not binding, push tech developers to adopt good practices and regulate themselves. This teamwork shows how an approach involving many parties - not just regulators, but also industry leaders and civil society - can create balanced, scalable, and flexible policies.

A suggested framework to govern AI involves setting up multi-stakeholder councils. These groups would include people from government agencies civil society, universities, and businesses. They would oversee and guide how AI policies are developed and put into action. By bringing in different viewpoints, these councils would be in a better position to tackle the complex wide-ranging effects of AI. This approach would help create policies that reflect what society values while also making room for new tech ideas.

For example, the OECD Principles on AI, which stress inclusion, fairness, and openness, serve as a key guide for AI policy in many countries. These principles have an impact on national plans by highlighting the need to develop ethical AI that matches democratic ideals and human rights. When countries adopt and adjust these guidelines into their own laws, they can make sure their policies cover all bases but still bend with new breakthroughs.

A key part of ethical AI management is to make transparency and explainability happen in AI systems. Using XAI methods can help algorithms give outputs that make sense allowing people affected and regulators to understand and question decisions. Steps to be more open, like keeping records and checking how algorithms affect things, would not just make AI more responsible but also help people trust it more. Setting up must-have openness rules, like the ones we see in money reporting, would set an example for how to handle high-risk AI systems. Public-private partnerships also offer a big chance to govern. When government groups team up with private tech companies, they can create rules that draw on real-world tech know-how while still putting the public's needs first. Take Finland's AI strategy as an example. It focuses on teaching people and working with businesses to develop AI in ways that help society as a whole. This shows that these team-ups can play a key role in striking the right balance.

AI governance that includes international teamwork helps stop rule differences that could create gaps and uneven protections. Joint global efforts, like those the Global Partnership on AI (GPAI) leads, aim to create unified standards that match human rights laws. This kind of teamwork can help set up a foundation for AI ethics and control making sure all involved parties work under the same accepted rules.

To wrap up, AI governance faces many big regulatory hurdles, but we can find ways to balance new ideas and human rights protection. Regulators should create flexible, risk-based rules that keep up with AI progress. AI design needs to include ethical guidelines, with clear practices and oversight from various groups to ensure responsibility and public confidence. These methods will help make sure AI growth matches what society values supporting long-term progress that respects both tech and human goals.

4. The EU AI Act

4.1 Diving into the Act

Say hello to the EU AI Act! This big move is all about laying down the law for artificial intelligence across the EU. The path to this Act wasn't just a stroll in the park - it went through loads of chats influenced by bunches of EU [8] white papers, crowds giving their two cents, and draft policies all about striking the right balance with AI rules. It all kicked off with the European Commission’s White Paper on Artificial Intelligence that dropped in February 2020.

[8] European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM (2021) 206 final (Apr. 21, 2021).

This pivotal doc put the spotlight on boosting innovation while ensuring our basic rights stay safe. Talking about "trustworthy" AI that gives a nod to European values got the ball rolling on figuring out how to whip up these rules without putting a damper on the techy progress.

People were worried about how AI was being used to watch over everyone and make big decisions without human input, and that's why lawmakers[9] felt they had to do something. When the cops in Europe started using face-scanning tech that a bunch of people didn't like, and there were problems with AI picking who should get loans more folks demanded rules to make sure things stayed fair. Groups fighting for our rights online, like European Digital Rights (EDRi), pushed to make sure the tech wouldn't discriminate or invade our privacy. Plus, the folks at the European Parliament were pretty anxious about whether AI could mess with how we run our democracies with worries about it being used to skew elections or spread fake news.

Creating the Act was a reaction to the pressing demand for strong legal tools to control AI's extensive influence on our world. The EU's[10] big plan, the Digital Strategy, set this up, and its goal was to get Europe ready for the tech era but still respect ethics. When lawmakers talked this over, they listened to different people involved, like tech firms, groups focused on rights, and the governments of EU countries. This shows how the EU wants to keep the peace between new ideas and making sure people's rights are safe.

4.2 Main Parts

Right at the centre of the EU AI Act you'll find this system that sorts AI stuff into four buckets: stuff that's just not okay super risky biz kind of risky, and no biggie. The whole point is to make sure rules fit how much an AI could mess with peeps' rights and safety.

Stuff on the unacceptable risk list is no-go zone because it clashes with what the EU is all about. Take for example those AI gadgets that some places might use for giving people scores on how they act—yeah, that's got vibes like that thing they got going on over in China's social credit system. The Act's like, "Nope, not going to happen," cause it's all about keeping AI from trampling everyone's freedom and what we stand for.

[9] *European Digital Rights (EDRi), "EDRi's Response to the European Commission's White Paper on AI" (2020), available at https://edri.org/.*

[10] European Commission, White Paper on Artificial Intelligence: A European Approach to Excellence and Trust, COM (2020) 65 final (Feb. 19, 2020), available at https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en.

AI systems that are labelled as high-risk have a huge influence on vital parts of our daily lives. Think stuff like job-related software, learning programs, police work gadgets, and super important equipment that keeps things running. Take those programs the banks use to decide if you get a loan or not, like credit scoring in banking — they're in this risky group. There's this wild story that shows what can go wrong if nobody's keeping an eye on these things — the Apple Card gender bias incident. It's when dudes got way better credit limits than ladies who were just as good on paper. Over in the EU, they're super serious about keeping these tricky AI tools in check. They're all about being clear about what the AI's doing making sure actual people can step in when needed, and checking up on everything to make sure all's good.

So there's this big argument about how we sort AI stuff, and it's kind of like a tug-o-war. Some folks reckon being super strict can slow down all the cool tech we could make, and it might make Europe's businesses fall behind everyone else. On the flip side, others believe having tough rules helps people feel good about AI, and that's super important if we want to keep coming up with smart ideas. Margrethe Vestager, who's the top dog for making Europe all digital and stuff, says, “trust is a prerequisite for technology to work for the people.” She's all about how we got to trust our tech.

AI setups like chatbots and some customer help tools tagged as "Limited risk," got to let folks know they're chatting with AI tech. They're doing this to bump up what people know and let them choose smarter. We picked up this trick because there were times when people talked to AI without a clue, and that stirred up some serious questions about what's right and what folks agree to.

Now, for the "Minimal risk" stuff, like loads of AI out there - think spam stoppers and computer games that think for themselves - they don't get watched over too much. We got this kind of like levels so the rules make sense putting the effort into checking out the big-deal AI stuff while the chill less risky new things get to grow without getting bogged down by tons of rules.

4.3 Digging into Cases and What They Mean in Real Life

The EU AI Act's rules make a difference in areas like healthcare and finance. Like, AI gadgets that doctors use to check on patients or figure out what's making them sick are seen as super risky cause they could mess up someone's health or spill their secrets., a bunch of research showed that sometimes these AI thingies can get it wrong cause of biases against certain races or genders, which isn't cool for folks who aren't in the majority. The Act's big plan is to make sure there's a clear view and tight control over stuff that's risky so everybody gets a fair shake. In finance, people are always checking the "credit assessments" algorithms because the old data they use often shows unfair biases that existed before. The EU's Artificial Intelligence Act wants to fix this with regular check-ups and making the algorithms' workings clear so everyone gets a fair shake.

4.3 Protection of Human Rights

The EU AI Act features specific sections tailored to protect human freedoms sticking true to the EU's dedication to moral AI use[11]. The heart of these defences includes clear rules and ways to help folks hit by AI get help for any complaints. These steps strive to strike a fair balance seeing that AI can push society forward but also threaten basic rights like privacy, being treated the same, and not facing bias.

The Act considers "transparency obligations"[12] super important. Rules say that AI setups with high risk must stick to tough transparency rules. They got to have clear records that explain what they're for where they get their data, and how they make choices. They want to fix the whole "black box" problem[13]. That's when it's all hush-hush about how AI makes decisions that mess with people's lives. Like when someone gets a no-go on their loan application or doesn't snag a job, and they're left scratching their heads wondering why. The EU AI Act says hold up, you need to give those folks some answers. It's about keeping things straight-up and building trust with the users.

So, you've got these things called redress mechanisms that are super important for protecting people's rights. Here's the deal: the law says that folks should be able to seek legal remedies whenever they feel like some AI system stepped on their rights. This part of the rule is all about giving people the power to stand up against computer-made choices that seem shady or just plain wrong. Take someone who figures an AI hiring gadget was unfair during the job hunt

[11] European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM (2021) 206 final (Apr. 21, 2021), available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

[12] Andrea Renda, "Artificial Intelligence and Human Rights: The AI Act and the Need for Meaningful Transparency," 47 *CEPS Policy Brief* 1, available at https://www.ceps.eu/.

[13] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* 19-21 (Harvard Univ. Press 2015).

because of their sex or where they come from. They have the opportunity to seek redress. It's kind of like what the General Data Protection Regulation (GDPR) talks about. People already have the permission to say "nope" to choices made without human touch.

Experts foresee hurdles when enforcing these safeguards transparency rules. Senior researcher Dr. Andrea Renda from Centre for European Policy Studies (CEPS) highlights a big snag: although the Act calls for openness, the intricate nature of certain AI systems can stump those who have to check and grasp their decision-making. This problem gets tougher with private tech because firms keep their algorithms secret, which bumps heads with the need to follow regulations.

In Europe various pilot programs are testing out ways to put these clear rules into action. Take Denmark's Data Ethics Council for example; they're running experiments to check if current AI setups respect these clear guidelines from the Act. What they're seeing at first glance is that even though the rules are pretty solid in theory real-world issues like not enough folks understanding data and not enough watchdogs to keep an eye on things could make these rules less potent.

Putting in place redress mechanisms[14] that promise quick and just results turns out to be a sticky problem. Some smart folks point out that if we don't give enough cash and know-how to the people watching over things, the whole system for fighting back against AI choices might turn super slow and clunky. This could make people who got the short end of the stick think twice about going after what's fair. Plus, the whole deal depends a lot on each country's big shots to keep things in line. This could lead to a bit of a mess across the EU, cut not all members are on the same page about how much effort and resources they're willing to pony up for these protections.

In a nutshell, the EU AI Act's human rights shields, like the need to be clear and ways to fix stuff, are huge leaps forward in AI rules. They show they're trying hard to fit human rights into the rules for AI tech. But to make this work, we need strong rule-enforcing stuff, we got to keep teaching folks how to understand data, and everyone, like folks who make laws big shot

[14] Bart Custers, "The Power of Data Protection Rights: The GDPR as a Model for Other Jurisdictions," 10 *Journal of Law and Innovation* 213 (2021), available at https://scholarship.law.upenn.edu/jli/.

business peeps, and everyday people need to work together. If the EU can deal with these tough bits well, it might drop some wisdom on other places that want to set up the same kind of safeguards in their AI rule books.

5. Integrating Theoretical Insights and Real-World Case Studies

Thus, by employing theoretical approaches, including utilitarianism, proportionality, and legal pluralism as well as human-centric AI, this review is configured to reveal that AI regulation is a complex process. Some examples from real-life situations[15] mentioned, for example, in connection with the EU's AI act [16]can be used to explain the meaning of proportionality, namely how it is used in practice to safeguard human rights and promote innovation. Comparing the U.S. approach to AI regulation which is more fragmented and less integrated than the EU's can also help understand how the differences in regulatory outlook are reflected in real life cases Besides, the experience of non- Western countries is also crucial for a global perspective. The examination of China's SCS [17]demonstrates that AI regulation and deployment in that country put state power first, causing concerns of potential human rights violations. This is very much different from the frameworks in democratic societies centred on civil liberties. Examining these approaches fits the methodological question into the more general theoretical question of whether general frameworks for the governance of AI are possible or whether localized frameworks are more suitable to meet the needs of diverse societies. To sum it up, there is still a baseline of research on AI and human rights, but there are many research gaps, such as the long-term socio-macroeconomic impact of AI, the failure to provide accountability to developing countries, and cross Thus, future regulations have sound anchors in utilitarianism, proportionality, and human AF principles that respect human rights and foster innovation. The state of discussion on how AI affects human rights and subsequent regulatory efforts and where the literature lacks dossier gaps is long term socio-economic impacts of AI and non-western voices. Basis for today's legal frameworks like utilitarianism and proportionality need to be in tandem with ideas from philosophy and ethical assertions, but practicality needs uninterrupted discourse with philosophy and ethics for proper governance.

[15] Robert Alexy, *A Theory of Constitutional Rights*, 66-69 (Julian Rivers trans., Oxford Univ. Press 2002)

[16] European Commission, Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), COM (2021) 206 final (Apr. 21, 2021), available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

[17] Rogier Creemers et al., *China's Social Credit System: A Model for Other Countries?*, 34 *Journal of European Policy* 102 (2020).

6. Conclusion

6.1 Summary of Findings

This research paper looks into the complex link between AI technologies and human rights. It tackles both AI's power to change things and the problems it brings up. The talks highlight AI's two sides: it can boost efficiency and accuracy in areas like healthcare and finance, but it also raises serious concerns about privacy, discrimination, and who's responsible.

The main findings show that AI has big upsides—like better diagnostic tools and predictive analytics—but also major risks such as privacy violations and biased algorithms. Looking at cases like Clearview AI's face recognition tech and the Cambridge Analytica mess shows we need strong rules. The EU AI Act is a big step to deal with these issues. It suggests regulating AI based on how risky it is. But it's clear that AI tech is so complex that laws need to keep changing to stay useful and flexible enough to keep up with fast tech progress.

The paper sheds light on how crucial it is to have systems in place to hold AI accountable. While rules like the GDPR provide some safeguards, there are still areas where we lack openness and ways to fix problems. A key point in the analysis is that we need to take a broader view when it comes to controlling AI. This approach should think about human rights at every step, from when AI is first created to when it's put to use.

6.2 Implications for Policy and Practice

This study's results carry weight for those who make and carry out policies. For those who craft laws, what we've learned about current rules points to a need for flexible laws that can keep up with how AI tech changes. The EU AI Act shows we urgently need laws that don't just push for new tech but also protect basic human rights. Those who make laws must see that new ideas and protecting rights can work together when done right.

To strike this balance, those who work with AI—from creators to companies—need to think about human rights when they design and build their systems. They might use ethical rules and plans, check for risks to human rights, and work in ways that cut down on bias in AI systems. When tech makers, law experts, and regular people work together, we can create AI tech that's not just new and clever, but also careful and in line with human rights rules.

6.3 Future Research Directions

Moving forward, a few up-and-coming trends need more digging into when we're talking about AI rules and stuff. A big thing to watch is how quantum computing might mess with AI manners and what that means for keeping our data secret and safe. See, as quantum stuff gets better old ways to keep info locked up might not work anymore. That's got people thinking about how we make sure private details stay private.

Plus, the tough situations that countries in the global South deal with call for their own research. A bunch of places down there are starting to grab AI tech, but they don't all have solid rules to manage it yet. It's super important to get what's going on, money-wise, culture-wise, and law-wise when it comes to steering AI in these spots. Upcoming research might look at tweaking worldwide guidelines to better fit what the global South needs making sure everyone's got a fair shake when it comes to AI rules.

Overall, as AI keeps getting better and spreading into more parts of society looking at how tech and human rights hang out together is super important. This piece has set the stage to dive deeper into ways laws can change to look after human rights while still giving innovation a thumbs up. Finding the sweet spot between these big deals is mega important, not just for putting AI to good use without being sketchy, but also for making sure people stay respected and dignified in a world where everything's going digital.