ISSN: 3107-7161 (Online)

Technological Progress vs. Human Rights: Privacy, Free Expression, and Reputation in the Era of A.I and Deepfakes

By: 1) N. Likhitha Prasad, Jain School of Law (Deemed to Be) University, E-mail id: nlikithaprasad@gmail.com.

2) Ishika D Jain, Jain School of Law (Deemed to Be) University.

ABSTRACT

The 21st century technology has totally transformed the way we socialize, communicate and participate in the society. Technology has become an integral part of the exercise of fundamental rights - altering the whole tenor of what liberty, dignity, and accountability mean in the modern world. With all these digital platforms, AI, and synthetic media, we have new ways to jump in and make money and trade knowledge, but it also opens up new cracks through which people can be vulnerable.

Technology has drastically changed our perception of human rights; privacy, expression, and reputation are top of our list. In the digital era, people are aggregating and archiving personal information at an unparalleled pace via social media, surveillance and artificial intelligence, thus setting up a genuine contest between state security and privacy. AI-enabled surveillance tools - including predictive policing, facial recognition and mass surveillance - tend to discourage dissent and force people into self-censorship, ultimately eroding our freedom of expression.

At the same time, deepfakes are destroying the right to reputation by allowing people to create hyper-real but false content that can destroy credibility, mislead, and disrupt democratic discourse. Even if courts and lawmakers are trying to keep up with privacy rights, data protection laws, and defamation rules, they still can't keep up with all the emerging threats.

The right to privacy is in a losing battle against mass surveillance, data harvest mishaps and those algorithmic "profiles" that blur the lines between consent and brain-washing. AI is accelerating the development of surveillance that can dictate our behaviour, suppress people's thoughts and speech, causing some to keep their heads down, others to scream in terror. And deepfakes - which use machine learning - get to the heart of who we are, by creating almost-

ISSN: 3107-7161 (Online)

unrecognizable fake content that spreads lie, sows distrust and undermines democracy. These issues transcend borders; thus, we truly need internationally applicable legal rules and standards, firm ethical standards. Yes, new tools allow us to get connected and to learn faster, but they also raise significant concerns about the extent to which we are in fact free, about government surveillance, about the restrictions on free speech, and about the ways in which our reputation can be damaged. In my paper, I'll examine the right to privacy online, the chilling effect of AI-powered spying on people's free speech rights, and how deepfakes can harm people's reputations. I'll take a look at the current laws and court cases and the hot debates in this arena and then propose how we can strike a balance between growing the tech and defending our human rights.

This paper explores the intersection of technological advancement and human rights, emphasizing the critical need to establish governance frameworks that balance technological innovation with the preservation of human autonomy, integrity, and dignity. The bottom line? We're not interested in hating tech; we're just interested in making sure that it develops in a way that reinforces the global human-rights system, not undermines it.

keywords: Technology, Artificial Intelligence, Privacy, Fundamental Rights, Surveillance Tools.

INTRODUCTION

The last two decades have seen adequate increase in technology that captures, processes and utilises individual data. Smartphones, cloud-based computing platforms, ubiquitous sensors and social media have all contributed to the development of this digital world where we all create digital footprints on a universal scale. Those footprints have a great value; they enable customised services, simplify governance and power innovation. But data can be misused in other ways: breaching business partner data, biassed and automated decisions, blocking dissident voices, educative media smearing reputations - outcomes that as well as being experienced as a private harm, spill out into civic harm. Human rights norms (UDHR, ICCPR, ECHR and constitutional protections in jurisdictions) entrench privacy, freedom of expression, and reputation as fundamentals. These are conceptually robust but operationally threatened by technical complexity, cross-border data flows, and platform dominance. Courts and legislatures

ISSN: 3107-7161 (Online)

have started to evolve, but regulatory solutions are patchy. This article explores the essential legal contradictions and charts practical solutions that integrate law, technology design, corporate.

Technology is increasingly becoming a major factor in both the enjoyment and infringement of fundamental rights. In the digital world, the power that states and corporations have over our personal data, communication, and individual identity is greater than ever before. On the one hand, artificial intelligence can lead to better governance, on the other hand, it can make the practice of mass surveillance easier, thus, putting our privacy and autonomy at risk. At the same time, the deepfake technology is getting better at distorting the facts, thereby, making the victim's reputation be at stake and losing the victim's trust in others. These changes have posed challenging questions in law, ethics, and society about human rights protection. The present research explores these different aspects by studying the impact of emerging technologies on traditional rights frameworks and by examining the potential ways in which rights to privacy, freedom of expression, and personal integrity can be safe-guarded in an ever-increasingly digital world.

OBJECTIVE OF THE PAPER

This study aims to critically analyse the way in which core human rights are being redefined by tech changes. In essence, we would like to examine how privacy is being knocked out by the ongoing data collecting and surveillance measures that are interfering with our privacy. We would also like to examine the effect of AI-enabled surveillance systems on the freedom of speech, and how surveillance can suppress free discussion and speech. The other important objective is to evaluate the pitfalls of deepfakes, how they can be used to destroy personal reputation and bend the truth. Lastly, we are considering the effectiveness of the existing legal frameworks and reforms and seeking opportunities to reconcile the advances in technology with human dignity and rights.

RESEARCH PROBLEM

ISSN: 3107-7161 (Online)

This study is aimed at finding a solution to one of the major issues in the world today, that being the conflict between the advancement of technology and the safeguarding of basic human rights. In this article we are examining the collision of technology advancements and fundamental human rights. Although we have constitutional protections and global regulations, emerging technology continues to allow individuals to invade our privacy, strangle the freedom of expression, and sabotage our image. The collection of masses of data, AI-based surveillance, and deep-fakes are aspects of a larger issue that is undermining our democracy and dignity. These problems affect the most vulnerable ones first, and this is how fragile our laws are and worries us as to who is really responsible in the digital age.

HYPOTHESIS

In essence, this paper believes that tech is becoming so rapid that, in as much as it is enabling a myriad of exciting opportunities regarding innovation and governance, it is also wreaking a massive wrench on the entire human-rights game. More so, it is stripping people of their privacy, right of expression and reputation, basically, when we refer to the uncontrolled use of digital surveillance, AI, and deepfake technology. Unless we establish sound legal frameworks and ethical controls, such tools will continue to inflict violations, disproportionately affecting the vulnerable population, and undermining democracy (and law) in the eyes of the population.

RESEARCH METHODOLOGY

The study research methods legislation, primarily doctrinal and analytical. As a core part of the research, the researchers reviewed legal instruments, e.g., constitutional provisions, laws, and recognized human rights treaties to understand the rights to privacy issue, freedom of speech, and image protection in the digital era.

The research also operates case law through determining the courts' interpretation and reaction to the technology that causes problems in fields such as digital surveillance, AI governance, and deepfake-related offenses. To understand the best and find the deficits in the present legal regimes, the authors examined the worldwide cases like the EU's GDPR and AI ethics

ISSN: 3107-7161 (Online)

guidelines. Such a method facilitates a profound comprehension of the technology-human rights nexus, thus identifying those areas of a potential reform and policy interventions.

RESEARCH QUESTIONS

1) In what ways does the use of artificial intelligence in surveillance systems affect freedom of expression, and how does the resulting chilling effect influence individual behaviour and public discourse?
2) What are the legal, ethical, and social challenges posed by deepfake technology, particularly concerning personal reputation, misinformation, and the manipulation of public perception?
3) To what extent do existing national and international legal frameworks address the risks posed by emerging technologies, and where do significant gaps or inconsistencies exist?
4) How can policymakers, courts, and regulatory bodies balance technological innovation with the protection of fundamental human rights, ensuring accountability, transparency, and fairness in the use of digital tools?

LITERATURE REVIEW

1. **"The Right to Privacy" remain relevant in the digital era, and how have they influenced contemporary jurisprudence on privacy in India and globally?**

   The pioneer essay on the right to privacy, essentially denotes that every one of us is entitled to possess a basic right over our personal data and to remain undisturbed by invasive inquiries. India demonstrates the extent to which these ideas remain relevant by its courts. In Justice K.S. Puttaswamy v. The Supreme Court, Union of India (2017) 10 SCC 1, opined that privacy is inherent to life and liberty in the second Article of the Constitution, Article 21.

   Concisely, the masterpiece is one of the pillars when it comes to the framing of privacy as a fundamental human right. They have had an immense impact on the course of

ISSN: 3107-7161 (Online)

history, law, and even the modern tech industry, which provides a firm theoretical basis of court rulings, legislative modifications, and arguments on digital privacy. Their beliefs continue to inform the contemporary jurisprudence in India and other parts of the world proving that despite the changing nature of technology, the fundamental human right of privacy requires unremitting attention.

2. **How can privacy be understood as a multifaceted and relational right in the digital era, and what frameworks can be used to identify and address contemporary privacy violations arising from advanced technologies?**

   Privacy in the new millennium is not a simple legal right, but a mess of issues that encroaches on our personal lives as well as the operations of institutions. Speaking of privacy breaches, they come in a multiplicity of forms data collecting, processing, sharing, even literally intrusion. To add to that, even international regulations such as the General Data Protection Regulation (GDPR) of the EU attempt to follow this complicated image. They provide us with the rights to verify information, correct errors, transfer data and to delete it- to address not only the question of data collection but the question of data utilization.

   Therefore, in fact, the application of privacy as a multi-layered perspective is of relevance to current changes in law and policy. It takes the measure of the cleverness and entrenched nature of the new threats, but provides us with a solid framework through which to Mold our decisions in court and legislation to safeguard our liberties in the digital era of everything.

3. **How does the collection and monetization of personal data by corporations through advanced technologies impact individual autonomy, freedom of expression, and democratic participation?**

   Corporate data collection on a massive scale, analysing and selling of our private digital footprints are the main factors that have changed the traditional power balance between the 'users of the digital space' and the 'providers'. The new economic system, often referred to as "surveillance capitalism", is essentially keeping detailed records of people's habits, preferences and communications. Beside this, AI technologies like

ISSN: 3107-7161 (Online)

machine learning, using huge data sets can form predictive models which further empower AI surveillance. This kind of high-tech monitoring is not only absolute but also is present not far away from the person, being sometimes hidden and opaque at the same time. This chain of events is called "chilling effect", where individuals are afraid to talk, participate or practice democratic rights as they fear negative consequences if they happen to be watched by false friends: corporations and government authorities.

ANALYSIS

1) In what ways does the use of artificial intelligence in surveillance systems affect freedom of expression, and how does the resulting chilling effect influence individual behaviour and public discourse?

The emergence of AI in surveillance has completely revolutionized the way we consider the freedom of expression, not only in India but also in the rest of the world. The algorithms of AI, such as face recognition or predictive policing and surveillance of big data, allow the police to spy on us, in ways that never crossed our minds before. Although the governments may claim it to be in the name of security, the sheer extent of such systems puts a chilling effect making people censor themselves and to restrain their thoughts and opinions in open places.

In India, free speech is guaranteed by the Constitution through Article 19(1)(a) but with also reasonable restrictions through Article 19(2) of the Constitution regarding factors such as security or orderly conduct. A good example is the 2015 ruling of Shreya Singhal v. Union of India (2015) 5 SCC 1, where the Supreme Court struck down Section 66A of the Information Technology Act, emphasizing that vague or overbroad provisions which suppress speech violate the essence of free expression. It demonstrates that in case any monitoring tool is too general or vague, it can lead to the lack of trust that individuals have in expressing themselves freely.

In 2017, Justice K.S. Puttaswamy v. Union of India (2017) 10 SCC 1, added privacy to the list of things that are associated with expression. As the Court stated that privacy is fundamental to the right to live and liberty, it was made clear that invading the privacy of the individual is more difficult in a world where AI traces every step and discussion,

ISSN: 3107-7161 (Online)

making people less free to express themselves. That sense of being followed continuously will drive us towards self-censorship and less engagement with the public.

Likewise, the Supreme Court in the U.S. in the case of Carpenter v. United States (2018) 585 U.S., determined that a warrantless collection of cell-site data is a Fourth Amendment search. Even such decisions, despite their orientation on privacy, point to the uncontrollable data fuelling behavioural shifts such as closing down discourse or suppressing opinions. The awareness that we are being tracked by the algorithms makes most of us pause and reconsider joining a heated discussion or a social cause more than ever, whether it is in India, where activism and whistleblowing are usually enacted via digital platforms. It is even more chilling when users edit their posts, avoid polarised content, or avoid politics altogether since they are afraid of being flagged or criticised alarmingly. When citizens fear to protest, express their views, or speak out against injustice then a democracy is undermined by a weak public debate, a decrease in civic participation and by the mere fact that democracy has suffered a blow. In India, where social media has become a key instrument of organising crowds and highlighting corruption, excessive AI surveillance is posing a threat to the very heart of our democracy.

The Puttaswamy Case decision teaches us that privacy should not be sacrificed on the altar of any state objective, and the GDPR demonstrates the possibility to check the use of data to safeguard the rights of citizens. In a word, then, AI surveillance is a two-sided sword. Although it makes governance and security leaner, it is a threat to the freedom of expression as it generates an all-seeing-eye in every person. Indian and foreign courts have demonstrated that unregulated, particularly automated, surveillance is detrimental to autonomy, encourages self-censorship and undermines democratic discourse. The best way to safeguard free speech in this AI age would be to establish solid legal and ethical technology defences to ensure that innovation does not pose a danger to our most basic rights.

ISSN: 3107-7161 (Online)

2) What are the legal, ethical, and social challenges posed by deepfake technology, particularly concerning personal reputation, misinformation, and the manipulation of public perception?

Deepfake technology, which involves applying AI to create audio-visual content that appears to be super real, but which is in fact fake, is proving to be a huge source of legal, ethical, and social headaches. It confuses the reputation of people, misleads and provides bad strangers with a means to skew the image of the world. Deepfakes can completely ruin personal identity and expose individuals to severe defamation when a video or image depicts someone saying or doing something that they never did, even though it may appear to be convincing in a crazy way. On social media where content goes viral in seconds, a single deepfake can begin to balloon and inflict serious irreparable damage before anyone can even fact-check or perform any kind of remediation.

In legal perspective tools available today simply do not cut it. In India, laws such as Information Technology Act of 2000 and the Indian Penal Code (66D cheating by impersonation and 499-500 defamation) play a minor role, though these were not designed to be able to move at AI-scale or its quirks. The case of Shreya Singhal v. Union of India, by the Supreme Court, explained that regulation must be specific to prevent the stifling of speech. The same cautious attitude can be used with regard to deepfakes. Courts all over the world are beginning to have it: In United States v. Christensen (2019), Adding to the fact that a specific legal approach is required, claimed that deepfake video used in fraud or harassment is regarded as criminal acts.

Fake speeches by officials are political deepfakes which pose a danger to democracy. During the 2020 election in the U.S., AI videos circulated with fake information, influenced the masses, and even changed the votes. It has been demonstrated in India that unchecked deepfakes have triggered unrest among politicians or fuelled communal rumours, which caused unrest in India by utilizing fake videos. On the social level, deepfakes destroy media and general information trust. It is not only that victims get to bear the brunt of public scrutiny, but also that they experience mental stress, harassment, and depression. It is even more deplorable when deepfakes are directed at gender or minority groups as they are used to suppress and intimidate those voices.

ISSN: 3107-7161 (Online)

Lastly, education of the masses is essential-- make users aware of verifying content before posting and this can reduce reputational and social losses.

In a word, deepfakes combine legal, ethical, and social risks in such a manner that endangers the personal reputation and social credibility. By remaining silent, we will be running the risk of destroying the rights of individuality and the democratic fabric in this digital media age.

3) To what extent do existing national and international legal frameworks address the risks posed by emerging technologies, and where do significant gaps or inconsistencies exist?

Current national and international legal regimes provide partial coverage of the threats of new technologies with significant gaps and inconsistencies remaining. The Indian Constitution provides privacy (Article 21) and freedom of speech (Article 19 (1) (a)). The ruling of the Supreme Court in 2017 in the case Justice K.S. Puttaswamy vs. Union of India (10SCC1), The right to privacy was also established as a fundamental right. The digital communications and the online data processing are regulated by the Information Technology Act of 2000 and the Digital Personal Data Protection Act of 2023. But these laws tend to lag behind the faster technological innovation, and it is unclear how AI surveillance, algorithmic profiling, and synthetic media like deepfakes might be regulated.

Stronger norms exist internationally with the General Data Protection Regulation (GDPR) by the European Union and the upcoming AI Act. The GDPR puts as well as rigid regulations on data collection, data processing, and data consent, and the AI act focuses on high-risk AI systems to avoid discrimination, prejudice, and privacy breaches. Big Brother Watch v. United Kingdom (2018) 64 EHRR 1 of Human Rights. it was held that mass surveillance without prior notice infringed the rights in Article 8 of the European Convention on Human Rights creating a worldwide privacy standard. The case of United States (2018) affirmed that digital location data collection is considered a search, and the Fourth Amendment privacy rights are upheld. Although these innovations have been made, there are many jurisdictions that do not have detailed

ISSN: 3107-7161 (Online)

regulations on deepfakes, AI-based surveillance and algorithmic decision-making. The AI ethics frameworks in India are present in the form of advisory statements only; thus, they are not uniformly enforced. Countries such as China have adopted large-scale surveillance with few protections on individual freedoms, a contrast to the narrower protection of individual freedoms advocated by GDPR in the rest of the world.

Overall, national and international frameworks offer a conceptual framework to deal with the threats of emerging technologies, but are broadly reactive and disjointed. The development of AI, data analytics, and synthetic media reveal the loopholes in the legal coverage, enforcement procedures, and ethical regulation. As a result, integrative and future-oriented regulatory policies are in great demand.

4) **How can policymakers, courts, and regulatory bodies balance technological innovation with the protection of fundamental human rights, ensuring accountability, transparency, and fairness in the use of digital tools?**

Policymakers, courts and regulators need to take a holistic approach to balance both technological innovation and the safety of basic human rights. Artificial intelligence, big-data analytics, and deepfakes can be used to enhance governance and improve services to people, but pose a risk to privacy, freedom of expression, and reputation. In order to avoid these risks, we must have explicit laws, judicial checks, and balances, ethical standards, and mechanisms that will keep the people in the know.

The digital age has been limited significantly by the courts in India. In the 2017, the case K.S. Puttaswamy v. Union of India, The Supreme Court declared the right to privacy as the fundamental right. It stated that any state intervention concerning personal data was to be legal, necessary and proportionate. It was also ruled that state surveillance and AI tools need to be transparent and open to control. In 2015 in Shreya Singhal v. union of India, a similar message was received, the Court decided that any regulation of online speech has to be defined in a limited manner to prevent the ability to censor legitimate debate. These two rulings support the idea that technology needs to be controlled in a just manner.

ISSN: 3107-7161 (Online)

Various models are used to demonstrate the ways of balancing innovation and rights across the world. The General Data Protection Regulation of the European Union has stringent data processing requirements, which demand consent, restrictions of purpose, transparency and accountability. The EU Artificial Intelligence Act submitted will group AI systems based on risk and impose responsibilities on risky uses of AI applications, so they are safe and just. The application requires both technological and ethical protection. Those who design AI must establish it with fairness, accountability, and explainability. As an example, AI is used in social media to identify deepfakes and provide users with the opportunity to report suspicious posts together with technical detection and regulatory policies to safeguard users. In terms of ethics, companies should celebrate autonomy, consent and dignity. Deepfake technology may be utilized with entertainment or education purposes, but it is misused as a means of harassing others, misinformation, or manipulating politics has to be highly restricted. Singapore and the United Kingdom have developed legislation that criminalises harmful deepfakes. All these demonstrate that technology can go hand in hand with proactive laws. Government -business collaboration may drive innovations and protect safety. Civil society and academicians assist in evaluating the social effects and suggests moral principles.

To sum up, the issue of technological advancement and primary rights is a never-ending process. It is established in the case law and international structures that AI, surveillance and use of synthetic media should be guided by accountability, transparency and proportionality. It is important that policymakers and regulators should be forward-looking, ethically informed to build democracy instead of undermining privacy, freedom, and social trust.

CONCLUSION

Technology has transformed the way human rights are used, abused and guarded. The use of AI monitoring, mass surveillance, and deepfake has established the environment where privacy, free speech, and reputation are threatened. We have found that these threats are international rather than local. They are based on loopholes in the law, technological authority,

ISSN: 3107-7161 (Online)

and morality as grey areas. There is a possibility that technology can enhance efficiency, connectivity and governance. But unless more proactive rules are put in place, democratic values and human dignity may be threatened. Flexible frameworks should now be developed by policymakers and regulators. Courts have to continue their interpretation of rights according to a digital world.

To sum up, technology and human rights have to co-exist. This is key to a working democracy and requires vigilance, moral prescience and collective government. Being a student who is living in an era of rapid digital transformation, I understand that ensuring autonomy, privacy, and reputation is not only a legal issue, but a moral one, as well. Our ability to combine both innovation and accountability will determine the future of human rights and therefore technology is not a servant but a master of people.

REFERENCES

1) Solove, D. J. (2008) “Understanding privacy” - Harvard University Press.

2) Zuboff, S. (2019) “The age of surveillance capitalism” - The fight for a human future at the new frontier of power, PublicAffairs.

3) Warren, S. D., & Brandeis, L. D. (1890), “The right to privacy” Harvard Law Review, 4(5), 193–220.

4) Citron, D. K., & Chesney, R. (2019) “Deep fakes and the law”: Challenges and responses, Oxford University Press.

5) Citron, D. K., & Chesney, R. (2019) “Deep fakes: A looming challenge for privacy, democracy, and national security” - California Law Review, 107(6), 1753–1819.

6) Solove, D. J. (2021) “Privacy harms in the digital age” - Stanford Law Review, 73(5), 1383–1425.

7) Zuboff, S. (2015) “Big other: Surveillance capitalism and the prospects of an information civilization” -Journal of Information Technology, 30(1), 75–89.

8) Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

ISSN: 3107-7161 (Online)

9) Shreya Singhal v. Union of India, (2015) 5 SCC 1.

10) Big Brother Watch v. United Kingdom, (2018) 64 EHRR 1.

11) Carpenter v. United States, 585 U.S (2018).

12) European Commission (2021), Proposal for a regulation laying down harmonized rules on artificial intelligence (Artificial Intelligence Act), Retrieved from https://eur-lex.europa.eu/search.html?scope=EURLEX&text=Proposal+for+a+regulation+laying+down+harmonized+rules+on+artificial+intelligence+%28Artificial+Intelligence+Act%29&lang=en&type=quick&qid=1759135483743