International Journal of Modern Agriculture, Volume 10, No.2, 2021
ISSN: 2305-7246

IS AI-BASED SURVEILLANCE AND FACIAL RECOGNITION TECHNOLOGY DEVALUING HUMAN RIGHTS?

Aarya Chhangani[1], Priyanka Majumdar[2]*

[1,2] Symbiosis Law School, Pune,, Symbiosis International (Deemed University), Pune, India

[2]*Email: priyanka.majumdar@symlaw.ac.in

Abstract

Innovations in Artificial Intelligence technology have demonstrated great potential to advance the society by alleviating some of the world's most significant problems, which is a way forward towards the attainment of the UN Sustainable Development Goals. These technological advancements enable mass surveillance by the State to track, monitor, and digitally surveil its citizens through facial recognition technology. As facial recognition systems are rapidly proliferating, its propensity to unjustifiably interfere with human rights, such as privacy, data protection, equality and non-discrimination further escalates. In consideration of the fact that Artificial Intelligence (AI) technology has not yet attained its highest level of advancement, this paper aims to study the impact of AI-based surveillance and facial recognition technology on human rights at present and its potential impact in the future. Based on doctrinal research, this paper analyses the positive and negative impact of deployment of AI technology in the European Union and India upon human rights. This paper evaluates the governance of AI technology through existing laws in the EU from a human rights perspective. It is highly imperative for India to formulate an AI governance mechanism to protect against abuse of human rights. Drawing from the best practices of EU, this paper suggests some considerations relevant for formulating a regulatory or policy framework for AI-based surveillance in India.

Key words: Artificial Intelligence, Bias, Data Protection, Discrimination, European Union, Facial Recognition, Human Rights, India, Privacy, Surveillance, Sustainable Development Goals.

Introduction

Artificial Intelligence (AI)"traditionally refers to the scientific pursuit of teaching machines to think like humans. AI is often used as an umbrella term that covers several sub disciplines"(Chollet, 2017). It has a profound presence in our everyday lives. The AI applications range from curating entertainment and social media feeds to making recommendations on e-commerce websites, and from unmanned automobiles to utility applications such as virtual smart assistants, speech recognition, web filtering and web browsers (Feldstein S. , 2019).The classic concept of AI dates back to 1956, when John McCarthy along with other researchers identified AI as "making a machine behave in ways that would be called intelligent if a person was to act in that way" (Smith, 2006), Succinctly put, AI, can be viewed as a "reservoir of smart agency on tap."(Floridi & Cowls, 2019). AI has been highly prominent in the discourse of academia, government and business professionals with regards to its application. Perhaps, the most distinctive characteristic of AI is its instantaneous ubiquity. As the advancement in technology progresses, the AI-based surveillance tools have amplified as it simplifies the conduct of surveillance coupled with increased efficiency. The most permeating use of these technologies is the increasing deployment by the government for the purpose of surveillance and law enforcement. (Parsheera, 2019). The "AI Global Surveillance Index" released by the Carnegie Endowment for International Peace reveals that there is evidence from around the globe of the use of facial recognition technology by both democratic as well as authoritarian states, as 85% of the countries they studied (64 out of 75 countries) were deploying facial recognition system for the purpose of surveillance. As of May 2020, at least 15 European countries, including the UK, Denmark, Czech Republic, Germany, France, Hungary, Greece, Italy,

International Journal of Modern Agriculture, Volume 10, No.2, 2021
ISSN: 2305-7246

Poland, Netherlands, Romania, Slovenia, Serbia, Sweden and Switzerland have experimented with the use of biometric technologies for mass surveillance.

Responsible implementation of AI can yield significant productive benefits. Responsible and fair AI also has the ability to deliver new ways of protecting and upholding human rights. They may be used to track and record human rights violations (Koettl, 2018); and can be highly instrumental in the achievement of the United Nations Sustainable Development Goals (SDGs) (UN Global Pulse, 2019). These goals are aimed at enhancing protection and promotion of human rights at a global level and are complementary to the basic objective of promoting wellbeing of all the people. AI based facial recognition technology can help in achieving the UN SDGs, especially SDG 1 (No poverty), SDG 2 (zero hunger), SDG 3 (Ensure good health and well-being), SDG 10 (Reducing Inequalities) and SDG 16 (Promoting peace, justice and strong institutions). For example, in the US, Kenya and Ethiopia, a social enterprise named "Kimetrica" is working on a project called "Method for Extremely Rapid Observation of Nutritional Status" (MERON), in which machine learning uses photos and extracts facial images to detect malnutrition(Abbany, 2018). Facial recognition can also be used to analyse images for diagnosing oral cancer (Abbany, 2018). The application of AI must be coupled with the benefits of technology which help in achieving the SDGs, and guarantees socio-economic and political rights in consonance with the international standards to ensure that basic human rights are guaranteed to every citizen (Schutter, Ramasastry, Taylor, & Thompson, 2012).

However, big data and AI also pose a serious threat to human rights, and may further introduce new threats that exacerbate and amplify the current human rights problems (Kim, 2018).The rapid preferment of the facial recognition system raises serious challenges (Hodson, 2018). European Countries, the UK, France and Germany have tested technologies and have a great concern for using such over-abusive measures (Jacob, 2017). In India, digital surveillance (even though not mass surveillance), are being deployed which are real-time facial recognition programs to track its citizens, for example, *Aadhaar (*a 12-digit number, containing personal details of Indian residents stored in a database, issued for various purposes including identification of beneficiaries of government welfare schemes), *the Central Monitoring System* (for interception of communications in the interest of public safety and national security), *the National Intelligence Grid*(for the purpose of counter-terrorism and tracking terror suspects using real-time data) and so on (Murali, 2018). These systems are often devoid of transparency and accountability, and they unjustly violate citizen's right to data protection and privacy, right to equality and right against discrimination. Further, the Personal Data Protection Bill, 2019 which is still pending, does not contain provisions for data protection concerning technology-based surveillance in India.

Scholars have time and again observed that deploying AI-based surveillance tools poses threat to human rights as it can severely and systematically discriminate. Erik P.M. Vermeulen opines that the privacy concerns of AI are the most alarming and overdependence on AI will overshadow privacy (Vermeulen, 2017). Bohn et al.agree that surveillance using AI invades privacy (Bohn, Coroamă, Langheinrich, & Rohs, 2005). Jon Kofas raises concerns regarding the use of AI by government as it can cause greater threat to the very institution of democracy (Kofas, 2017).Ruggieri et al. suggest that using discriminatory framework to develop an algorithm can be the reason behind the bias (Ruggieri, Pedreschi, & Turini, 2010).Recently in 2019, the European Union Agency for Fundamental Rights has published one of the most comprehensive reports on use of facial recognition technology and its impact on human rights and enforcement of law, explaining the stand of EU on the same (EU Agency for Fundamental rights, 2019).

The paper is segmented into three parts. Part I discusses the ethics and philosophy of surveillance, and illustrates various mass surveillance practices employed by EU and India through the use of facial recognition technology (FRT). In part II, the authors analyze the implementation of existing human rights principles in the governance and regulation of AI-based surveillance and facial recognition in the EU, while focussing upon the right to data protection and privacy, right to equality and right against discrimination. In part III,drawing from the best

International Journal of Modern Agriculture, Volume 10, No.2, 2021
ISSN: 2305-7246

practices of EU, the authors suggest some considerations relevant for formulating a regulatory or policy framework for AI-based surveillance in India.

AI Powered Surveillance

Digital surveillance is a global concern. It can colossally be defined as the act of real-time and retrospective viewing, processing, storing and categorizing of online footprint against one's autonomy and/or knowledge of the individuals to whom such data belongs (Gary, 2003) The main issue surrounding surveillance is how the data is stored, processed and used.The advent of social media and a significant increase in digital interconnectedness provides a platform to individuals to share their personal information. This information can neither be reliably deleted nor does it expire; it can propagate across digital platforms at an infinite rate and high speed. The ethics and philosophy of surveillance extrapolate a lot from Jeremy Bentham's 'panopticon' (Bentham, 1971) and Michel Foucault's 'panopticism' (Foucault, 1995). The panopticon was a late 18^{th} century idealized prison model, which consisted of a central, concealed watchtower that guarded every cell, without the prisoners being able to see whether they are being watched. The system is based on a collective psychology of fear and being constantly traced or monitored. This was Jeremy's manifestation that "power should be visible and unverifiable". He believed that such constant surveillance would help in gaining control over all the groups of the society (Lyons, 1997). The theory of panopticon had a revealing influence over Michel Foucault's work on authoritarian regimes and surveillance. According to him, the ultimate goal of panopticon is to induce a sense of constant surveillance in the inmates. He used the term 'panopticism' to define the modern disciplinary societies, where the ability to intrude in anindividual's life without being monitored, creates a sense of control (Foucault, 1995). Gertrude Himmelfarb(Himmelfarb, 2005) and Jacques-Alain Miller (Miller & Miller, 1987)also critically interpreted the concept of panopticon and connected it with oppression and social control, reinforcing the uniform collective behavior. In the present times, the likelihood of identifying panopticism is higher in AI driven technologies than in prisons. It is a symbol of unrelenting surveillance and continues to reign supreme. As in modern societies, surveillance by government is an emerging technique and the governments have enacted legislationsto gather information on the internet about terror suspects and criminals. Public transit cards can also be used to track the citizen's travel history. Collection of data and monitoring of this nature is particularly similar to that of the panopticon (Lyon, 2007). Democracies all around the globe and authoritarian states engage in mass surveillance practices. Governments have valid reasons to use AI based surveillance, which are not for the purpose of imposing political control and limiting its citizens.For instance, in the year 2016, the EU adopted 'EU Passenger Name Record' (Bellanova & Fuster, 2019) which is a pan European programme. It represents a progressive shift of security practices towards data-based governance by collecting, storing and processing passenger information.

Digital surveillance is widely employed by countries across the globe. Biometrics is the most unique marker of personal information, as they are special for each and every individual. The most commonly used and the oldest type of biometric is fingerprinting. However, novel innovations in technology have enabled surveillance in new forms of biometric data such as voice recognition, facial recognition etc. The rationale behind the popularity of such novice technology is the ease with which they can be stored and their granularity.The facial recognition technology is more intrusive when compared to the standard CCTV cameras, as it can scan peculiar features of an individual and create detailed biometric maps without obtaining consent (Feldstein S. , 2019). It processes the biometric data and creates a 'biometric template' that detects and measures facial features (Rathgeb & Uhl, 2011). This technique is based on the machine learning application of AI. It uses both video and still images technology to match either live footage or stored data of individuals from a database (Introna & Nissebaum, 2010). It has begun to move to the forefront because of its conjectural advantages, and can be typically used for authentication,identification, and categorization (Phillips, et al., 2003). The authentication and identification technique compares the unique biometric templates of individuals to ascertain their identities.

International Journal of Modern Agriculture, Volume 10, No.2, 2021
ISSN: 2305-7246

In the EU, for example, in the border checks through Automated Border Control (ABC) gates, a live image or image from the passport of the person is taken and the two images are compared by the facial recognition technology to verify the person's identity. For verification or authentication, the data is attached to a database; rather it is stored in a card or an identity (EU Agency for Fundamental rights, 2019). On the other hand, in the Live Facial Recognition Technology (LFRT), the face image or video is extracted and compared to the data deposited in the database (Fussey & Murray, 2019). Categorization is used to profile individuals based on their personal characteristics to deduce the specific group to which an individual belongs such as race, sex, age etc. (European Union Agency for Fundamental Rights, 2018). FRT is also increasingly being employed by the police and other law enforcement agencies around the world for ensuring public safety and national security. European countries, such as the UK, Germany and France, are using such technologies for identification of terrorists and criminals in public places (Jacob, 2017). These applications are, however, not governed by legislations and therefore, raise concerns among civil rights activists, academicians and legal practitioners (Madianou, 2019). The UK has developed FRT to surveil people using street CCTV cameras in real-time and the UK police has been the most active in deploying such technology. Other member states of the EU have affianced with this technology. In Hungary, a venture known as "Szitakötő"have planned deployment of 35,000 facial-recognition cameras in Budapest and across the country, for the purpose of capturing facial images as well asdriver license plates for the maintenance of public order and road safety (Vass, 2018). The Czech Government has passed a measure to extend the use of facial recognition cameras at international airports (Mayhew, 2019). The Sweden's data protection authority has deployed FRT by state police to locate suspected lawbreaker, and compare facial images to a database containing more than 40,000 images (NE Online, 2019).

In India, the Punjab Police has commissioned the Punjab AI System, in association with the company Staqu technologies, which enables the police to retrieve all the background information of the suspect within minutes using facial recognition system (Bhasin, 2019). The Ministry of Home Affairs has also announced the implementation of Automated Facial Recognition System (AFRS) through National Crime RecordsBureau (NCRB), which will be used across the countries by the police for identification of criminals and authentication using CCTV cameras against the database (Parsheera, 2019). In Chennai, the police place a heavy reliance on *FaceTagr*, a facial recognition technology, to maintain law and order (Sterling, 2018). The *NeoFace* technology deployed by Surat Police is used for both facial as well as vehicle number plate recognition for tracking and monitoring purposes. Although in democratic societies the ultimate objective of surveillance is public welfare, for example, through tracking criminals, detecting frauds and identity thefts, or helping to find missing persons, such technology-based surveillance still possess great potential for harm, even if unintended, such as limited privacy, loss of accountability, highly probable built-in bias, and loss of personal data owing to misuse (Donahoe & Metzger, 2019).In today's digitally-equipped democracies, discussion surrounding the negative impact of AI ranges from privacy to data breach and problems relating to accuracy resulting in a discriminatory algorithm that makes biased hiring decisions. States have access to unprecedented volumes and unfiltered citizen information, ranging from their consumer behavior, preferences, health data, voter behavior etc. (Feldstein S. , 2019). This zeitgeist of digital fear and common resentment makes the citizens vulnerable to surveillance in different ways. The Gordian knot of digital surveillance has whooping implications in all spheres, forcing citizens to self-censor, and being subject to "arbitrary or unlawful interference with an individual's privacy, home, family or correspondence" (Report of the High Commissioner for Human Rights, 2018).

AI and Human Rights

As Artificial Intelligence system permeates unmistakably into every sphere of life, its blue devils have affected the most vulnerable and powerless (Veen, 2018). Human Rights are universal and dynamic; the concept implies that they are basic rights that belong to each and every member of the human race. There is an established network of regional, national, and international institutions that have well-developed framework for addressinghuman rights issues all around the globe. Infringement of human rights have repercussions ranging

International Journal of Modern Agriculture, Volume 10, No.2, 2021
ISSN: 2305-7246

from political costs to low global reputation.Anyrestrictions imposed upon the fundamental rights are required to meet the tests of strict proportionality and necessity(Murray & Fussey, 2019).The more the political participation rests on social media, the more they are exposed to danger. Wherever there is AI, AS (Artificial Stupidity) is also extant and it could be worse (Risse, 2019). If AI is used sans sufficing transparency and capability for human audit, legal rights can be threatened. As human rights are interrelated and interdependent, they affect almost every recognized human right. Regulating these AI-based technologies through the lens of international human rights law and national legislationsis highly pertinent in the current era of digital governance.

With regard to the application of AI systems in the EU, the same must be in conformity with the fundamental rights in the EU Charter and as per the international standards(Charter of Fundamental Rights of the European Union, 2012). The use of this technology raises serious ethical and legal concerns. Therefore, the use of FRT must comply with the existing ethical principles and laws relating to fundamental rights(Marina & Winfield, 2018). TheEU High-Level Expert Group on AI identifies four ethical principles: Prevent Harm; Respect Autonomy; Explicability; and Fairness(European Commission, 2019). Besides the ethical principles and fundamental rights, AI must also comply with the legislations laid down in EU, especially the data protection laws.

India, a member of the UN, has ratified the "International Covenant on Civil and Political Rights" (ICCPR), 1966, which provides the right to privacy, equality, and non-discrimination. India is thereby obligated to incorporate such rights in its municipal laws and regulatory policies. Thus, the regulatory framework encompassing AI based surveillance must be in conformity with the international human rights standards.

Right to Data Protection and Privacy

Privacy is essential and indispensable to human dignity; it reinforces many other rights such as freedom of choice, freedom of association, freedom of expression, etc.(Payton & Claypoole, 2014), as well as a wide array of societal norms(Solove, 2013). According to the international human rights instruments, restrictions, if any, imposed upon the right to privacy shall be in consonance with the law, and shall be necessary and proportionate(Brown, 2016).The European Court of Human Rights in the case of *López Ribalda and Others v. Spain*describes the notion of "private life" and opines that it covers physical as well as psychological integrity of an individual (López Ribalda and Others v. Spain, 2019). Although right to data protection and privacy are closely related to each other, they are still freestanding. "The right to privacy is described as a 'classic' right and, on the other hand, the right to protect personal data is classified more as a 'modern' right"(Volker und Markus Schecke and EifertGbR and HartmutEifert v. Land Heffen, 2010). Data Protection has an important role in guarding privacy. Both these rights are highly significant in protecting human dignity. AI systems often have access to large datasets for training and application purposes.This data storage and usage interferes with data protection and privacy rights. Such data is extracted from large data sets containingprivate information about individuals. Therefore, its confidentiality should be maintainedthroughout the training of the AI system based on such data and its subsequent storage and application(Bellovin, Hutchins, Jebara, & Zimmeck, 2014).

It has been confirmed in the case of *M. Schwarz v. Stadt Bochum*by the Court of Justice of the European Union, and in *Szabó & Vissy v. Hungary*by the European Court of Human Rights that facial images constitute personal data, and the courts further observed that protection of facial image is an important part of personal development(Council of Europe/European Court of Human Rights, 2020).Nowadays, the use of social media monitoring programs and AI based surveillance tools have expanded. The Facial Recognition System connects the image with the identity of the person and also connects this with any other information held in the database(Nissenbaum, 2004). Therefore, unchecked used of this technology poses threat. Facial recognition tools have correctly identified around 69% of people wearing scarves and caps to hide their faces during protest(Walker, 2016). With regard to law enforcement, FRT may enable police officials to identify people without reasonable suspicion, probable cause or any other legal principle that might have been otherwise

International Journal of Modern Agriculture, Volume 10, No.2, 2021
ISSN: 2305-7246

required for identification by conventional means (Electronic Privacy Information Center, 2016). The Metropolitan Police of London, in the past years, has carried several tests in order to examine the FRT which identifiesindividuals on watch list(Fussey & Murray, 2019). These testsare carried out by various members of the EU by CCTV or any other means. Apart from this, EU has introduced the Entry/Exit System Regulation for security checks of nationals crossing the external borders of EU Member states. This regulation allows theuse of facial images for the purpose of verification in (European Parliament, Council of the European Union, 2017).Article 5 of the EU General Data Protection Regulation (GDPR) necessitates a legal ground for processing of data. Apart from the principles of "fairness, accountability and transparency" (FAT), it lays down the principle of "data minimization"(European Parliament and Council of European Union, 2016). Article 22 of the GDPR prohibits (with narrow exceptions) automated decisions, which bear legal or other significant effects(European Parliament and Council of European Union, 2016). The GDPR contains provisions encouraging the designing of systems which pose lesser threats to privacy. These provisions have significant bearing upon designing of AI. The Data Protection Impact Assessment is mandatory as per the GDPR guidelines. The European Commission published a"White Paper on Artificial Intelligence: An European Approach to Excellence and Trust" in February, 2020 which included biometrics and facial recognition within "high risk" framework of regulation (European Commission, 2020). The European Digital Rights (EDRi), an international non-profit association, analyzed the White Paperand stated in its report that the Commission should "risk-assess" the fundamental issues surrounding mass surveillancewhich violate the human rights, and EDRi strongly encourages EU to ban such surveillance(Jaubowska & Naranjo, 2020). The Data Protection Impact Assessmentrequires "assessment of risks" related to data(Nemtiz, 2018). Further the legislation in the EU does not include a mandate for testing unfair bias and regulating scope and limit of surveillance by the state. Therefore, there is a dire need for guidelines regulating these aspects with regard to FRT in the EU. In 2020, the EU is considering the introduction of a five-year moratorium on FRT in public spaces so that it can work on the risk management and simultaneously devise a way to regulate this technology(Chen, 2020).

Currently, India does not have aspecific legislationfor regulation of use and storage of personal data, which includes biometrics and FRT. The data protection regime in India is alarmingly weak considering the current growth of AI and increasing AI applications across various sectors. The Information Technology Act, 2000 is silent with regard to biometrics and facial recognition. The EU GDPR influenced a debate in India(Goswami & Haran, 2017). The Personal Data Protection Bill, 2019 drafted by the B.N. Srikrishna Committee is also silent with regard to regulation of FRT and storage of data gathered using it. In the meanwhile, constitutional provisions may be used to assess AI applications(Basu & Hickok).India also plans to introduce anAutomated Facial Recognition System to facilitate as a searchable platform for identification and verification of criminal suspects, and sharing of such information across different government organisations. However, such an application is susceptible to risks of misuse and poses severe threats to rights and dignity of the citizens (Saini & Sylvester, 2019). It ostensibly sidesteps the fundamental right to privacy validated by the Supreme Courtin 2017 in the case of *"Justice K.S. Puttuswamy (Retd.) & Anr. V. Union of India & Ors."*

Right to Equality and Non-Discrimination

Discrimination can be explained as "where one individual is treated inferior than another in a comparable situation, on the basis of real or perceived characteristics"(Council of the European Union, 2000).Discrimination interferes with human rights of the people. Discrimination and bias are immanent perils of any society. Human decision itself is not exempt from such biases.In this context, AI technology can prove to be useful to the society as it may promote diversityowing to its objective nature as compared to humans(Andersen, 2018).However, AI is designed by humans and the objectivity in its outputs is heavily dependent on the quality and nature of training data fed into the system, leaving ample scope for perpetuating bias from humans into the AI system(European Union Agency for Fundamental Rights, 2019). The objectivity of AI based decision making will also be dependent on the human rights standards and parameters observed while designing and implementing AI. For accuracy, the facial recognition system requires large sets of data which

International Journal of Modern Agriculture, Volume 10, No.2, 2021
ISSN: 2305-7246

includerepresentative set of faces reflecting different groups in the society. However, the facial images used in technology over-represent white males, with lesser number of females and people from ethnic backgrounds. Therefore, there are a lot of cases where the FRT has worked accurately for white males, but not for black females(West, Whittaker, & Crawford, 2019). As error rates are higher for dark skinned faces, misidentification is a challenge. "The ACLU's test of Amazon Rekognition facial recognition software, it scanned the faces of all 535 Congress members of the U.S. against 25,000 public criminal mug shots using Rekognition's API with the default 80% confidence level. Although no one in the U.S. Congress was actually in the mug shot database, yet there were 28 false matches. Of these matches, 38% were people of color, even though only 20% of members of Congress are people of color.(Brandom, 2018)" Owing to such technical irregularities, where even the phenotypical characteristics can influence the outcome, people are therefore, vulnerable to be wrongly matched as false positiveswhen such images are compared in the database(European union Agency for Fundamental Rights, 2018). This leads to discrimination, based on the skin colour. There are instances where people with disabilities such as face alteration due to paralysis or an accident, or people with facial surgeries etc., have faced such bias. This technology may also be used by government in countries where homosexuality is socially unacceptable or illegal, to surveil areas frequented by the LGBTQ people or to track any 'illegal' homosexual activity, thereby violating the privacy and dignity of such individuals(Levin, 2017). The presence of bias in Artificial Intelligence could be highly risky and discriminatory againstpersons without it being consciously programmed to do so by its programmers and operators(Advisory Committee on Equal Opportunities for Women and Men, 2020).

Conclusion

The growth of AI based surveillance through facial recognition technology (FRT)and biometrics has evolved rapidly over the last decade and its spread is unabated. Its use by the authoritarian regimes against a certain group of populations has already rung alarm bells.Despite an existing regulatory framework governing AI applications in the EU and observance of rule of law, the use of AI-based technology continues to give rise to ethical and legal concerns undermining human rights of individuals.Even if its accuracy is improved to address the negative impacts of such technology, it will always come with error rates. Therefore, FRT must conformto human rights as well as the established ethical principles in accordance with the international standards. Owing to various negative implications posed by AI, there is a need for a regulatory framework addressing the surveillance concerns in this regard in order to have a fair, unbiased and trustworthy AI. An international uniform regulation governing AI technology is not currently desirable as it will present the countries across the globe with a myriad of problems concerning its practical applicability and jurisdictional issues. Therefore, it is suggested that India should devise a national regulatory or policy framework governing AI based surveillance and facial recognition technology. Such a framework shall, in accordance with the rule of law, address theconcerns surrounding privacy, bias and non-discrimination, and be aligned towards the attainment of UN SDGs. In the meanwhile, application of constitutional provisions (right to equality under Article 14, right against discrimination under Article 15, and right to privacy as implied under Article 21) to assess AI applications is the only probable solution,in the absence of comprehensive legal provisions that protect against human rights infringement resulting from technology-based surveillance. It is further suggested that, like the EU,India mayintroduce a five-year moratorium to facilitate operation of technology-based governance while ensuring protection against risks arising therefrom.The human rights implications of facial recognition technologyare both positive and negative in nature. It is imperative to maintain a balance between the positive and negative impacts through a regulatory framework which shall effectively address the negative impacts and ensure that they do not overpower the positive impacts of AI technology.

References

1. Abbany, Z. (2018, May 5). What good is AI for UN Development Goals? Retrieved from Dw: https://www.dw.com/en/what-good-is-ai-for-un-development-goals/a-43797637

International Journal of Modern Agriculture, Volume 10, No.2, 2021
ISSN: 2305-7246

2. Advisory committee on equal opportunities for women and men. (2020). Opinion on Artificial Intelligence- opportunities and challenges for gender equality.

3. Andersen, L. (2018). Human rigts in the age of artificial inteliigence. Acess now.

4. Basu, A., & Hickok, E. (n.d.). Artificial Intelligence in the governance sector in India. The centre for Internet and Society.

5. Bellanova, R., & Fuster, G. G. (2019, October). Composting and computing: On digital security compositions. European Journal of International Security, 4(3), 345-365.

6. Bellovin, S. M., Hutchins, R. M., Jebara, T., & Zimmeck, S. (2014). When Enough is Enough: Location Tracking, Mosaic Theory, and Machine Learning. NYU Journal of Law & Liberty, 8(2), 555--628.

7. Bentham, J. (1971). Panopticon: The Inspection House. T. Payne.

8. Bhasin, S. (2019, August 24). Tribune News Service. Retrieved from Tribune India: https://www.tribuneindia.com/news/archive/bathinda/punjab-police-win-ficci-smart-award-821839

9. Binns, R. (2017, April 28). Data protection impact assessments: a meta-regulatory approach. International Data Privacy Law, 7(1), 22-35.

10. Bohn, J., Coroamă, V., Langheinrich, M., & Rohs, F. (2005). Social, economic, and ethical implications of ambient intelligence and ubiquitous computing in Ambient intelligence. Springer Berlin Heidelberg .

11. Brandom, R. (2018, July 26). Amazon's facial recognition matched 28 members of Congress to criminal mugshots. Retrieved from The Verge: https://www.theverge.com/2018/7/26/17615634/amazon-rekognition-aclu-mug-shot-congress-facial-recognition

12. Brown, D. (2016). New UN resolution on the right to privacy in the digital age: crucial and timely. Internet Policy Review.

13. Cardon, D., Cointet, J. P., & Mazieres, A. (2018). Neurons Spike Back: The invention of inductive machines and the artificial intelligence controversy. Reseaux, 5(211), 173-220.

14. Chadwick, A., & Howards, P. N. (2010). Routledge Handbook of Internet Politics .

15. Charter of Fundamental Rights. (2012, October 26). Official Journal of te European Union, 364.

16. Charter of Fundamental Rights of the European Union. (2012, October 26). Retrieved from https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights_en

17. Chen, A. (2020, January 17). EU might ban facial recognition in public for 5 years. Retrieved from MIT Technology Review: https://www.technologyreview.com/2020/01/17/238092/facial-recognition-european-union-temporary-ban-privacy-ethics-regulation/

18. Chollet, F. (2017). Deep Learning with Python Shelter Island. Manning Publications.

19. Choudhary, M., & Moglen, E. (2020, February 2020). Why India must resist facial recognition tech | Opinion. Retrieved from Hindustan times: https://www.hindustantimes.com/analysis/why-india-must-resist-facial-recognition-tech-opinion/story-18O8lvhiXj5L2D7cW3gCqJ.html

International Journal of Modern Agriculture, Volume 10, No.2, 2021
ISSN: 2305-7246

20. Council of Europe/European Court of Human Rights. (2020, April 30). Guide on Article 8 of European Convention of Human Rights.

21. Council of the European Union. (2000, June 29). implementing the principle of equal treatment between persons irrespective of racial or ethnic origin. Retrieved from Eur-Lex: https://eur-lex.europa.eu/eli/dir/2000/43/oj

22. Donahoe, E., & Metzger, M. M. (2019, April). Artificial Intelligence and Human Rights. Journal of Democracy, 30(2), 115-126.

23. Electronic Privacy Information Center. (2016, June 23). The FBI's Use of Facial Recognition and Proposal to Exempt the Bureau's Next. Retrieved from Epic.org: https://epic. org/privacy/fbi/NGI-Congressional-Oversight-Letter.pdf

24. EU Agency for Fundamental rights. (2019). Facial recognition technology: fundamental rights considerations in the context of law enforcement. Retrieved from https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper.pdf

25. European Commission. (2019). Ethics guidelines for trustworthy AI.

26. European Commission. (2020, February 19). White Paper on Artificial Intelligence-A European approach to excellence and trust. Retrieved from Europa: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

27. European Parliament. (2019). A comprehensive European industrial policy on artificial intelligence and robotics. Strasbourg.

28. European Parliament and Council of European Union. (2016). Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (Data Protection Directive). Retrieved from Eur-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

29. European Parliament, Council of the European Union. (2017, November 30). Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 767/2008, Regulation (EC) No 810/2009, Regulation (EU) 2017/2226, Regulation (EU) 2016/399, Regulation XX/2018 [Interoperability Regulation], and Decision . Official Journal of the European Union.

30. European Union Agency for Fundamental Rights. (2018, December 5). Preventing unlawful profiling today and in the future: a guide. Luxemborg: Publications Office of the European Union.

31. European union Agency for Fundamental Rights. (2018). Under watchful eyes – biometrics, EU IT-systems and fundamental rights. Luxemborg: Publications Office of the European Union.

32. European Union Agency for Fundamental Rights. (2019). Data quality and artificial intelligence – mitigating bias and error to protect fundamental rights.

33. Feldstein, S. (2019). The Global Expansion of AI Surveillance. Carnegie, 5.

34. Feldstein, S. (2019, January). The Road to Digital Unfreedom: How Artificial Intelligence Is Reshaping Repression. Journal of Democracy, 30(1), 40-52.

35. Floridi, L., & Cowls, J. (2019, July 18). A united framework of five principles for AI in society. Harvard Data Science Review.

International Journal of Modern Agriculture, Volume 10, No.2, 2021
ISSN: 2305-7246

36. Foucault, M. (1995). Discipline & Punish: The Birth of the Prison. (A. Sheridan, Trans.) Vintage Books.

37. Fussey, P. P., & Murray, D. D. (2019). London Metropolitan Police's Trial of Live Facial Recognition Technology. University of Essex, Ecdonomic and Social Research Council (E.S.R.C). The Human Rights, Big Data and Technology Project.

38. Gary, T. M. (2003). A Tack in the Shoe: Neutralizing and Resisting the New Surveillance. Journal of Social Issues, 2(59), 369-90.

39. Goswami, S., & Haran, V. (2017, April 26). Analysis: Data Protection in India - Getting It Right. Retrieved from BankInfo Security: https://www.bankinfosecurity.asia/analysis-data-protection-in-india-getting-right-a-9866

40. Himmelfarb, G. (2005). The Roads to Modernity: The British, French, and American Enlightenments. Random House.

41. Hodson, H. (2018). Walking barcodes. (123). The Economist.

42. International Covenant on Civil and Political Rights. (1996, December 16). Retrieved from https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

43. Introna, L. D., & Nissebaum, H. (2010). Facial Recognition Technology A Survey of Policy and Implementation Issues.

44. Jacob, M. (2017, October 20). Facial Recognition gains ground in Europe, among big brother fears. (P. Tamma, Trans.) EurActive.

45. Jaubowska, E., & Naranjo, D. (2020). Ban Biometric Mass Surveillance. Brussels: European Digital Rights.

46. Justice K.S. Puttuswamy (Retd.) and Anr. v. Union of India and Ors., 10 SCC 1 (August 24, 2017).

47. Kim, L. (2018, September 25). Artificial Intelligence and human rights: opportunities and threats. Berkman Klien Center for Internet and Society.

48. Koettl, C. (2018, September 4). Retrieved from The New York Times: https://www.nytimes.com/2018/09/04/reader-center/social-media-video-how-to-verify.html

49. Kofas, J. (2017, April 22). Artificial Intelligence: Socioeconomic, Political and Ethical Dimensions. Retrieved from https://countercurrents.org/2017/04/artificial-intelligence-socioeconomic-political-and-ethical-dimensions/

50. Levin, S. (2017, September 8). New AI can guess whether you're gay or straight from a photograph. Retrieved from The Guardian: https://www.theguardian.com/technology/2017/sep/07/new-artificial-intelligence-can-tell-whether-youre-gay-or-straight-from-a-photograph

51. López Ribalda and Others v. Spain, 1874/13 and 8567/13 (European Court of Human Rights October 17, 2019).

52. Lorenz, P., & Saslow, K. (2019). Demystifying AI & AI Companies. Stiftung Neue Verantwortung.

53. Lyon, D. (2007). Surveillance studies: an overview. Wiley.

International Journal of Modern Agriculture, Volume 10, No.2, 2021
ISSN: 2305-7246

54. Lyons, R. G. (1997). Jeremy Bentham's Ethics of Surveillance: A Critical Analysis. 4(32). Journal of Thought. Retrieved from https://www.jstor.org/stable42589514

55. Madianou, M. (2019, July 2). The Biometric Assemblage: Surveillance, Experimentation, Profit, and the Measuring of Refugee Bodies. Sage Journals, 20(6), 581–599.

56. Marina, J., & Winfield, A. F. (2018, October 15). Ethical governance is essential to building trust in robotics and artificial intelligence systems. Philosophical Transactions of the Royal Society.

57. Máté Szbo and Beatrix Vissy, 37138/14 (European Court of Human Rights May 13, 2014).

58. Mayhew, S. (2019, March 10). Retrieved from BiometricUpdate: https://www.biometricupdate.com/201903/expanded-use-of-facial-recognition-at-prague-international-airport-approved

59. Michael Schwarz v Stadt Bochum., C 291/12 (Judgment of the Court (Fourth Chamber) October 17, 2013).

60. Miller, J. A., & Miller, R. (1987). Jeremy Bentham's Panoptic Device. October, 41, 3-29. Retrieved from https://www.jstor.org/stable/778327?seq=1

61. Murali, A. (2018, August 13). Retrieved from Factor Daily: https://factordaily.com/face-recognition-mass-surveillance-in-india/

62. Murray, D., & Fussey, P. (2019, March). Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data. Irsael Law Review, 52(1), 31-60.

63. NE Online. (2019, October 28). Sweden authorises the use of facial recognition technology by the police. Retrieved from New Europe: https://www.neweurope.eu/article/sweden-authorises-the-use-of-facial-recognition-technology-by-the-police/#:~:text=Sweden's%20data%20protection%20authority%20has,to%20help%20identify%20criminal%20suspects.&text=According%20to%20the%20Swedish%20authority,L

64. Nemtiz, P. (2018). Constitutional democracy and technology in the age of artificial intelligence. Philosophical Transactions of the Royal Society .

65. Nissenbaum, H. (2004, February). Privacy as contextual integrity. Washington Law Review Association, 79(1), 119-157.

66. Parsheera, S. (2019). Adoption and regulation of facial recognition technologies in India: Why and why not? Data Governance Working Paper, 5(6).

67. Payton, T. M., & Claypoole, T. (2014). Privacy in the Age of Big Data: Recognizing Threats, Defending Your Rights, and Protecting Your Family. Rowman & Littlefield Publishers.

68. Phillips, P. J., Grother, P., Michaels, R. J., Blackburn, D. M., Tabassi, E., & Bone, M. (2003). Facial recognition vender test 2002. National Institute of Standards and Technology, Defense Advanced Research Projects Agency (DARPA). DoD Counterdrug Technology Development Program Office.

69. Rathgeb, C., & Uhl, A. (2011). A survey on biometric cryptosystems and cancelable biometrics. EURASIP Journal on Information Security volume(3).

International Journal of Modern Agriculture, Volume 10, No.2, 2021
ISSN: 2305-7246

70. Report of the High Commissioner for Human Rights. (2018). The Right to Privacy in the Digital Age. the UN.

71. Risse, M. (2019, February). Human Rights and Artificial Intelligence: An Urgently Needed. Human Rights Quaterly, 41(1), 1-16.

72. Ruggieri, S., Pedreschi, D., & Turini, F. (2010, May). Data mining for discrimination discovery. ACM transactions from knowledge discovery from data, 4(2). ACM Journals.

73. Saini, K., & Sylvester, P. (2019, July 23). India Is Falling Down the Facial Recognition Rabbit Hole. Retrieved from The Wire: https://thewire.in/tech/india-is-falling-down-the-facial-recognition-rabbit-hole

74. Schutter, P. O., Ramasastry, P. A., Taylor, M. B., & Thompson, R. C. (2012). Human Rights due diligence: The role of states.

75. Smith, C. (2006, December). The History of Artificial Intelligence. University of Washington.

76. Solove, D. J. (2013). Nothing to Hide: The False tradeoff between Privacy and Security. Yale Universty Press.

77. Sterling, B. (2018, August 15). Indian face Recognition. Retrieved from The Wired: https://www.wired.com/beyond-the-beyond/2018/08/indian-face-recognition/

78. The Indormation and Technology Act. (2000, October 17).

79. The Personal Data Protection Bill. (2019). Retrieved from meity.gov.in: https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf

80. (2019). UN Global Pulse. Retrieved from The Sustainable Development Goals (SDGs) Projects: https://www.un.org/en/sections/issues-depth/big-data-sustainable-development/index.html

81. Universal Declaration of Human Rights. (1948, December 10). Retrieved from https://www.un.org/en/universal-declaration-human-rights/

82. Vass, A. (2018, January 1). Hungary Today. Retrieved from CCTV: Is It Big Brother or the Eye of Providence?: https://hungarytoday.hu/cctv-is-it-big-brother-or-the-eye-of-providence/

83. Veen, C. V. (2018, May 14). Artificial Intelligence: What's Human Rights Got To Do With It? Retrieved from Points Data & Society: https://points.datasociety.net/artificial-intelligence-whats-human-rights-got-to-do-with-it-4622ec1566d5

84. Vermeulen, E. P. (2017, April 27). Retrieved from Medium: https://medium.com/startup-grind/artificial-intelligence-is-taking-over-privacy-is-gone-d9eb131d6eca

85. Volker und Markus Schecke and EifertGbR and HartmutEifert v. Land Heffen, C-92/09 and C-93/09 (European Court of Justice June 17, 2010).

86. Walker, S. (2016, May 17). Face recognition app taking Russia by storm may bring end to public anonymity. Retrieved from The Guardian: https://www.theguardian.com/technology/2016/may/17/findface-face-recognition-app-end-public-anonymity-vkontakte

87. West, S. M., Whittaker, M., & Crawford, K. (2019, April). Discriminating Systems: Gender, Race, and Power in AI. Retrieved from AI Now Institute: https://ainowinstitute.org/discriminatingsystems.pdf