Journal of Posthumanism

2025
Volume: 5, No: 2, pp. 1114–1153
ISSN: 2634-3576 (Print) | ISSN 2634-3584 (Online)
posthumanism.co.uk

DOI: https://doi.org/10.63332/joph.v5i2.490

A Study on Human Rights Impact with the Advancement of Artificial Intelligence

Hugo Wai Hoo Chan[1], Noble Po Kan Lo[2]

Abstract

The widespread use of AI-powered surveillance technologies by government agencies and commercial enterprises poses a significant and unprecedented threat to the fundamental human right to privacy. This article examines the use of advanced AI systems, such as facial recognition, predictive policing algorithms, AI-powered drones, and smart sensors, to facilitate pervasive surveillance. These technologies enable the covert collection, integration, and analysis of revealing personal information, rendering traditional notions of privacy obsolete. This study reviews technical documentation, legislative frameworks, business practices, and social implications across various countries, illustrating the widespread implementation of AI surveillance akin to a digital Panopticon. The findings highlight critical deficiencies in current legal protections and ethical principles, particularly concerning consent, human rights, and democratic values. The lack of transparency, fairness, and accountability in AI systems often marginalises vulnerable populations and establishes privatised systems of social control. Furthermore, the paper demonstrates how the normalisation of continuous monitoring has begun to erode societal norms, cultural perspectives, and fundamental human behaviours regarding privacy. Without intervention, such technologies risk creating a dystopian future where individuality, freedom of choice, and opposition are illusions under oppressive AI surveillance. In response, this research advocates for corrective frameworks that prioritise human rights, including privacy-by-design, algorithmic transparency, and human oversight. By fostering collaboration among policymakers, technology developers, and civil society, the article provides practical recommendations to ensure AI developments align with the protection of human dignity, democratic liberties, and ethical principles foundational to civilised societies.

Keywords: *AI Surveillance; Privacy Rights; Ethical AI; Dataveillance; Human Rights and Technology*

Introduction

This research is highly relevant due to the growing worldwide use of AI-driven surveillance technology by both governmental entities and commercial companies. Governments frequently defend the utilisation of such technology for the purpose of ensuring security and maintaining public order, while commercial organisations exploit them to improve consumer data analytics. The extensive acceptance of this technology creates substantial issues over the infringement upon privacy, which is commonly acknowledged as an essential human entitlement. This deterioration necessitates immediate and strong regulatory measures. The risk of AI technology being misused and causing harm to privacy and wider human rights is increasing as these technologies become more deeply embedded in everyday life. This circumstance requires a thorough evaluation of their influence. Moreover, the research goes beyond examining the impact on privacy and delves

[1] Lofter Group, 18/F Pioneer Centre, 750 Nathan Road, Mong Kok, Kowloon, Hong Kong, China. The Inns of Court College of Advocacy, 33 Chancery Lane, London, United Kingdom. E-mail: waihoo.hugochan295@icca.ac.uk.

[2] Division of Languages and Communication, College of Professional and Continuing Education, The Hong Kong Polytechnic University. PolyU West Kowloon Campus, 9 Hoi Ting Road, Yau Ma Tei, Kowloon, Hong Kong, China. Department of Educational Research, Lancaster University, Educational Research, County South, Lancaster University, Lancaster, United Kingdom. https://orcid.org/0000-0001-7636-6146. E-mail: noble.lo@cpce-polyu.edu.hk. (Corresponding Author)

into the broader consequences of AI on other aspects of human rights. It advocates for the creation of AI systems that are not just transparent but also capable of providing explanations for their actions.

This article provides an in-depth examination of international legislative efforts that focus on the relationship between AI, privacy, and human rights. This comprehensive investigation provides strategic analysis and strong suggestions for a collaborative strategy combining politicians, technological developers, and civil society. These ideas seek to promote a future where AI technologies not only progress but also prioritise the improvement and safeguarding of human rights. The suggested approach emphasises the significance of ethically directed research and responsible deployment of AI technologies, guaranteeing their role as instruments for beneficial society transformation rather than means of control or oppression. This paper contributes to the current discussion on how to effectively address the issues posed by AI while respecting and protecting the well-being, privacy, dignity, and rights of persons worldwide. It advocates for policies that prioritise these aspects alongside innovation.

Background

AI surveillance technology is being utilised worldwide, as nations globally implement these systems to augment their surveillance capabilities. AI surveillance technology is being used by at least 75 out of 176 nations worldwide, indicating its extensive global presence and influence.[3] China has been a significant catalyst for global AI surveillance, providing technology to 63 nations. Huawei, a Chinese corporation, exclusively supplies AI surveillance technologies to a minimum of 50 nations.[4] The proliferation of AI surveillance technologies extends beyond the borders of China. Furthermore, American corporations are actively involved in the field of AI surveillance, providing their technology to a total of 32 nations.[5] The implementation of AI surveillance systems differs among several categories of nations. Advanced democracies, which place a high value on individual rights and liberties, extensively utilise AI surveillance systems, with 51% of these countries implementing such technology.[6] These nations utilise AI technologies to bolster their surveillance capabilities, boost public safety, and combat criminal activities. Nevertheless, the implementation of AI surveillance systems in liberal democracies is frequently governed by legislation and monitoring to safeguard individual privacy rights and deter misuse. Conversely, governments in autocratic and semi-autocratic nations are more inclined to misuse AI surveillance technologies.[7] These regimes might potentially utilise AI technology to repress dissent, surveil political adversaries, and uphold societal control. The absence of strong democratic institutions and mechanisms for oversight might possibly result in the misuse of AI surveillance systems, so violating the rights and liberties of individuals. A noteworthy observation is that there exists a robust association between a nation's military spending and its use of AI surveillance systems.[8] Nations that allocate greater financial resources to their military tend to prioritise the development and deployment of AI surveillance technologies. These expenditures are frequently motivated by national security considerations and the imperative to safeguard borders, key infrastructure, and individuals. Utilising AI

[3] Feldstein S, *The Global Expansion of AI Surveillance* (Carnegie Endowment for International Peace 2019)

[4] Papageorgiou M, Can M and Vieira A, “China as a Threat and Balancing Behavior in the Realm of Emerging Technologies” (2024) Chinese Political Science Review

[5] Ibid[1]

[6] Ibid[1]

[7] Read A, ‘Increased Uptake of Surveillance Technologies during COVID-19’ (2020) 22 European Journal of Law Reform 448

[8] Ibid

surveillance technologies in military contexts may bolster situational awareness, detect threats, and improve reaction capabilities. American intelligence services employ AI systems to analyse extensive quantities of data gathered from diverse sources, such as security cameras and satellite photography, to detect possible threats to national security and noteworthy trends.[9] China, however, is not an exception. It has deployed an advanced monitoring technology to monitor and regulate human conduct. Cameras installed at crosswalks frequently capture images of individuals who illegally cross the street, regardless of their age. These images are considered with similar importance by the local traffic police, regardless of whether the jaywalker is a youngster or an adult. In addition, a park in China uses Facial recognition technology (FRT) to control the distribution of toilet paper by scanning individuals' faces.[10] Security measures utilise facial recognition cameras, smart city platforms, and social credit score to surveil its residents and uphold social order. Ultimately, AI surveillance technology is extensively employed in several countries due to a range of variables including apprehensions about security, safeguarding the public, and deterring criminal activities. The implementation of AI surveillance systems varies among nations depending on their political systems, with liberal democracies and autocratic/semi-autocratic regimes demonstrating different methods. Ensuring the appropriate and ethical use of AI in surveillance requires finding a harmonious equilibrium between security requirements and the rights to individual privacy. Comprehensive rules and safeguards are necessary to handle the issues related with the deployment of AI surveillance technology, which is expanding globally.

All throughout the globe, governments are bolstering their capacity for monitoring by utilising AI technologies. Using AI techniques, intelligence services are able to sift through mountains of data gathered from a variety of sources, such as internet platforms, security cameras, and satellite photography. The way governments carry out surveillance activities has been completely transformed by this capacity to process and understand massive amounts of data swiftly and accurately. Intelligence agencies utilise AI techniques for domestic and foreign monitoring, and the usage of AI in government surveillance has grown more common. In order to aid human analysts in their decision-making, these technologies help discover possible targets, analyse patterns of interest, and provide insights. AI technologies may assist law enforcement by scanning licence plates, faces, and other details in real-time, allowing them to follow and identify anyone of interest. Concerns and controversies have also surfaced over the government's use of AI for surveillance purposes. Concerns about possible invasions of privacy are high. A growing number of sophisticated and ubiquitous AI monitoring systems raise concerns about potential privacy invasions and the unauthorised acquisition of personal information. Furthermore, others worry that AI will be weaponized and used to silence political opposition or discriminate against certain groups. Use of AI in government surveillance must be done responsibly and ethically if these issues are to be addressed. Transparency, accountability, and the preservation of individual rights necessitate the establishment of regulations and protections. Data collection, storage, and sharing practices using AI surveillance systems should be regulated by governments. One way to make sure these rules are being followed is to implement regular audits and other forms of control. The Fourth Amendment is one of several American laws that protect citizens' right to privacy by prohibiting the government from conducting warrantless searches and seizures.

[9] Blanchard A and Taddeo M, "The Ethics of Artificial Intelligence for Intelligence Analysis: A Review of the Key Challenges with Recommendations" (2023) 2 Digital Society 1

[10] Ong R, "Privacy and Personal Information Protection in China's All-Seeing State" (2023) 31 International Journal of Law and Information Technology 349

Oversight and accountability are ensured by the legislative frameworks that regulate the surveillance operations of intelligence services working within the country. Nevertheless, there are still obstacles to overcome in order to update these frameworks to match the lightning-fast progress in AI. Finally, government surveillance using AI has revolutionised intelligence agency operations by facilitating the efficient processing and analysis of massive volumes of data. However, it is crucial to utilise AI surveillance technology responsibly and ethically due to worries about privacy invasions and possible abuses. In order to maintain public trust and safeguard civil liberties, it is crucial to find a middle ground between the necessity for security measures and the right to personal privacy.

AI technology extends beyond government monitoring and is extensively embraced in the corporate sector. Companies in several sectors are employing AI to augment their monitoring capabilities and increase security measures. The utilisation of AI in private sector monitoring has a multitude of advantages, but it also gives rise to apprehensions surrounding privacy and ethical considerations. AI surveillance technology is utilised in the private sector to oversee sites, identify irregularities, and strengthen security processes.[11] Smart policing tactics utilise AI algorithms to analyse trends and forecast criminal activity, allowing law enforcement organisations to spend resources efficiently. These systems have the capability to analyse substantial amounts of data from many sources, including CCTV cameras, social media platforms, and sensor networks, to detect possible dangers and risks. The advantages of AI in private sector monitoring are substantial. AI technology facilitates the rapid and effective processing of vast quantities of visual data, resulting in expedited response times and the implementation of proactive security measures. This is especially beneficial in high-risk areas or key infrastructure where the immediate identification of potential dangers is essential. Surveillance systems driven by AI may promptly detect suspicious behaviour, unauthorised access attempts, or prospective security breaches, therefore reducing risks and pre-empting any incidents.

On the other hand, there are moral questions about using AI for corporate spying. The collection and processing of personal data by AI surveillance systems has put privacy issues front and centre. Strong data security measures and compliance with privacy legislation are crucial in view of the seriousness of the problem of possible misuse and unauthorised access to sensitive information. One sector that has seen success in using AI-powered surveillance systems is retail, namely in the detection of stealing and other suspicious activities. These systems use object recognition algorithms to sift through security camera footage in search of possible theft occurrences. This gives business owners the ability to respond quickly and stop losses in their tracks. Some worry that this technology might lead to false positives or misidentification, which would result in innocent people being falsely implicated, even while it can improve security. Companies in the private sector that use AI for surveillance purposes should make accountability and openness their top priorities if they want to solve these issues. To ensure that data is handled properly and that privacy rights are respected, clear rules and standards should be put in place to control the use of AI surveillance systems. To ensure these standards are being met, it is helpful to conduct audits and independent evaluations on a regular basis. To sum up, the commercial sector is rapidly embracing AI technology to strengthen security measures and monitoring capacities. AI has many advantages for private sector surveillance, including the ability to

[11] Almeida D, Shmarko K and Lomas E, "The Ethics of Facial Recognition Technologies, Surveillance, and Accountability in an Age of Artificial Intelligence: A Comparative Analysis of US, EU, and UK Regulatory Frameworks" (2021) 2 AI and Ethics 377

identify threats in real-time and implement proactive security measures. To make sure AI surveillance technology is used responsibly and ethically, however, privacy issues and other ethical considerations need to be addressed. Building public confidence and maintaining a balance between security demands and individual privacy rights requires organisations to prioritise openness, accountability, and data protection.

Research Question

What is the impact of AI-powered surveillance technology on the right to privacy? Primary investigation the primary research question that drives this article is: What is the impact of AI-powered surveillance technologies on the right to privacy?

Sub-Questions To thoroughly explore this overarching question, the study delineates several sub-questions to investigate the various dimensions of the impact of AI surveillance on privacy:

Scope and Mechanisms: What specific AI-driven surveillance technologies are currently prevalent, and what mechanisms do they employ to collect, analyse, and utilize personal data?

Privacy Intrusions: In what ways do these technologies intrude upon personal privacy? This includes examining both the overt and covert methods through which AI systems can invade personal spaces and data sanctuaries without the explicit consent or awareness of the individuals involved.

Legal and Ethical Considerations: Are the existing legal frameworks adequate in addressing privacy breaches facilitated by AI surveillance? Additionally, this question explores whether these legal frameworks are in alignment with ethical considerations surrounding autonomy, consent, and respect for personhood.

Comparative Analysis: How do the impacts of AI surveillance on privacy vary across different contexts and jurisdictions? For instance, the approach to privacy and surveillance differs significantly between regions like the European Union, which enforces the General Data Protection Regulation (GDPR), and other regions with less stringent privacy protections.

Future Implications: What are the potential long-term effects of AI-driven surveillance on societal norms and individual behaviours regarding privacy? This question aims to understand if and how the normalization of surveillance might alter fundamental human interactions and expectations concerning privacy.

Objectives

The primary objective of this article is to thoroughly investigate the effects of AI-powered surveillance technologies on the basic human right to privacy. The research focuses on identifying and analysing different AI-powered surveillance technologies that are currently being used, including facial recognition systems, predictive policing algorithms, and smart city platforms. The goal is to comprehend how these technologies gather, process, and utilise personal data. The aim is to examine how new technologies invade human privacy, both openly and secretly, by facilitating mass identification, tracking of location, monitoring of behaviour, and the creation of detailed personal profiles without express permission or individual knowledge. The research aims to assess the effectiveness of current legal frameworks, such as data protection legislation and privacy laws, in dealing with the specific issues and privacy violations enabled by AI surveillance technology. In addition, it will evaluate whether these legal frameworks are in line with ethical issues about individual autonomy, consent, and respect for persons.

The objective of the research is to do a comparison analysis in order to comprehend the variations in the effects of AI surveillance on privacy rights across various situations and jurisdictions. Specifically, the study will focus on comparing areas that have strong data protection policies with those that have less strict privacy safeguards. This study will analyse whether the widespread acceptance of constant monitoring could fundamentally change human interactions, expectations, and the general understanding of privacy in contemporary societies. The article seeks to attain these goals in order to provide a thorough comprehension of the intricate interaction of AI surveillance technology, privacy rights, and ethical issues. The study results will be used to provide policy recommendations, develop technology, and create governance frameworks that enable the responsible and ethical use of AI systems, while also protecting individual privacy and maintaining democratic principles. Moreover, this research aims to add to the continuing discussion about the connection between technological progress and human rights. It highlights the significance of finding a middle ground between innovation and safeguarding basic civil freedoms in the era of AI.

Significance

Ethical Considerations in AI Surveillance The increasing use of AI in surveillance raises important ethical considerations that must be addressed. Balancing security and privacy concerns is crucial to ensure the responsible and ethical use of AI surveillance technology. One of the primary ethical considerations in AI surveillance is the potential violation of privacy rights. An extensive amount of data is collected by AI surveillance systems, including personal information, without explicit consent from those whose data were collected. This raises concerns about the potential for abuse, unauthorized access, and the misuse of personal data. It is essential that appropriate regulations and clear guidelines are established in order to protect individual privacy rights, as well as to ensure that data is handled responsibly. Additionally, the potential for bias and discrimination in AI surveillance systems also pose ethical concern. AI algorithms are trained by using large datasets, and data biases may already be present in these datasets. If these biases are remained unaddressed, AI surveillance systems may exacerbate biases against specific groups or individuals. It is crucial to establish and implement mechanisms that detect and mitigate actual and potential biases in AI algorithms to prevent and eliminate discrimination while ensuring fairness. Furthermore, there is a need to address the potential for the weaponization of AI surveillance technology. As AI becomes more powerful and capable, there is a risk that it could be misused for political repression or to target specific populations. The development and deployment of AI surveillance systems should be subject to international standards and regulations to prevent their misuse for human rights abuses. To address these ethical considerations, regulations and safeguards must be put in place to ensure responsible and ethical use of AI surveillance technology. It is vital to find a balance between ensuring security and safeguarding personal privacy rights. Transparent, clear and responsible governance structures must be put in place to oversee the creation, implementation, and operation of AI surveillance systems. For example, the European Union's GDPR sets guidelines for the collection, storage, and processing of personal data, including data collected through AI surveillance systems. The GDPR is designed to safeguard individual privacy rights and mandate that organizations manage personal data in a responsible and transparent manner. Other countries and regions can draw inspiration from such regulations to develop their own frameworks tailored to their specific contexts. In conclusion, ethical considerations play a crucial role in the use of AI in surveillance. Striking a balance between security needs and individual privacy rights is essential. Regulations and safeguards must be in place to ensure responsible and ethical use of AI surveillance technology. Addressing concerns related to privacy, bias, and the weaponization of AI is vital to build public trust and ensure the positive impact of AI in global surveillance.

Balancing Security and Privacy Concerns Finding a balance between security and privacy concerns is one of the key challenges in the use of AI in surveillance. While AI surveillance technology offers significant benefits in terms of enhanced security and public safety, it also raises important privacy considerations. The challenge lies in ensuring public safety without compromising individual privacy rights. AI surveillance systems have the capability to process large volumes of data, including personal details, to detect potential threats and criminal activities. However, collecting and processing personal data without explicit consent from individuals can lead to issues regarding privacy infringements and unauthorized surveillance. To strike a balance, it is crucial to establish clear guidelines and regulations that govern the use of AI surveillance technology. These guidelines should outline the permissible uses of AI surveillance systems, the collection and storage of data, and the limitations on data sharing. Additionally, mechanisms for transparency, accountability, and public oversight should be put in place to ensure that the use of AI surveillance technology is subject to scrutiny and safeguards against abuse. Furthermore, privacy-enhancing technologies can be employed to mitigate privacy concerns while still leveraging the benefits of AI surveillance. Techniques such as data anonymization, encryption, and differential privacy can help protect individuals' privacy by minimizing the collection and retention of personally identifiable information. By implementing these technologies, organizations can enhance privacy protection and build public trust in the responsible use of AI surveillance systems. For example, some AI surveillance systems employ real-time object detection algorithms that analyse video feeds from security cameras. These algorithms can detect specific objects or behaviours, such as weapons or suspicious movements, without capturing or storing personal data. This approach allows for effective threat detection while minimizing privacy risks. In conclusion, finding a middle ground to ensure public safety without compromising privacy is a challenge in the use of AI surveillance technology. Clear guidelines and regulations, along with privacy-enhancing technologies, can help strike a balance. By adopting responsible and transparent practices, it is possible to harness the benefits of AI surveillance while respecting individual privacy rights.

Literature Review

Privacy Theories

The examination of privacy in the context of AI-driven surveillance starts with traditional privacy ideas, which prioritise the individual's entitlement to govern their own personal information. Foundational framework is provided by seminal works by academics such as Alan Westin, who defined privacy as the assertion of people to independently decide when, how, and to what degree information about them is shared with others.[12] This study also includes modern viewpoints, such as Helen Nissenbaum's notion of contextual integrity. According to this theory, privacy is not just about keeping things secret or having control, but rather about the proper exchange of personal information based on the norms that are relevant to certain situations.[13]

[12] Margulis ST, "On the Status and Contribution of Westin's and Altman's Theories of Privacy" (2003) 59 Journal of Social Issues 411

[13] Grodzinsky FS and Tavani HT, "Privacy in 'the Cloud'" (2011) 41 ACM SIGCAS Computers and Society 38

Surveillance Theories

Surveillance theories play a vital role in comprehending the fundamental principles of surveillance and control that are inherent in AI technology. Michel Foucault's idea of the panopticon demonstrates how surveillance functions as a tool of power that regulates society, a premise that is particularly pertinent at a time when digital monitoring is ever-present.[14] Furthermore, the research conducted by intellectuals such as David Lyon enhances our comprehension by conceptualising surveillance in the digital era as a multifaceted socio-technical occurrence that extends beyond mere monitoring to include data gathering, examination, and profiling.[15]

Technology Ethics

Various ethical frameworks are used to examine the moral consequences of deploying technology, particularly in relation to AI and surveillance, to understand the ethics of technology. Utilitarian viewpoints assess the advantages and disadvantages of surveillance technology with the goal of determining whether their utilisation maximises general well-being. Deontological methods, in contrast, prioritise the rights and obligations linked to AI technology, placing emphasis on concepts like autonomy, consent, and fairness. Furthermore, virtue ethics provides valuable understanding of the character and intentions of those responsible for designing and implementing AI systems, allowing for critical evaluation of the moral qualities embedded in these technologies.

This article also examines integrative theoretical frameworks that merge perspectives from privacy, surveillance, and ethics to tackle the distinct difficulties presented by AI. These methods promote a fair evaluation that considers the possible advantages and drawbacks of technology breakthroughs. They emphasise the need of being vigilant about the ethical aspects of privacy and monitoring. This involves analysing legislative frameworks such as the GDPR in Europe, which represents an effort to establish laws that achieve a harmonious equilibrium, guaranteeing that technology is used in an ethical and fair manner for the benefit of mankind. The article constructs a comprehensive framework by integrating many theoretical viewpoints. This framework enables a critical analysis of the effect of AI-driven surveillance technologies on privacy rights and identifies approaches to promote ethical standards in technology deployment.

The Intersection of Datafication, Dataveillance, and AI: Navigating Privacy and Surveillance in the Digital Era

Datafication is the process of converting many components of an entity into measurable data that can be tracked, supervised, and examined.[16] The collection of vast volumes of data, known as 'datafied', allows for the personalisation and generalisation of information. Knowledge is highly valued due to its impact on individuals, services, and society. Data enables the process of profiling individuals, monitoring workers, optimising systems, managing, and controlling operations, predicting probabilities, and increasing the value of assets.

Governments and corporations are increasingly using data in ways that border on mass surveillance.[17] Surveillance is a purposeful systematic attention that combines elements of care

[14] Felluga D, "Modules on Foucault: On Panoptic and Carceral Society." *Introductory Guide to Critical Theory* (Purdue 2011)

[15] Lyon D, "Surveillance Capitalism, Surveillance Culture and Data Politics 1" *Data Politics* (Routledge 2019)

[16] Van Dijck, J, "Datafication, Dataism and Dataveillance: Big Data Between Scientific Paradigm and Ideology" (2014) 12 Surveillance & Society 197

[17] Connor BT and Doan L, "Government and Corporate Surveillance: Moral Discourse on Privacy in the Civil Sphere" (2019) 24

and control, particularly when conducted by public authorities. This surveillance can be paternalistic, aligning with the state's role in protecting citizens. The differentiates between direct surveillance, targeting specific individuals for specific reasons, and indirect surveillance, which lacks a specific target or purpose.[18] Given that data storage allows for prolonged availability, the purpose behind collecting data can change over time, making surveillance's intentions unstable. Additionally, the generation and collection of data may not always be purposeful but can occur as a side effect of using certain services. Ref also discusses how surveillance impacts privacy and suggests evolving it from mere observation. The author distinguishes passive observation, which does not intend to influence, from active observation, where collected data can be used to sanction or proactively interfere with individuals.[19] Thus, in the era of datafication, defining surveillance involves understanding its intentional use of data. The intensification of surveillance practices raises critical concerns regarding the fundamental human right to privacy. As surveillance capabilities expand, it is essential to ensure that these practices are balanced with the need to protect individuals' privacy rights, which are enshrined in international human rights law. This balance is crucial in maintaining democratic values and individual freedoms in an increasingly monitored world.

Data veillance is the result of the combination of the ongoing trend of datafication with the motives behind surveillance. Dataveillance is a surveillance system that uses the organisation and analysis of information to detect, monitor, track, control, forecast, and influence behaviours.[20] This is distinct from mere datafication, since it does not include the deliberate act of observation that is inherent in dataveillance.[21] Dataveillance, unlike conventional surveillance, is characterised by continuous and pervasive monitoring, without openly influencing behaviour.[22] Dataveillance functions at both individual and social levels, and may be either consensual or enforced, open or concealed. It harnesses both historical and current data, made possible by the interconnection, rapid processing, and automation of systems in both public and private domains of existence. Covert dataveillance, specifically, presents substantial social dangers because of the obscure characteristics of these systems, which are often extensive and persistent.[23] This kind of monitoring may have a significant influence on privacy and independence without the individual's awareness or agreement.

Data veillance is a kind of surveillance that relies on analysing and organising information to detect, monitor, track, control, forecast, and prescribe actions.[24] The distinction lies in the fundamental aim of observation, setting it apart from datafication. Both surveillance and dataveillance do not always result in inference. However, surveillance indicates a deliberate intention and, when conducted openly, influences people's actions. On the other hand, dataveillance refers to the constant and widespread monitoring of individuals. Furthermore, dataveillance may be conducted at both the individual and social level, and can be either voluntary or mandatory, as well as overt or covert. The usage of stored data, as well as real-time

Information, Communication & Society 52

[18] Penfold R, “Review of Surveillance Society: Monitoring Everyday Life; Everyday Surveillance: Vigilance and Visibility in Post Modern Life, by D Lyon & W Staples” (2002) 42(1) The British Journal of Criminology 222.

[19] Ibid.

[20] Clarke R, “Information technology and dataveillance” (1988) 31 Communications of ACM 498

[21] Lyon D, *Surveillance Society: Monitoring Everyday Life* (Open University Press 2001)

[22] Lyon D, *Surveillance Studies: An Overview* (Polity 2007)

[23] Haggerty KD and Ericson RV, “The Surveillant Assemblage” (2000) 51 The British Journal of Sociology 605

[24] Ibid. [19]

data, is implicated owing to the interconnection, high speed processing capacity, and automation applied to systems in both public and private aspects of an individual's life. Covert dataveillance poses significant hazards to society because to its secretive and pervasive character, which limits understanding of its operations and widespread presence.[25]

Personal data, as well as non-personal data, includes intrinsic information about the individual. There are two main challenges that arise from this situation: societal risks, which involve the ability to track and make assumptions about individuals or groups and risks at the individual level, which pertain to personal privacy. This profiling endangers individual autonomy and the principles of democracy. Technically, a problem arises in the interpretation of data throughout the sense-making process. This interpretation is mostly based on quantitative analysis, which may not fully incorporate the context. Identifying and evaluating biased conclusions may be challenging in this regard. Several research have identified and defined the hazards and risks associated with the increased monitoring facilitated by big data and AI.[26] The incorporation of AI into data processing and surveillance systems presents an intricate range of privacy concerns that need meticulous oversight by privacy and AI governance experts. AI improves surveillance capabilities, enabling the acquisition of a greater amount and more detailed personal data, hence increasing the hazards associated with monitoring. Additionally, it facilitates the automatic association of identities from various data sources, so greatly heightening the vulnerability of personal identities being revealed. AI can gather diverse data points about people to draw certain conclusions, which might potentially result in violations of privacy. An emerging issue occurs when using AI to predict personality characteristics based on physical looks, resembling old ideas like phrenology and physiognomy. This creates specific privacy problems that have not been addressed in established frameworks like Solove's taxonomy. Additionally, AI has the potential to result in the secondary utilisation of personal data, when information is repurposed for purposes that were not initially intended, without obtaining the approval of the user. The lack of transparency in AI algorithms may lead to exclusion since it hinders consumers' ability to comprehend or manage the utilisation of their data. The substantial data storage demands of AI systems amplify the vulnerability to breaches and unauthorised access, increasing insecurity. AI approaches, particularly in the field of generative AI, have the potential to unintentionally reveal sensitive information. Additionally, AI's capacity to generate realistic but fabricated material may contribute to the dissemination of disinformation or the distortion of reality. Moreover, AI has the potential to reveal confidential information obtained from harmless data, and its advanced skills might inadvertently increase the accessibility of sensitive material, leading to concerns about inappropriate data distribution. AI technologies have the capability to invade personal areas, often as a component of heightened monitoring measures, so adding complexity to the privacy situation. The presence of these hazards highlights the need of using strong risk assessment models to thoroughly examine and minimise the potential privacy consequences of AI systems.

The Emergence of Data veillance of Public Spaces for Law Enforcement Purposes

The process of converting activity in public places into data intends to support authorities in

[25] Fontes C and others, "AI-Powered Public Surveillance Systems: Why We (Might) Need Them and How We Want Them" (2022) 71 Technology in Society 102137

[26] Sætra H, "Freedom under the gaze of Big Brother: Preparing the grounds for a liberal defence of privacy in the era of Big Data" (2019) 58 Technology in Society 101160; Ioannou A and Tussyadiah I, "Privacy and Surveillance Attitudes during Health Crises: Acceptance of Surveillance and Privacy Protection Behaviours" (2021) 67 Technology in Society 101774; Manheim K and Kaplan L, "AI: Risks to privacy and democracy" (2019) 21 Yale Journal of Law and Technology 106

managing urban areas by adopting a more objective and data-driven approach to political decision-making and urban policy. Although data is theoretically considered to be objective and unbiased, the interpretation of data may be influenced by ideological biases. This can result in the development of new techniques for gathering and analysing large amounts of data related to metropolitan areas. Public places, such as streets, squares, theatres, and sports halls, are open to everyone and have a significant impact on promoting inclusion, cultural values, and democratic participation. These areas also serve as venues for power dynamics and social interactions. Public space is an area where the public has control and is overseen by officials who are responsible for preserving order and upholding the law. Surveillance, such as the use of closed-circuit television (CCTV) cameras in urban areas, assists in the enforcement of law and order by facilitating street police and using advanced technology to monitor public spaces.

Surveillance is altering the essence of public space by influencing individuals' behaviour.[27] The implementation of CCTV systems has provided public authorities with a valuable instrument to bolster their efforts in police and law enforcement. However, recent studies have shown that these systems may not be as effective as anticipated, and it is important to consider individual conditions before determining if CCTV is the optimal answer for enhancing safety and decreasing crime in public areas.[28] In addition, the use of CCTV might give rise to ethical concerns about violations of individual privacy, as well as problems of transparency, discrimination, and exclusion.

AI application in Surveillance

The utilization of AI in security applications has surged significantly in recent years. AI has become crucial in advancing modern police services, improving interactions between law enforcement and communities, building trust, and strengthening community relations. Technologies such as biometrics, FRT, smart cameras, and video surveillance systems are seeing increased adoption. Deloitte's recent study indicates that smart technology deployment, including AI, could reduce urban crime rates by 30 to 40 percent, and potentially cut emergency service response times by 20 to 35 percent[29]. Privacy and data protection measures are deemed successful. Urban areas are enhancing their security measures by allocating resources towards advanced technologies. These include systems for mapping crime as it happens, controlling large gatherings effectively, and detecting gunshots in real time. This investment reflects a growing focus on leveraging technology to improve public safety across cities. only when they are properly utilized, implemented, monitored, and enforced. Furthermore, the European Data Protection Supervisor's Preliminary Opinion 5/2018 on privacy by design notes that the uptake of commercial products and services that fully incorporate privacy by design and by default is still limited. In certain cases, the primary objectives of an AI system or the intrinsic possibility for technology to conflict with societal norms and fundamental rights can diminish the efficacy of measures like privacy or data protection impact assessments and privacy by design principles.

[27] Day J, “What Is Wrong About Public Surveillance? I Liberties.Eu” (*Liberties.eu*, April 25, 2023) <https://www.liberties.eu/en/stories/public-surveillance/44774> accessed February 1, 2024; McGrath JE, *Loving Big Brother: Performance, Privacy and Surveillance Space* (Psychology Press 2004)

[28] Koskela H, “‘The Gaze without Eyes’: Video-Surveillance and the Changing Nature of Urban Space” (2000) 24 Progress in Human Geography 243

[29] Deloitte, “Surveillance and Predictive Policing Through AI” *Deloitte* <https://www.deloitte.com/global/en/Industries/government-public/perspectives/urban-future-with-a-purpose/surveillance-and-predictive-policing-through-ai.html> accessed February 1, 2024

This highlights a significant challenge in ensuring that these protective measures function as intended in real-world applications.[30] Urban regions are notably using facial recognition and biometrics (84%), as well as police body cameras and in-car cameras (55%). Furthermore, 46% of cities are employing drones and aerial surveillance, while 39% are adopting crowdsourced crime reporting and emergency apps to enhance public safety. However, only 8% of individuals engage in data-driven policing.[31] T The AI Global Surveillance Index 2019 highlights that a significant number of countries are integrating artificial intelligence into their public safety strategies. Specifically, 56 out of the 176 countries examined have adopted AI-based tools as part of their safe city initiatives aimed at enhancing surveillance capabilities. This adoption showcases a global trend towards the use of advanced technology in law enforcement and public safety operations.[32] The International Data Corporation has projected that around 40 percent of police agencies will have integrated digital tools into their operations. This integration is expected to include technologies such as live video streaming and shared workflow systems. The adoption of these digital tools is aimed at not only enhancing community safety but also at streamlining the response mechanisms of law enforcement. By utilizing these advanced technologies, police agencies intend to improve real-time communication and coordination during incidents, thereby creating a more effective and efficient response framework. This shift towards digitalization represents a significant evolution in policing strategies, reflecting a broader trend towards the use of technology in enhancing public safety and community engagement.[33]

Urban security has always relied on monitoring as a fundamental tool. However, cities are increasingly enhancing its effectiveness by using surveillance data analysis to forecast criminal activities. Surveillance cameras have historically recorded photos, but with the help of AI, the photos may now be examined and addressed with greater speed.[34] The fusion of machine learning and big data analytics enables the analysis of extensive volumes of crime and terrorist data to detect patterns, correlations, and trends. When law enforcement organisations have the right connections, technology becomes a fundamental tool that helps them work more efficiently and have an impact on changing behaviour. The primary objective is to create adaptable security systems that can identify criminal or terrorist networks and suspicious behaviour, hence improving the effectiveness of judicial systems.

Furthermore, cities are actively investigating alternative applications of surveillance and AI technology. Urban tolling and emission zones, which employ AI to reduce pollution and increase sustainability, are being put into place. The avoidance of potential health catastrophes is another rapidly expanding area of application. The metro system in Paris is monitored by AI systems to ensure that riders are wearing face masks as required. The objective is not to ascertain and penalise those who violate rules, but rather to provide anonymous data that assists authorities in

[30] Sloly P, “Emerging Tech That Can Make Smart Cities Safer” (*Deloitte Canada*, October 3, 2018) <https://www2.deloitte.com/ca/en/pages/public-sector/articles/emerging-tech-smart-cities-safer.html> accessed February 1, 2024

[31] ESI ThoughtLab, “Smart City Solutions for a Riskier World” (ESI ThoughtLab 2021)

[32] Feldstein S, *The Global Expansion of AI Surveillance* (Carnegie Endowment for International Peace 2019)

[33] Barker L and others, “IDC FutureScape: Worldwide Smart Cities and Communities 2024 Predictions” (IDC 2023)

[34] Apene OZ, Blamah NV and Aimufua GIO, “Advancements in Crime Prevention and Detection: From Traditional Approaches to Artificial Intelligence Solutions” (2024) 2 European Journal of Applied Science, Engineering and Technology 285

predicting future instances of infectious epidemics.[35]

Designing widely accepted ethical AI systems is almost unattainable due to the immense complexity of the different settings they must incorporate. The Deloitte report emphasises the need for careful consideration of ethical and regulatory issues while using AI for surveillance and predictive policing. While the value proposition of these technologies may seem appealing in terms of use cases, it is essential to safeguard freedoms and civil rights via appropriate rules on privacy and human rights. Despite its problematic nature in Western nations, predictive policing is being extensively used in Asia, even though several towns in the US have prohibited its use. A poll conducted by Deloitte has shown significant variations in the level of acceptability and attractiveness of these technologies across different locations. Surveillance and predictive policing are both seen as undesirable in privacy-conscious regions like the EU and North America. Latin America and Asia have seen higher levels of acceptance.

Legal Policy

Legal experts and data protection enforcement bodies assert that AI not only impacts various rights but also presents significant issues in terms of privacy and data protection.[36] These considerations encompass informed consent, surveillance, and breaches of individuals' data protection rights. These rights include the ability to access personal data, the right to halt processing that could lead to harm or distress, and the right to avoid decisions made solely through automated processing. Additionally, addressing these issues is crucial for maintaining trust and integrity in data management practices.[37] There are concerns regarding the accountability of algorithms, specifically the lack of control and oversight individuals have over the use of their personal data to make inferences about them. To bridge the existing accountability gap, advocates are proposing a new data protection entitlement termed the 'right to reasonable inferences'. This right aims to mitigate the risks associated with high-risk inferences, which are those that infringe on privacy or damage reputation and are difficult to verify in terms of predictiveness or being founded on personal opinions.[38]

Research has found the likelihood of enhanced privacy concerns and the amplification of surveillance capabilities.[39] The discussion paper from the UK Information Commissioner's Office explored the effects of big data, AI, and machine learning on data protection, emphasizing the invasive aspects of big data profiling and the transparency issues stemming from the complex methodologies employed in big data analytics.[40]

[35] Himeur Y and others, “Face Mask Detection in Smart Cities Using Deep and Transfer Learning: Lessons Learned from the COVID-19 Pandemic” (2023) 11 Systems 107

[36] libertés FranceC nationale de l’informatique et des, *How Can Humans Keep the Upper Hand?: The Ethical Matters Raised by Algorithms and Artificial Intelligence: Report on the Public Debate Led by the French Data Protectional Authority, CNIL, as Part of the Ethical Discussion Assignment Set by the Digital Republic Bill: December 2017* (CNIL 2018)

[37] Brundage M and others, “The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation” (2018) ArXiv

[38] Rodrigues R, “Legal and human rights issues of AI: Gaps, challenges and vulnerabilities” (2020) 4 Journal of Responsible Technology 100005

[39] Van den Hoven van Genderen R, “Privacy and Data Protection in the Age of Pervasive Technologies in AI and Robotics” (2017) 3 European Data Protection Law Review 338

[40] Information Commissioner’s Office, “Big Data, Artificial Intelligence, Machine Learning and Data Protection” (Information Commissioner’s Office 2017)

In the EU privacy and data protection laws, such as the GDPR, formally offer strong safeguards to protect against violations of data subjects' rights. These include rights to transparency, information, and access, ensuring that individuals have a clear understanding and control over how their personal data is used.[41], rectification[42] and erasure[43], right to object to automated individual decision-making[44] etc.

Disclosure of the risks associated with AI usage is highly encouraged in terms of informed consent[45]; Developers must ensure that they adhere closely to ethical standards and regulatory requirements throughout all stages of data processing. This approach is crucial not only for compliance but also for maintaining the integrity and security of the data they handle. By doing so, they can avoid potential legal issues and build trust with users by upholding high ethical practices." According to Vayena, data provenance and permission for use and reuse are seen to be very crucial.[46] It is advised to use secure multi-party computing in surveillance settings. This approach uses protocols that facilitate the joint computation of functions by multiple parties, while ensuring the privacy of each party's inputs remains protected.[47] Additional strategies that are being used or suggested include the use of auditable machine algorithms, privacy impact assessments, privacy by design, anonymization, privacy notifications, and privacy by design.[48]

Laws pertaining to privacy and data protection do not cover every AI concern. The rapidly evolving field of AI necessitates "understanding and resolving the scope of data protection law and principles in a challenging task, but it is essential to avoid burdening AI with needless regulatory requirements or with uncertainty about whether regulatory requirements apply".[49] Privacy and data protection measures are deemed successful only when they are properly utilized, implemented, monitored, and enforced. Furthermore, the European Data Protection Supervisor's Preliminary Opinion 5/2018 on privacy by design notes that the adoption of commercial products and services that fully integrate privacy by design and by default remains sparse. In certain cases, the primary objectives of an AI system or the inherent potential for technology to clash with societal values and fundamental rights may undermine the effectiveness of initiatives such as privacy or data protection impact assessments and privacy by design principles. This highlights a significant challenge in ensuring that these protective measures function as intended in real-world applications.[50] In order to help close the accountability gap currently caused by "high risk inferences," a new data protection right called the "right to reasonable inferences" is required. The GDPR falls short in offering sufficient protection against sensitive inference[51] and lacks adequate remedies for challenging inferences or significant decisions derived from them[52].

[41] (Article 15), General Data Protection Regulation

[42] (Article 16), General Data Protection Regulation

[43] (Article 17), General Data Protection Regulation

[44] (Article 21), General Data Protection Regulation

[45] Rigby MJ, "Ethical Dimensions of Using AI in Health Care" (2019) 21 AMA Journal of Ethics 121

[46] Vayena E, Blasimme A and Cohen IG, "Machine Learning in Medicine: Addressing Ethical Challenges" (2018) 15 PLOS Medicine e1002689

[47] Brundage M and others, "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation" (2018) ArXiv

[48] Ibid [38]

[49] Centre for Information Policy Leadership, "Artificial Intelligence and Data Protection: Delivering Sustainable AI Accountability in Practice" (2018)

[50] European Data Protection Supervisor, "Preliminary Opinion on Privacy by Design" (European Data Protection Supervisor, 2018)

[51] Article 9, General Data Protection Regulation

[52] Article 22(3), General Data Protection Regulation

Methodology

Research Design

The major research approach in this article is document analysis, which is done using a qualitative methodology. Getting a thorough grasp of the intricate social, ethical, and legal aspects of AI-driven surveillance technology is especially well-suited to document analysis. Four major document categories will be thoroughly examined as part of the document analysis. The first category includes academic literature, industry reports, and technical articles that describe the evolution and capabilities of important AI surveillance technologies, such as smart city platforms, face recognition, emotion detection, and predictive police algorithms. This offers perceptions on the state of technology now and how these technologies are developing. Documents from corporations and the government that describe the use and implementation of AI surveillance technology in both public and private sectors make up the second essential category. These publications' analysis clarifies the practical applications and implementations of these technologies in various industries and geographical areas. Existing laws, rules, legislation, and policy initiatives pertaining to AI governance, data protection, privacy, and industry-specific AI surveillance concerns make up the third major area. These materials are reviewed to analyse the state of policy and find areas where the privacy and human rights consequences of AI monitoring are not sufficiently addressed. The media stories and reports from civil society organisations that detail the social reactions and effects of AI surveillance technology from the viewpoint of impacted communities and groups make up the last category. This offers vital information on responses that are implemented outside of official policy channels. The goal of this article is to provide a thorough knowledge of the technological, deployment, policy, and sociological aspects related to AI surveillance technologies via a qualitative analysis of these four essential document types. The results of this comprehensive document analysis will draw attention to important issues, disagreements, and gaps. Consequently, policy suggestions and future research objectives will be informed by this, ensuring that the development of AI surveillance technology is consistent with ethical values and privacy rights.

Data Collection

The process of collecting data will include obtaining pertinent papers from a variety of sources in four main categories: technical documents, business and government documents, laws, rules, and policies, and reporting from the media and civil society.

Technical materials will be gathered to comprehend the advancements and potential of the main AI surveillance systems, including scholarly articles, conference proceedings, and company reports. Scholarly resources such as IEEE Xplore, ACM Digital Library, arXiv, and SpringerLink will be used for targeted searches in order to collect peer-reviewed academic material. You may find pertinent technical articles by searching for terms like "facial recognition," "affect recognition," "emotion detection," "predictive policing," "smart cities," and "intelligent video surveillance." Additional technical reports, white papers, and conference papers may be found with the help of Google Scholar. Additionally, industry white papers released by technology firms developing or using AI surveillance technologies might be found by doing general online searches. Beyond scholarly research, these industrial papers will provide insights into development and commercialization in the real world.

Corporate and Governmental Documents: Government documentation pertaining to the acquisition, application, and regulation of AI surveillance technology will be gathered in order to comprehend real-world deployment. These include of policy white papers, impact assessments, audit reports, oversight hearing recordings, and requests for proposals. Access to information requests, searchable legislative archives, and official government repositories will all be used to get these papers. Annual reports, press releases, marketing materials, and business policies regarding AI surveillance technologies will all be examined in relation to corporate deployment. These will be gathered via news announcements, media articles, and publicly accessible disclosures on business websites.

Laws, Rules, and Policies: The current regulatory environment around AI surveillance will be clarified via an examination of pertinent laws, rules, and policies. Official government gazettes, legislative archives, and policy databases will be the sources of legal papers that are methodically gathered. You may find rules and regulations by searching for phrases like "privacy," "surveillance," "AI," "facial recognition," "biometrics," and "data protection." We will also obtain draft legislation pertaining to AI monitoring regulations from official websites. Included will be international policy papers on AI ethics and governance from institutions such as the UN, OECD, and EU.

Documents from civil society and media reports: Media reports and documents from civil society may be gathered with the use of Google News searches, focused inquiries on digital rights organisations (such as Privacy International, ACLU, and EFF), and reference harvesting from important publications. These will give light on the effects of AI surveillance technologies locally and how the public reacts to them. Five years' worth of dates will be used in the compilation of media reports. The importance of rights-based viewpoints will be highlighted by ground-breaking reports from civil society that detail issues and campaigns pertaining to AI surveillance.

It is anticipated that between 100 and 200 papers would be collected in total for these four essential categories. During repeated searches, saturation sampling will be used to guarantee thorough coverage until fresh documents stop offering new insights.

Case Studies/Analysis

Overview

AI is developing at a fast pace, ushering in a new age of surveillance technologies that are revolutionising data collection, analysis, and use. Facial recognition systems and predictive policing algorithms are two of the most well-known applications. These have attracted a lot of attention because of their enormous effects on civil liberties, privacy, and human rights. Driven by advanced AI models, Facial Recognition Technology (FRT) has proliferated and is now used in a wide range of applications, from social media platforms to law enforcement. FRT has the potential to be revolutionary, but it also presents serious issues with prejudice, invasion of privacy, and abuse. Predictive policing algorithms have also come under fire for concerns of accountability, transparency, and the maintenance of systemic biases. These algorithms use machine learning methods to anticipate crime trends and allocate law enforcement resources. It is critical to examine the effects of these technologies from both a technical and a regulatory standpoint as they spread further. This case study explores prominent instances of AI-powered surveillance technology, showcasing the results of expert interviews and document analysis. The study delves into the complex interactions that occur between legal frameworks and technology breakthroughs, providing valuable perspectives on how these innovations might be appropriately used to protect basic rights and ethical ideals. This research intends to add to the continuing conversation by examining the subtleties of AI-driven surveillance and educating policymakers, technologists, and civil society organisations about the potential and problems that lie ahead. In the end, it emphasises how critical it is to adopt a balanced strategy that encourages creativity while providing strong protections against the possible abuse of these great technology.

FRT

AI could outwit efforts to circumvent face recognition technology. Methods such as liveness detection are used to verify the authenticity of the individual presenting, distinguishing them from a still image or a recorded video. AI algorithms undergo continuous learning and enhancement. By analysing large quantities of facial data, they are able to identify faces with much enhanced accuracy compared to previous methods. AI extends beyond first verification. It can continuously monitor and confirm a user's identity throughout a session. AI streamlines the verification process, enhancing its speed and efficiency for consumers. Eliminate the need for laborious manual inspections.

AI Making Facial Recognition Smarter and More Powerful

FRT is rapidly progressing and becoming widespread, being used in many fields such as law enforcement and social media. Although FRT can bring about enormous changes, it also gives rise to substantial issues over privacy and human rights. It is imperative for the United Nations and national governments to acknowledge and control these hazards associated with the technology.

The Yao Report highlights the significant progress achieved by deep learning in face recognition systems. This innovation has revolutionised the industry by introducing autonomous feature learning, enhancing accuracy, and providing strong representations.[53] Deep learning models have successfully addressed the constraints of old approaches by allowing the extraction of intricate face features from raw data. These models perform very well in real-world situations that include different stances, lighting conditions, and occlusions. Deep learning has many benefits in face recognition, including the capacity to scale, adapt, and perform in real-time. This makes it a very desirable option for a wide range of applications, such as access control and surveillance. The future of deep learning in face recognition has significant potential, as current research efforts aim to improve the resilience of models, address biases, and protect privacy. The combination of multimodal recognition and multidisciplinary cooperation will be crucial in determining the future path of this technology.

An important issue is the possibility of face recognition technology being misused by governments, companies, or people because of the absence of norms and standards. With few exceptions, the United States now lacks authoritative advice, rules, or legislation to effectively deal with issues concerning the use of face recognition technology.[54] The technology has the potential to infringe upon individuals' privacy by gathering and retaining large quantities of personal information without their authorization. FRT has the potential to disrupt and significantly impact the principles of privacy, civil liberties, human rights, and the creation of biased systems that unfairly target specific populations. It can also contribute to the perpetuation of discrimination, even if it may not explicitly violate legal statutes or constitutional provisions.[55]

[53] Yao Y, "Research on facial recognition system based on deep learning" (2024) 34 Applied and Computational Engineering 232

[54] Fleischer RS, "Bias in, Bias out: Why Legislation Placing Requirements on the Procurement of Commercialized Fascial Recognition Technology Must be Passed to Protect People of Color" (2020) 50 Pub. Cont. L.J. 63

[55] McClellan E, "Facial Recognition Technology: Balancing the Benefits and Concerns" (2020) 15 Journal of Business & Technology Law 2

Argentina, Brazil, Chile, Colombia, Ecuador, and Mexico are examples of states that possess both data privacy laws and operational facial recognition technology for law enforcement purposes.[56] Data protection laws provide a baseline of regulations and safeguards to guarantee that personal information is handled in a lawful and proportionate manner. These laws require that data is utilized solely for the purpose it was collected and that it remains accurate, relevant, and securely stored. Every legislation examined in the research has a comparable clause about the valid justification for handling personal data. Typically, every person should provide their explicit permission for the collection and processing of personal data, unless there are specific circumstances that allow for an exemption. Similarly, most of these laws include a provision that allows the government to handle personal data without seeking permission in cases where it is necessary for carrying out State-related activities and/or public policies, or where it is mandated by other laws and regulations. However, most nations that are using face recognition technology do not have clear legislation in place for video surveillance, and especially for facial recognition systems. The majority of the systems now in operation in Argentine and Colombian underground stations, as well as in the largest Mexican marketplace and the drones equipped with face recognition technology in Chilean sky, are operating without any kind of control. Governments have justified the application of these laws based on a broad national and public security mandate. However, there are no additional criteria or safeguards in place to protect people.[57] Preceding legislation is crucial for ensuring openness, safeguarding against possible abuses of authority, and preventing discrimination.

FRT is used in many areas including law enforcement, border security, advertising, financial services, real estate, and social networking sites. Although FRT offers benefits such as improved security and user ease, it also raises substantial issues surrounding privacy, human rights, and civil liberties. Furthermore, it has the potential to contradict the Sustainable Development Goals (SDGs) set by the United Nations, particularly those linked to gender equality (Goal 5), industry, innovation, and infrastructure (Goal 9), and peace, justice, and strong institutions (Goal 16). These problems emphasise the need of adopting a well-rounded strategy when using face recognition technology.

Governmental abuse an important issue with FRT is its susceptibility to misuse by governmental bodies and law enforcement authorities. The use of face recognition technology by authorities enables the identification and monitoring of persons without their knowledge, resulting in an escalation of government surveillance and the gradual erosion of personal private rights. Furthermore, FRT has the capacity to function as a mechanism for societal manipulation, especially inside autocratic governments. An egregious instance occurs when governments use FRT to surveil the presence of individuals during authorized demonstrations.

Risk of Gathering Biometric Data

A further risk arises from the possibility of a more advanced face recognition technology exacerbating existing prejudices and discrimination. Law enforcement's utilisation of FRT has prompted concerns regarding the impact of racial biases on its effectiveness. It has been observed

[56] Badillo M, "Navigating the Complexities of Facial Recognition for Public Security in Latin America" (*International Bar Association,* May 9, 2023) <https://www.ibanet.org/facial-recognition-security-latin-america> accessed March 1, 2024

[57] Findlay M, Ong LM and Zhang W, *Elgar Companion to Regulating AI and Big Data in Emerging Economies* (Edward Elgar Publishing 2023)

that FRT demonstrates reduced accuracy when identifying individuals with darker skin tones and women, leading to incorrect identifications and wrongful arrests.[58] This problem results in the unfair targeting and profiling of marginalised communities. The acquisition and use of biometric data also poses a risk to personal privacy and security. There is a basic absence of permission and transparency when individuals are vulnerable to face recognition technologies. FRT used in public areas, such as airports or retail centres, might engender a feeling of perpetual monitoring and obligatory agreement. Improper use of face recognition data may lead to identity theft and several types of cybercrime.

The potential harm posed by face recognition technology is pertinent to several SDGs, namely those pertaining to human rights, equality, and innovation. The objective of SDG 16 is to promote peaceful and inclusive societies, ensure access to justice for all, and build effective, accountable, and inclusive institutions at every level. FRT may compromise these objectives by allowing governments and other organisations to surreptitiously monitor people, resulting in a restriction on personal liberties. An inherent issue is in the absence of responsibility for organisations that misappropriate FRT. There have to exist explicit and unambiguous guidelines on the use of this technology in investigations and other law enforcement endeavours. A further method to enhance accountability is giving people the opportunity to contest the improper use of this technology.[59]

The objective of SDG 5 is to achieve gender equality and empower all women and girls. Nevertheless, face recognition technology has shown inherent biases and mistakes, especially in its ability to correctly identify individuals belonging to ethnic minorities and women. This may further entrench prevailing social disparities in domains such as work, education, and law enforcement - therefore reinforcing gender and racial prejudices.

The objective of SDG 9 is to is to build robust infrastructure, promote inclusive and sustainable industrialization, and foster innovation. FRT has the capacity to enhance security and reduce crime, but it also presents substantial risks to personal privacy and civil rights. For instance, FRT may be used to trace an individual's mobility, supervise their conduct, and gather confidential data without obtaining permission. Hence, it is crucial to guarantee that progress in this field is created and executed in a conscientious way that considers human rights issues. This may be achieved via the promotion of openness and the implementation of measures that empower people to exercise control over their personal information.

Existing Policies

When formulating policy restrictions for face recognition technology, it is possible to utilise current laws as a starting point. Two notable examples are the Biometric Information Privacy Act (“BIPA”) and the European Union's GDPR. The BIPA mandates that organisations must get informed permission from people before to gathering their biometric data, and must also declare the intended use, storage, and sharing of this data. Additionally, it grants people the legal entitlement to initiate legal proceedings against organisations that have infringed upon their biometric privacy. This incentivizes organisations to prioritise their responsibilities and

[58] Bacchini F and Lorusso L, “Race, Again: How Face Recognition Technology Reinforces Racial Discrimination” (2019) 17 Journal of Information, Communication and Ethics in Society 321

[59] Donahoe E, Metzger M and Wainscott K, “Global Digital Policy Snapshot: Protecting Human Rights in the Regulation of Facial Recognition Technology” (Stanford University Cyber Policy Center 2020)

guarantees that people have a legal recourse in case their rights are infringed upon. This ensures that the technology is used in an ethical fashion and safeguards persons from the adverse effects of biased systems. The GDPR requires organisations to get explicit and informed permission before to collecting biometric data. Furthermore, the data collected must be essential and proportional to the intended purpose. The UN might implement these principles to guarantee people' sovereignty over their biometric data.[60]

Defect and Challenge

The advancement of deep learning in face recognition has had a profound effect on the discipline, however it is not without challenges. Data bias is a significant concern, since biased training data may result in erroneous and unfair conclusions, especially for marginalised communities.[61] In addition, privacy problems emerge from the inclusion of sensitive biometric data in face recognition technology, which may lead to ethical and legal difficulties owing to the possibility for abuse or unauthorised access to this information. Adversarial assaults provide a security threat, since even subtle alterations to face, photos may lead to incorrect categorization. Furthermore, deep learning models may have difficulties in correctly executing in real-world scenarios that include different lighting conditions, stances, and occlusions, hence impacting their resilience. The demanding training requirements and ethical issues associated with monitoring and discrimination make the adoption of face recognition technology more complex.

Prospects

However, despite these obstacles, the prospects for deep learning in face recognition are encouraging. Current research efforts are centred on improving the durability and impartiality of models, mitigating biases, and expanding privacy-preserving strategies.[62] The use of hardware acceleration and multimodal recognition enables the practical and reliable implementation of real-time deployment in many situations. It is essential to prioritise multidisciplinary cooperation between computer scientists, ethicists, legal experts, and politicians to shape a future where face recognition technology may be used responsibly to create great social effects while still protecting human rights and privacy.

Policy Recommendations

International bodies such as the International Telecommunication Union, The United Nations Educational, Scientific and Cultural Organization, and the Office of the United Nations High Commissioner for Human Rights should establish specific guidelines for the use of FRT. They may form a task force to evaluate the potential risks of FRT to SDGs 5, 9, and 16. The purpose of this task group is to provide suggestions for the handling, retention, and dissemination of biometric data, as well as the use of FRT in law enforcement and international security contexts, with the aim of ensuring accountable utilisation and openness. It is imperative that FRT be specifically developed to tackle existing prejudices and inaccuracies, especially those that put women and individuals belonging to racial and ethnic minorities at a disadvantage. Enhancing the diversity of the teams involved in developing this technology and undertaking more research on its gender and racial biases might potentially address these difficulties. Moreover, enhancing the transparency and accessibility of data sharing is crucial for safeguarding personal privacy and

[60] Nguyen FQ, "The Standard for Biometric Data Protection" (2018) 7 *Journal of Law & Cyber Warfare* 1

[61] Kaur P and others, "Facial-Recognition Algorithms: A Literature Review" (2020) 60 Medicine, Science and the Law 131

[62] Adjabi I and others, "Past, Present, and Future of Face Recognition: A Review" (2020) 9 Electronics 1188

fostering trust between citizens and governments. Public education initiatives should be undertaken by governments and business organisations to enhance knowledge of the risks and advantages associated with FRT. Organisations using FRT must provide explicit details on the types of data collected, the purpose for which it is used, any sharing of data with external parties, the duration for which it is stored, the criteria for data deletion, and the procedures for people to opt out of data sharing. In order to tackle these issues, the United Nations may contemplate the establishment of a dedicated panel of experts on FRT. This group is responsible for developing regulatory standards and assessing the impact of FRT on privacy and human rights.

AI empowered Drone

Ethical Issues

The incorporation of AI into drone technology gives rise to a multitude of ethical problems that need meticulous attention and resolution. An important issue is the possible abuse of drones for surveillance, which might violate people's private rights and civil freedoms. With the increasing prevalence of drones outfitted with cameras powered by AI, it is imperative to establish explicit norms and laws to control their use in places that need special consideration, such as public spaces, residential neighbourhoods, and business premises.[63]

AI and Drone Application

An important use of AI in drone technology is autonomous navigation, which entails the use of AI to calculate flight paths. Conventional drones depended on predetermined flying routes, which restricted their capacity to adjust to dynamic circumstances. AI enables drones to independently strategize and modify their flight routes in real-time, considering environmental conditions, mission goals, and safety concerns.[64] AI algorithms process data from several sensors on board, including GPS, inertial measurement units, and obstacle detection systems, to develop flight routes that are optimised in real-time. These algorithms consider variables like as weather conditions, airspace rules, and terrain characteristics to guarantee optimal and secure navigation. By AI-powered flight path planning, drones can traverse intricate surroundings with accuracy and dexterity, hence creating opportunities for many applications such as aerial surveillance, mapping, and inspection.[65]

Another crucial use of AI in drone navigation is the identification and evasion of obstacles. Conventional drones relied on human intervention to avoid obstacles, which restricted their capacity to function in crowded or unexpected surroundings. Autonomous drones, using AI technology, are fitted with sophisticated sensors and computer vision systems that enable them to identify impediments in their trajectory and navigate around them. AI systems process sensor data in real-time to accurately detect and classify obstacles such as structures, vegetation, or other unmanned aerial vehicles. Subsequently, they develop alternate flight routes to escape collisions while also optimising for mission goals. This feature is especially advantageous in tasks like

[63] Ezeigweneme CA and others, “Review of telecommunication regulation and policy: comparative analysis USA and Africa” (2024) 5 Computer Science & IT Research Journal 81
[64] AlMahamid F and Grolinger K, “Autonomous Unmanned Aerial Vehicle Navigation Using Reinforcement Learning: A Systematic Review” (2022) 115 Engineering Applications of Artificial Intelligence 105321
[65] Ibid

search and rescue, where drones must manoeuvre through intricate urban settings or thick vegetation to find and aid those in need.[66]

Computer vision is essential for drones to identify and monitor items in their environment. AI systems use visual data obtained from cameras on board to detect and categorise items, such as automobiles, people, or animals. Once detected, drones have the capability to monitor the movement of these items in real-time, offering important situational awareness for a range of applications. Object identification and tracking are crucial in fields including law enforcement, border surveillance, and wildlife monitoring.[67] Authorities may enhance their surveillance capabilities by using drones fitted with AI-powered computer vision systems. These drones can efficiently and accurately follow criminals, monitor border crossings, and perform wildlife assessments. AI-powered drones have exceptional proficiency in analysing visual data for a wide range of applications in many sectors. AI algorithms use visual data acquired by drones to analyse and extract important insights, which may then be used to guide decision-making in many fields such as infrastructure inspection and environmental monitoring. Drones outfitted with computer vision systems can identify problems or abnormalities in infrastructure during inspection, including structures like bridges, pipelines, and electricity lines. AI systems use visual data analysis to detect indications of damage, corrosion, or deterioration, facilitating proactive maintenance and repair efforts. Similarly, drones may be used in environmental monitoring to record visual data for the purpose of assessing the health of ecosystems, monitoring animal populations, or detecting changes in land use patterns. AI systems analyse this data to identify environmental hazards, monitor changes in habitats, or discover unlawful actions such as deforestation or poaching.

To summarise, the use of AI in drone technology is wide-ranging and revolutionary, including autonomous navigation and computer vision. AI-driven drones are transforming several sectors by facilitating independent planning of flight paths, detecting and avoiding obstacles, recognising and monitoring objects, and making data-based decisions in precision agriculture. As AI progresses, drones will experience increased capabilities, leading to the exploration of new opportunities for innovation and efficiency in several fields.

Machine Learning

To avoid costly breakdowns, drone technology uses machine learning for predictive maintenance, which involves finding and fixing system issues before they happen. AI systems have the potential to spot patterns and outliers in drone performance data, which might indicate component failure or malfunction. Machine learning models using telemetry data, sensor readings, and flight records have the capability to identify mechanical defects, battery degradation, and software mistakes at an early stage. AI equipped drones could identify deviations from expected behaviour and alert operators to possible issues, allowing for proactive maintenance.[68]

Implementing machine learning techniques for predictive maintenance improves the dependability and lifespan of drones, resulting in decreased periods of inactivity and lower

[66] Tullu A and others, “Machine Learning Approach to Real-Time 3D Path Planning for Autonomous Navigation of Unmanned Aerial Vehicle” (2021) 11 Applied Sciences 4706

[67] Ogundairo O and others, “Review on maldi mass spectrometry and its application in clinical research” (2023) 3 International Medical Science Research Journal 108

[68] Nwank Nwankwo CO and others, “Reviewing the Role of AI in Drone Technology and Applications” (2024) 5 Computer Science & IT Research Journal 741

operating expenses. Through proactive measures to tackle system difficulties, drones may function with enhanced dependability and effectiveness, hence reducing the likelihood of unforeseen interruptions or equipment malfunctions. Algorithms facilitate the optimisation of maintenance schedules, prioritisation of repairs according to criticality, and prediction of component lifespans for drones. The proactive maintenance method guarantees that drones are kept in their best functioning state, so maximising their operational lifetime and providing long-term value to users.[69] Machine learning is essential for processing and analysing the large volumes of data produced by drones throughout their flying missions. AI algorithms could understand data in real-time, deriving practical insights from sensor data, images, and telemetry streams.[70] Machine learning models, when trained on varied datasets, could recognise and categorise objects, distinguish different characteristics of terrain, and detect changes in environmental conditions. These algorithms empower drones to carry out tasks such as land surveying, mapping, and environmental monitoring with exceptional speed and precision.

By using machine learning, drones are able to perform very well in several fields such as surveying, mapping, and environmental monitoring. AI-powered drones have the capability to provide detailed maps, 3D models, and spatial information for a wide range of sectors, including construction, infrastructure, agriculture, and conservation.[71] Drones fitted with machine learning algorithms are capable of precisely capturing topographical data, recognising land features, and producing intricate maps for purposes like as urban planning, infrastructure development, and disaster response in the field of surveying and mapping. These functionalities optimise the process of surveying, decrease expenses, and enhance the precision of geospatial information.

AI-powered drones play a significant role in environmental monitoring by aiding in the evaluation of biodiversity, mapping habitats, and analysing ecosystems. Machine learning algorithms use aerial images to identify changes in plant coverage, track animal populations, and evaluate the influence of human activities on natural ecosystems. Drones help conservation efforts, land management initiatives, and scientific research endeavours by providing immediate and accurate information on environmental dynamics.[72]

Privacy Issue

The combination of AI with drones poses a substantial problem in terms of privacy, namely in relation to the gathering, retention, and analysis of personal information. AI-enabled drones with advanced cameras and sensors have the capacity to gather confidential data on people, such as their actions, conduct, and mobility. This gives rise to apprehensions over unauthorised monitoring, data breaches, and the possibility of personal information being misused. The problem is made more complex by regulatory hurdles, since current privacy rules and regulations may not sufficiently deal with the distinct issues presented by AI-powered drones. Comprehensive guidelines and regulations are necessary to oversee the acquisition, utilisation, and dissemination of data obtained through unmanned aerial vehicles, guaranteeing the

[69] Olawade DB and others, “Using Artificial Intelligence to Improve Public Health: A Narrative Review” (2023) 11 Frontiers in Public Health 1196397

[70] Ibid.

[71] Kaushal H and Bhatnagar A, “Application of Artificial Intelligence in Drones for the Analysis of Agricultural Land Use in the Mining Lease” (2023) 13 International Journal of Environment and Climate Change 1606

[72] Díaz-Delgado R and Mücher S, “Editorial of Special Issue ‘Drones for Biodiversity Conservation and Ecological Monitoring’” (2019) 3 Drones 47

safeguarding of individuals' privacy rights, while still permitting lawful applications such as public safety, environmental monitoring, and scientific research.[73] Comprehensive guidelines and regulations are necessary to oversee the acquisition, utilisation, and dissemination of data obtained by unmanned aerial vehicles (UAVs), guaranteeing the safeguarding of individuals' privacy rights while permitting lawful applications such as public safety, environmental surveillance, and scientific investigation.[74]

The incorporation of AI into drone technology greatly amplifies its monitoring capabilities, giving rise to substantial issues over human rights and privacy. AI-enabled drones could swiftly and accurately analyse large volumes of data captured by their sensors and cameras, which poses significant dangers in terms of systematic breaches of privacy and unauthorised monitoring. This technical innovation in monitoring presents a direct threat to the private rights protected by several national and international laws.

This technical innovation in monitoring is a direct threat to the private rights protected by several national and international laws. Finn and Wright (2016) state that the use of drones for surveillance includes not just recording photographs and videos, but also potentially gathering biometric data, which might be considered more intrusive.[75] The capacity to collect confidential personal information without agreement has been recognised as a possible menace to individual privacy and self-governance.[76]

The extensive monitoring capabilities of AI-enabled drones have the potential to result in privacy infringements that are challenging to identify and avert. The authors contend that the privacy ramifications of these technologies must be addressed via rigorous legal frameworks that can adapt to technological progress.[77]

The GDPR provides a comprehensive structure that encompasses regulations for safeguarding data, which may be relevant to drones that are upgraded with AI. Nevertheless, there are apprehensions over the adequacy of these regulations in tackling the distinct issues presented by these technologies. Pagallo argues that while the GDPR offers a strong structure for safeguarding data, its provisions mostly focus on basic privacy issues and may not completely cover the difficulties presented by drone and AI technology.[78] These technologies provide distinct challenges, such as the collecting of data in real-time, decision-making that is autonomous, and activities that span many jurisdictions. These challenges need more specific legislation. Therefore, it is essential to establish precise legal frameworks that specifically tackle these intricacies, guaranteeing the preservation of privacy and safety in the swiftly advancing realm of drone and AI applications.

In the United States, the reaction has been more divided and lacking unity. The primary focus of the Federal Aviation Administration is on ensuring the safety and seamless integration of drones into the national airspace, with relatively little attention given to privacy concerns. As a result, organisations such as the American Civil Liberties Union (ACLU) have advocated for the

[73] Babatunde FO and others, "A Review on Waste-Wood Reinforced Polymer Matrix Composites for Sustainable Development" (2021) 1107 IOP Conference Series: Materials Science and Engineering 012057

[74] Ibid

[75] Finn RL and Wright D, "Unmanned Aircraft Systems: Surveillance, Ethics and Privacy in Civil Applications" (2012) 28 Computer Law & Security Review 184

[76] Ibid

[77] Clarke R, "The Regulation of Civilian Drones' Impacts on Behavioural Privacy" (2014) 30 Computer Law & Security Review 286

[78] Pagallo U, "The Legal Challenges of Big Data:" (2017) 3 European Data Protection Law Review 36

enactment of comprehensive law that incorporates privacy safeguards specifically tailored to the use of drones. The ACLU supports legislation that mandates law enforcement agencies to get warrants for drone monitoring and implements procedures to guarantee openness in the use of drones in public areas.[79]

Cross Border Privacy Issue

Drone flights across borders might provide additional difficulties for regulatory compliance and enforcement. Global harmonisation of privacy laws and regulations is crucial for ensuring privacy rights and facilitating regulatory cooperation. Integrating AI with drones raises significant safety and security issues about the dependability, resilience, and susceptibility of AI-driven drone systems. Robots using AI for autonomous navigation, obstacle identification, and collision avoidance need thorough testing and verification to establish their reliability in real-world scenarios. Due to the potential hindrance caused by a disorganised collection of regulations, it is imperative to establish an international framework to address issues of drone jurisdiction and facilitate the development and adoption of drone technology. The importance of privacy and legal considerations is equal to that of safety and security when integrating AI with drones. To prevent accidents and abuse, it is necessary to focus on the dependability, robustness, and vulnerability of drone systems that are driven by AI. Thorough testing and validation are crucial for vital AI systems like autonomous navigation, obstacle recognition, and collision avoidance. The purpose of these tests is to verify the algorithms' operation in both expected and unexpected real-world scenarios.

The active involvement of the public sector will significantly facilitate the establishment and upkeep of ethical standards for the integration of AI with drones. Government assistance, in the form of financing and policy suggestions, is necessary for responsible innovation in this sector. An environment that fosters collaboration among academic institutions, corporate sector players, and government organisations may facilitate the exchange of knowledge, transfer of technology, and adherence to regulatory requirements. Partnerships of this kind will cultivate a conducive atmosphere for the emergence of innovative enterprises and revolutionary progress in the capabilities of AI-powered drones. Regulatory frameworks will play a critical role in ensuring the ethical and responsible use of the evolving combination of AI and UAS. Regulatory authorities will have the responsibility of defining comprehensive standards and regulations to govern the development, operation, and deployment of drones powered by AI. These measures must use a holistic approach to address crucial aspects pertaining to safety, security, privacy, and environmental effect. The incorporation of AI capabilities into drone technology necessitates the implementation of regulatory rules to effectively mitigate risks and uphold societal norms. An equilibrium between technological progress and safeguarding fundamental rights and liberties may be attained by meticulously crafted regulations that establish ethical boundaries while fostering the growth of innovation.

Summary

Our current notions of privacy and civil rights are under grave danger due to the unchecked development of AI-powered monitoring systems. The fast growth of algorithms for facial recognition and predictive policing has already broken through the wall of what was once thought

[79] Stanley J and Crump C, *Protecting Privacy from Aerial Surveillance: Recommendations for Government Use of Drone Aircraft: Report* (American Civil Liberties Union 2011)

to be a legitimate expectation of privacy, and it shows no indications of stopping anytime soon. The results of this case study show how bad governance and regulatory systems are at controlling these technologies. With the rapid advancement of technology, public and commercial organisations driven by power and profit have been able to bypass policymakers and civil society, creating an opportunity for exploitation. There is no way to remedy the prejudice and discrimination built into these AI systems; it is a part of the faulty training data and biased goals that define their functioning. Algorithmic oppression masquerading as objectivity often targets marginalised populations. We are on the brink of a great societal shift, where the promise of AI-powered efficiency and security hangs precariously in the balance, while the threat to our cherished liberties looms large. Just saying you believe in ethical ideals isn't enough. There must be immediate, unfaltering responsibility, complete openness, and the sacredness of personal privacy guaranteed. We run the danger of unknowingly slipping into a dystopian nightmare of pervasive monitoring and social control unless we radically refocus these technologies on human rights and civic freedoms. Our options are stark: either we take the initiative to find a middle ground between technological advancement and respect for human dignity, or we give up our most sacred liberties to the impersonal logic of AI. As we balance precariously between the utopian ideal and the totalitarian nightmare, the stakes are greater than they have ever been. If we want to ensure that we keep our fundamental humanity in the future, we must avoid complacency at all costs and act with vigilance and unwavering resolve.

Discussion

The use of AI in surveillance presents a concerning danger to the protection of private rights and civil freedoms. The ubiquitous and sometimes unnoticed presence of these technologies, which able to recognise, monitor, and analyse human behaviour, might lead to a general tendency to censor oneself as people modify their behaviours and utterances due to the fear of being misunderstood by flawed AI systems. The sheer presence of such ubiquitous monitoring equipment hinders the essential aspect of privacy in our life. Although AI monitoring is often praised for its improved security measures, the vast scope and lack of transparency in this technology pose a significant threat to human autonomy and liberties, as it might lead to a society constantly monitored by private entities. As this potent capacity spreads across public and commercial sectors, strong governance is essential to protect privacy as a fundamental principle of democratic society. We must not let unchecked enthusiasm for technology to erode the fundamental freedoms that give our society significance.

AI-driven monitoring poses a significant consequence. The widespread and imperceptible characteristics of AI systems, together with their capacity to recognise and monitor conduct, may have a substantial inhibiting impact on the freedom of privacy. This may occur via the practice of self-censorship, as well as by modifying one's conduct in both public areas and private conversations. The use of technologies such as video surveillance, FRT, drones, and behavioural analysis by both governmental entities and private enterprises presents a risk to the freedom of expression and infringes upon the core tenets of the right to privacy.[80] Mass surveillance is an excessive intrusion on privacy and freedom of speech, while targeted monitoring is only acceptable when it is authorised by law, essential to accomplish a valid objective, and commensurate with the objective sought.

AI applications can be employed to precisely identify and subsequently track individuals across

[80] Article 19, The Global Principles on Protection of Freedom of Expression and Privacy

different devices, within their homes, workplaces, and public spaces. For instance, although personal data is frequently anonymized within datasets, AI can be used to de-anonymize this information and pinpoint individual identities, thus obscuring the distinction between personal and non-personal data that underpins current data protection laws. In a 2015 research, undertaken by scientists at the French Institute for Research in Computer Science, it was shown that machine learning algorithms, along with the usage of just two smartphone apps, can properly identify Over seventy- of mobile phone users within a dataset. Using four apps significantly enhances the probability of successful identification to 95%.[81]

Facial recognition is a method that may be used to monitor and identify persons, potentially changing the way people expect to remain anonymous in public areas. Machine learning techniques have successfully detected around 69% of demonstrators who are using headgear such as hats and scarves to conceal their identities. When shown with photographs of five individuals whose faces were obscured by hats or scarves, the model successfully identified the person in question 56% of the time. By using the ensemble of a hat, scarf, and glasses, the proportion decreased significantly to a just 43%.[82] FRT allows police enforcement to identify persons without having to meet the usual legal requirements, such as demonstrating probable cause or reasonable suspicion. This feature raises significant privacy issues since it enables the possibility of abuse. The technology has the capability to be used in public spaces for the ongoing surveillance and monitoring of individuals' movements, even without their explicit agreement. This has the potential to significantly alter the nature of surveillance and have implications for civil liberties.[83]

Privacy

The complexity of policy discussions on AI and privacy arises from the fact that regulatory and policy discussions include a wide array of applications, uses, and methodologies under the phrase. In debates surrounding AI, there is often a belief that the technology introduces challenges so uniquely new that existing rules, regulations, and standards become obsolete or inadequate. An alternative perspective to that argument is to advocate for the regulation of the technology itself, irrespective of its specific applications and contexts. International human rights law recognises the fundamental entitlement to privacy. The Universal declaration of Human Right stipulates that individuals are entitled to protection against arbitrary or unjustified violations of their privacy, family life, home, or communication. Moreover, each person is entitled to legal protections against such intrusion or attacks.

Various international legal frameworks and standards emphasise the need of protecting personal privacy from unwanted or abusive intrusions. Key legal provisions that safeguard individuals against unjustified intrusion into their privacy, family life, homes, and communication include Article 17(1) of the International Covenant on Civil and Political Rights (“ICCPR”) and Article 11 of the American Convention on Human Rights. According to Article 8(2) of the European Convention on Human Rights, any participation of public authorities in the protection of private and family life must adhere to legal standards. The U.N. Human Rights Committee's General

[81] Achara JP, Acs G and Castelluccia C, “On the Unicity of Smartphone Applications,” *Proceedings of the 14th ACM Workshop on Privacy in the Electronic Society* (ACM 2015)

[82] Singh A and others, “Disguised Face Identification (DFI) with Facial KeyPoints Using Spatial Fusion Convolutional Network,” *2017 IEEE International Conference on Computer Vision Workshops (ICCVW)* (IEEE 2017) <http://dx.doi.org/10.1109/iccvw.2017.193> accessed March 1, 2024

[83] Brown KN, “Anonymity, faceprints, and the Constitution” (2013) 21 Geo. Mason L. Rev, 409

Comment No. 16 on Article 17 of the ICCPR, which was published in 1988, provides further guidance. This declaration asserts that every kind of interference must not only be legal, but also in accordance with the objectives of the Covenant, ensuring that allowed interferences are justifiable within this framework.[84] The "Necessary and Proportionate Principles" were formed in 2013 by a worldwide coalition of civil society, privacy, and technology experts, building upon this basis. The purpose of these principles is to use contemporary digital surveillance techniques in compliance with international human rights standards.[85] Backed by almost 600 groups worldwide, these principles advocate for the meticulous enforcement of human rights standards in the realm of communications surveillance, showing a significant global consensus on this vital issue.

If governments engage in the use or development of AI technologies in a manner that encroaches upon individual privacy rights, it is imperative that these actions undergo a thorough evaluation. This assessment should be rigorously based on three fundamental criteria: legality, ensuring that the actions are in accordance with the law; necessity, verifying that the use of AI is essential for achieving a legitimate aim; and proportionality, confirming that the measures are appropriately balanced with the rights being impacted. This structured approach helps to safeguard personal privacy and uphold the integrity of AI applications within governmental operations. In 2017, the United Nations Human Rights Council expressed concerns regarding the potential discriminatory effects and human rights implications of using automated processes to profile personal data. These concerns encompassed economic, social, and cultural rights.[86] The right to remain anonymous is becoming more acknowledged by international human rights organisations as a right alongside the rights to privacy and freedom of speech. What this means for AI that can recognise people in public, at home, and online is significant. For instance, the United Nations Special Rapporteur on Freedom of Expression has frequently highlighted this link and emphasized that state interference with anonymity, much like any other interference with these rights, must be scrutinized using the three-pronged framework of legality, necessity, and proportionality. This approach ensures that any governmental actions affecting such rights are legally justified, essential for their intended purpose, and appropriately balanced.[87]

Data Protection

Research, development, and use of AI are governed by data protection standards to the degree that personal data is involved. Therefore, data protection standards govern the processing of personal data by AI systems even in the absence of direct mention of AI. Many different regulatory frameworks exist in different parts of the globe, but they all have a common goal: safeguarding personal information. To supersede the EU Directive 95/46/EC, which dealt with the “protection of persons in relation to the processing of personal data and the free movement of such data”, the GDPR was established in 2016 and entered effect in 2018. Increased rights and additional regulations are part of the GDPR. Following technological advancements,

[84] United Nations Human Rights Committee, “General Comment No. 16: Article 17 (Right to Privacy)” (United Nations Human Rights Committee 1998)

[85] International Principles on the Application of Human Rights to Communications Surveillance

[86] United Nations Human Rights Council Resolution on the Right to Privacy in the Digital Age

[87] Office of the United Nations High Commissioner for Human Rights, Report on encryption, anonymity, and human rights framework, “A/HRC/29/32: Report on Encryption, Anonymity, and the Human Rights Framework” (*OHCHR*, May 22, 2015) <https://www.ohchr.org/en/documents/thematic-reports/ahrc2932-report-encryption-anonymity-and-human-rights-framework> accessed February 1, 2024

globalisation, and the EU's constitutionalising of the right to data protection, the GDPR seeks to modernise data protection governance, unite the digital single market, and give individuals control over their data.

Article 13, 14, and 22 of the GDPR impose restrictions on the use of automated decision-making in specific situations. It also mandates that individuals must be informed about the presence of automated decision-making, the reasoning behind it, and the potential impact and expected outcomes of the data processing for the individual. The legislation imposes a general ban on exclusively automated judgements that have legal or other important consequences. Significantly, the GDPR explicitly defines profiling as the automated processing of data for the purpose of analysing or making predictions about persons, as stated in Article 25. This concept recognises that machine learning systems and other profiling methods may generate personal data. In order for companies to successfully manage privacy concerns, it is necessary for them to conduct data privacy impact assessments. They are necessary for applications of artificial intelligence and machine learning that violate users' privacy, which are governed by data protection legislation and present serious hazards that are expected.[88] Data protection is essential for protecting the right to privacy, but it is not capable of addressing all the privacy threats that occur from various AI application. Data protection is restricted to safeguarding data that pertains to a known or identifiable individual, even if it is indirectly related. This does not address the protection of privacy for organisations or other violations of privacy that may not specifically include personal information. While legislation like the GDPR that focus on tracking and machine learning in decision-making are crucial, their influence will likely be restricted to certain instances of AI in automated decision-making or tracking. In addition, data protection regimes sometimes include provisions that exclude national security concerns, therefore restricting rights and protections in important privacy-compromising uses of AI, such as government surveillance.

Data protection policies in nations are complemented with sectoral privacy laws. The ePrivacy Regulation now under consideration in the EU addresses the protection of privacy and confidentiality in communications. Consequently, it has consequences for consumer goods that use AI, such as digital assistants. The French Code that regulates the interactions between the public and administrative entities entitled individuals to receive explanations for decisions made by algorithms within administrative contexts that have an impact on their lives. This legal framework ensures that citizens have the necessary transparency when it comes to understanding how automated decisions are formulated and the basis on which they are applied. It acts as a safeguard, providing individuals with the opportunity to question and understand the rationale behind such decisions, thereby promoting fairness and accountability in public administration.[89] The scope of this clause is wider and more inclusive compared to the requirements of GDPR regarding automated decision-making. Sectoral privacy legislation is significant in governments that lack a comprehensive data protection framework. In US, all uses of AI must adhere to current rules.[90] New York City has proposed legislation to create a taskforce that would assess the city's 'automatic decision systems' with the aim of enhancing their fairness and increasing transparency for examination. This will be relevant to automated algorithms that regulate the allocation of

[88] Safari BA, "Intangible privacy rights: How Europe’s GDPR will set a new global standard for personal data protection." (2016) 47 Seton Hall L. Rev. 809

[89] Malgieri G, “Automated Decision-Making in the EU Member States: The Right to Explanation and Other ‘Suitable Safeguards’ in the National Legislations” (2019) 35 Computer Law &amp; Security Review 105327

[90] US Health Insurance Portability and Accountability Act of 1996

resources such as law enforcement and fire stations. Sectoral regulation may also be useful in tackling specific difficulties of AI, such as autonomous automobiles, that are closely related to a particular environment or domain. Nevertheless, the current sectoral privacy legislation is inadequate in safeguarding individuals against the emerging privacy risks presented by AI applications. AI has the potential to weaken the efficiency of regulations that are limited to certain sectors of the economy due to its impact on data. Strong regulation of medical records sometimes fails to account for the possibility that health data might be obtained, deduced, or anticipated from surfing histories or credit card data.

Implication & Principle

The use of AI technology, especially in the realm of surveillance, need to be in accordance with the fundamental principles delineated in important texts, with a focus on advancing the well-being of both humans and the environment. This alignment emphasises the ethical implementation of AI surveillance systems, guaranteeing that they prioritise the welfare of humans and comply with rigorous ethical principles.

Regarding AI surveillance, it is essential to create and implement technologies in a manner that improves security while safeguarding individual liberties. The principles of AI should prioritise the welfare of all conscious creatures, proposing a surveillance system that respects privacy and dignity. It is crucial to prioritise human well-being in all system designs, including the responsible and beneficial use of AI surveillance technologies for the benefit of society. The deployment of AI should be focused on prioritising the "common good" and the benefit of mankind. In the context of AI surveillance, this entails the implementation of technologies that protect public safety while also being visible, responsible, and subject to monitoring to avoid misuse and guarantee that they do not violate human rights. The Partnership on AI emphasises the significance of maximising the benefits and empowerment for a wide range of individuals. Within the realm of surveillance, this notion may serve as a guiding force for the creation of systems that are fair and unbiased, providing both safety and security to all individuals without any kind of prejudice or discrimination. The European Group on Ethics in Science and New Technologies presents the concepts of "human dignity" and "sustainability" as guiding principles.[91] These principles advocate for the use of AI in all areas to not only uphold individual rights and liberties, but also to ensure long-term sustainability by avoiding behaviours that may cause society divides or environmental damage. By integrating these principles into the implementation of AI surveillance systems, we guarantee that their use is justified, ethical, and advantageous for society. It emphasises the need of maintaining a balance between security and human liberties, guaranteeing that AI functions as a tool for beneficial effects on society rather than an unjustified invasion.[92]

Within the domain of AI surveillance, the ethical concepts of beneficence (doing good) and non-maleficence (avoiding damage) have important implications for human rights and privacy. Although these principles may seem identical on the surface, they really impose separate and essential responsibilities when it comes to the creation and deployment of AI. Ensuring that AI

[91] European Group on Ethics in Science and New Technologies, “Ethics of Information and Communication Technologies Part C: 5 Recommendations” (2012) 17(1) Jahrbuch für Wissenschaft und Ethik

[92] Directorate-General for Research and Innovation, “Ethics of Artificial Intelligence: Statement of the EGE Is Released” (*Research and innovation*, March 9, 2018) <https://research-and-innovation.ec.europa.eu/news/all-research-and-innovation-news/ethics-artificial-intelligence-statement-ege-released-2018-03-09_en> accessed February 1, 2024

technologies contribute favourably to society wellbeing requires intentional measures to uphold beneficence. This may include strengthening safety measures, boosting public services, or using AI technology to effectively handle emergencies. Nevertheless, it is crucial to carefully maintain a delicate equilibrium between this concept and the essential need of non-maleficence, which prioritises the avoidance of unintentional injury, especially when it comes to safeguarding personal privacy and autonomy. The violation of privacy is a significant issue in the context of AI monitoring. The Asilomar Principles, along with other ethical frameworks, emphasise the urgent need of preventing the abuse of AI technologies, which have the potential to cause substantial privacy violations. These principles advocate for AI systems to be created and administered with stringent limitations to avoid them being used as instruments for intrusive surveillance or data manipulation. Moreover, the possible use of AI surveillance technology in a competition for weapons or for iterative self-enhancement presents a substantial menace. These advancements may result in AI systems that function without human control or ethical supervision, hence raising the risk of causing damage. The Partnership on AI emphasises the need of developers to reduce these dangers by ensuring that AI functions within well-defined safety and ethical parameters. The lack of clarity on the party responsible for mitigating damage in AI development, whether it is the developers or the AI systems themselves, highlights a more fundamental problem of autonomy. As AI systems gain greater autonomy, it becomes more difficult to differentiate between the behaviours of the technology and the activities of its developers. This situation emphasises the need of implementing transparent accountability systems to guarantee that both AI developers and the technologies they produce rigorously conform to principles of doing good and avoiding harm. Ultimately, the ethical AI monitoring must be guided by the fundamental principles of beneficence and non-maleficence, but their implementation requires careful attention to detail and constant vigilance. To guarantee that AI upholds and improves human rights while safeguarding privacy, it is necessary to maintain a careful equilibrium, ongoing ethical examination, and a strong structure that precisely outlines the boundaries and obligations of both AI systems and their developers. Adopting this approach is crucial in protecting against the possible negative consequences that these strong instruments may bring.

Conclusion

Summary of Findings

Scope and Mechanisms: What specific AI-driven surveillance technologies are currently prevalent, and what mechanisms do they employ to collect, analyse, and utilize personal data?

An analysis of common AI surveillance systems has shown the many methods by which they invade human privacy. Neural network-based face recognition systems, when integrated with extensive facial databases, have the capability to methodically recognise and monitor persons in various public areas such as transportation hubs, streets, and parks, as well as private residential communities, without any transparency or permission. Predictive policing and risk assessment algorithms that use machine learning on past crime data facilitate biased profiling and excessive monitoring focused on minority populations and poor areas. State-of-the-art smart city systems use advanced technology to combine data from various sensors such as cameras, microphones, and IoT devices. This data is then analysed using AI to continuously monitor public areas for any unusual activity. This monitoring is done with the goal of improving efficiency and ensuring public safety. Significantly, these AI systems have the capacity to secretly gather, combine, and deduce important conclusions from apparently harmless streams of data in both public and private domains, which signifies a major transformation in surveillance capabilities. The vast amount of diverse data combined with AI allows for the creation of detailed personal profiles that may include information on race, political views, and sexual orientation, bypassing the usual expectations of privacy.

Privacy Intrusions: In what ways do these technologies intrude upon personal privacy? This includes examining both the overt and covert methods through which AI systems can invade personal spaces and data sanctuaries without the explicit consent or awareness of the individuals involved.

This project has methodically recorded how AI surveillance technologies enable many forms of privacy violations, both obvious and hidden. Publicly accessible AI analytics, face recognition, and sensor networks are used to identify and track individuals on a large scale, and monitor their behaviour, frequently without their knowledge or agreement. However, much more concerning are the hidden privacy breaches that occur when AI is able to deduce highly revealing personal profiles by uncovering unexpected connections between long-term datasets that merge online activities with offline sensor data. The widespread deployment of sensors in smart cities and the advanced ability of AI to combine information from several sources are progressively eroding any remaining personal privacy in various domains such as our homes, gadgets, automobiles, and public areas. As a result, all our behaviours, relationships, interests, and tendencies are at risk of being thoroughly monitored, measured as complex sets of data, and continuously used for financial gain or societal manipulation, disguised as personalised experiences and public protection.

Legal and Ethical Considerations: Are the existing legal frameworks adequate in addressing privacy breaches facilitated by AI surveillance? Additionally, this question explores whether these legal frameworks are in alignment with ethical considerations surrounding autonomy, consent, and respect for personhood.

Furthermore, it has shown that the secretive and unclear behaviour of AI systems conceals the process by which they invade privacy. As a result, persons are deprived of their fundamental right to control and provide permission over their private, as established in moral philosophy and legal frameworks. The ethical concepts of personal autonomy, human rights, consent, and respect for human dignity are being consistently disregarded as AI surveillance technologies compel us to enter a realm of assumed surveillance and continuous exploitation of data without our free assent.

A comprehensive analysis of the current privacy legislation and data protection rules such as GDPR, CCPA, and HIPAA has shown their insufficiency in effectively tackling the unique difficulties presented by AI surveillance. Although these frameworks provide guidelines regarding purpose limitation, data minimization, user consent, and subject rights, they are not effective in controlling advanced techniques such as synthetic data generation, inferential analytics, multimodal sensor fusion, and opaque model reasoning that enable AI's surveillance capabilities. There are troubling discrepancies between the moral principles embedded in these ethical-legal frameworks, which focus on individual consent, human agency, and privacy self-determination, and the intrusive nature of AI surveillance systems that undermine these ideals by operating without significant transparency or choice. The act of normalising ubiquitous surveillance goes against the ethical principles of human dignity, democratic liberties, and open societies.

Comparative Analysis: How do the impacts of AI surveillance on privacy vary across different contexts and jurisdictions? For instance, the approach to privacy and surveillance differs significantly between regions like the European Union, which enforces the GDPR, and other regions with less stringent privacy protections.

This study has also thoroughly examined how the effects of AI surveillance on privacy rights vary differently in various legal regimes, depending on their goals for data governance. The European Union's GDPR does establish certain baseline protections by mandating organizational practices centred around data minimization principles, purpose limitation requirements, privacy impact assessments, and consent management workflows. Nevertheless, the extensive national security exemptions still allow unimpeded state monitoring by means of exchanging data via covert communication channels. Conversely, the absence of a comprehensive federal privacy legislation in the United States has led to a fragmented system of self-regulation and corporate data policies that are primarily focused on consumer profiling, behavioural advertising, and predictive analytics, often at the expense of customer privacy. The capacity of IT firms to accumulate large amounts of user data and use it with advanced AI models makes current sector-specific regulations like HIPAA insufficient.

Future Implications: What are the potential long-term effects of AI-driven surveillance on societal norms and individual behaviours regarding privacy? This question aims to understand if and how the normalization of surveillance might alter fundamental human interactions and expectations concerning privacy.

The most alarming discovery pertains to the enduring consequences of AI monitoring in reconfiguring society norms, cultural attitudes, and essential human behaviours concerning privacy and personal liberties. If AI monitoring systems are allowed to develop without restrictions, their widespread presence and constant surveillance may lead to people unconsciously censoring themselves and conforming to societal norms as they gradually internalise the constant scrutiny they are under. Communities that are marginalised and subjected to excessive monitoring will proactively withdraw from participating in society. The pervasive scrutiny of AI systems may push individuals to proactively alter their behaviours, consumption habits, and life decisions in response to speculative scoring systems that are beyond their understanding. The widespread adoption of AI-enabled mass surveillance and the commercialization of personal data as the societal norm presents a significant threat to individual human autonomy, identity, privacy, and the inherent dignity of being human. As data becomes more valuable, people may find themselves being monitored, anticipated, and used as subjects in emerging systems of algorithmic control.

To put it simply, our study presents a concerning prediction - AI-driven surveillance technologies are causing a crucial turning point that has the potential to permanently upset the balance of power between institutions and people in terms of digital privacy rights and civil liberties. Their powerful ability to extensively observe, continuously measure, and constantly exploit every aspect of human life for mysterious intentions has the potential to severely weaken individual control, democratic liberties, and the ethical principles that shape human society. If immediate action is not taken to establish effective governance and technical measures that enforce strict safeguards, uphold ethical boundaries, and protect privacy as an inviolable human right, unregulated AI surveillance poses a significant risk of gradually normalising a dystopian existence characterised by pervasive and inescapable oppressive monitoring. The most important task that will shape the direction of society in the age of AI is to find a balance that promotes responsible technology advancement while also strengthening regulations to protect personal privacy. Choosing to be complacent or acquiescent is not a practical choice. Instead, it is ethically necessary to take proactive and principled action, guided by multidisciplinary foresight, in order to protect our digital freedoms from being unintentionally compromised by the pursuit of computational dominance.

Conclusions

The rapid advancement of AI-driven surveillance technology has led us to a critical juncture about the future of privacy rights in the digital age. This thorough examination has shown how the revolutionary powers of AI systems to continuously observe, measure, and predictively take advantage of the little details of human life offers an unparalleled technological disruption. Without restraint, the overwhelming computational power of AI surveillance poses a serious threat to human autonomy, erodes personal dignity, and normalises a state of constant surveillance. This would eliminate our reasonable expectations of privacy, serving the interests of institutional power, security theatre, and the profit-driven motives of surveillance capitalism. Nevertheless, yielding to such a bleak and oppressive path would destroy the ethical principles and democratic ideals upon which contemporary societies have been built. Therefore, based on the insights gained from this research, it is crucial to strike a delicate equilibrium between the responsible advancement of AI technologies and the protection of privacy, which is both a basic human right and a crucial social obligation. There is an urgent need for strict governance structures that include privacy safeguards into the fundamental architectural design of AI surveillance systems. Simply adding AI capabilities to current privacy regulations is insufficient to control their powerful capacity to systematically undermine privacy standards and civil rights. Establishing strong guidelines regarding data handling practices, model transparency, human oversight, and explicit consent workflows is crucial before AI systems become widespread and deeply ingrained. This requires collaboration among policymakers, AI developers, domain experts, and civic rights groups. Legislative instruments should require the use of privacy-preserving computing paradigms such as secure enclaves, differential privacy, and cryptographic anonymization methods as essential protections. It is crucial to prioritise privacy as an absolute need from the beginning of the design process to properly and fairly achieve the significant socioeconomic advantages of AI. Adopting a privacy-focused approach guided by ethical principles and legal design principles may help avoid harmful conflicts between innovation and regulation in the future. It can allow AI systems to be fine-tuned for measurable public service standards, responsibility for errors, and equitable results, without becoming entangled in exploitative surveillance capitalism methods that undermine human rights. At a fundamental level, we need to collectively adopt a human-centred perspective in which technology advancements are aligned with and subordinate to the moral importance and protection of human rights, individual independence, and democratic liberties. Compromising individual privacy in the pursuit of computing efficiency, security measures, or economic convenience would erode the fundamental principles of personal freedom that are integral to our human society. Diminishing expectations for privacy would further exacerbate generational inequities arising from pre-existing social prejudices, oppressions, and power disparities. Further vulnerability and alienation will be imposed onto marginalised communities that are already exposed to excessive scrutiny. An escalating series of privacy violations might lead mankind into a suffocating digital dystopia devoid of dissent, independent thinking, and personal identity. The imminent dangers of forced scoring systems, established social stratifications, and widespread automated discrimination are too harmful to ignore. AI monitoring systems that amplify confirmation bias and engage in demographic kaleidoscoping have the potential to undermine the societal progress that has been achieved, by further dividing different groups and destroying social cohesion. Ultimately, while technical growth is crucial for the progression of humanity, it must never exceed our moral and ethical development as a species. The delicate equilibrium between AI advancement and privacy rights is precarious. We must carefully and intentionally guide the direction in which science and innovation go, ensuring that they continue to be empowering and enriching forces, rather than becoming instruments of societal manipulation, coercion, and suppression. By establishing proactive and enforceable governance guardrails via collaborative foresight, we can effectively use the potential of AI for the overall good of mankind. At the same time, we can ensure that our personal privacies, identities, and human rights are protected and inviolable. Ensuring and maintaining this equilibrium is the utmost responsibility and moral duty we owe not just to the current generation but to the liberation of all future generations. It is imperative that we steadfastly protect personal privacy as inviolable, since it is the foundation of human dignity, civil freedoms, and the highest aspirations of civilised communities. Failing to fulfil this responsibility would only result in future generations being trapped in a dehumanised society where technical tyranny is disguised as progress.

Limitation

This article offers a comprehensive analysis of the privacy issues linked to surveillance technologies that are driven by AI. Nevertheless, it is crucial to acknowledge that there are some constraints that must be acknowledged and dealt with. Given the rapid pace of technology advancement, there is a potential for any research to become obsolete prior to its publication. This is especially true in the domain of AI, which is constantly progressing with novel talents and uses. However, the aim of this research was to focus on fundamental concepts and frameworks that may be used as a foundation for assessing future advancements.

Acquiring a complete and inclusive sample of papers from all nations is intrinsically difficult because of the global nature of the task. Unforeseen deficiencies in data gathering may have emerged as a result of issues pertaining to accessibility, linguistic barriers, and the absence of openness in some governmental or company activities. To tackle this problem, we reached out to a diverse range of sources from various regions and used data triangulation wherever possible.

The accurate understanding and projection of long-term societal consequences and changes in behaviour that arise from the widespread acceptance of AI surveillance present challenges. These phenomena are undergoing changes and their whole ramifications may not be apparent now. In this research, while theoretical viewpoints and ethnographic observations were included, it was unavoidable that some conjecture about future events would be included. Ongoing monitoring and reassessment of effect assessments will be necessary.

Moreover, this research specifically examines the surveillance of AI with regards to the protection of private rights and civil liberties. While acknowledging their significance, this research did not provide a comprehensive assessment of all the interdependencies with other human rights, such as freedom of expression and socioeconomic rights. Further analysis of intersectional human rights in the future might provide valuable further research.

Furthermore, biases and blind spots are intrinsic weaknesses in any qualitative research. While the author attempted to maintain objectivity, their own viewpoint, experiences, and philosophical convictions may have inadvertently influenced the analysis and interpretation. It is prudent to promote interdisciplinary research and publicly recognise any boundaries that have not been identified.

While document research and book study are extensive, they may not provide as deep an insight of real-life situations as ethnographic fieldwork undertaken among the populations directly impacted.

Notwithstanding these limitations, this article provides a robust and all-encompassing structure for policymakers, engineers, and civil society to tackle the challenges posed by AI monitoring. This initiative aims to provide a solid foundation for future research on the compatibility of technological breakthroughs with the protection of fundamental human rights and democratic ideals. It does this via a transparent methodology and an interdisciplinary approach.

Future Research

Affective Computing and Emotion Recognition: The rapidly growing area of affective computing, which focuses on identifying and understanding human emotions via the use of several sensors, raises substantial privacy issues. Subsequent investigations should thoroughly examine the ethical implications of using these technologies to monitor emotional states and create profiles based on psychological and emotional characteristics without obtaining consent. Establishing ethical principles and consent frameworks is crucial in order to safeguard persons from unauthorised psychological monitoring.

Neural Sensor Interfaces and Brain-Computer Interaction: The progress of neural interfaces that enable direct connection between the brain and computers has the potential to bring about considerable advantages, especially in the field of assistive technology. Nevertheless, these interfaces also pose a potential threat to mental privacy by gaining access to cognitive information such as thoughts and memories. Research should establish strong and reliable legal and ethical structures to protect cognitive data and maintain the confidentiality of mental information.

The advancement of deepfake technologies, powered by generative adversarial networks, presents significant risks such as spreading false information, stealing identities, and exploiting individuals without their consent. Future research should prioritise improving detection techniques and implementing provenance tracking systems to avoid the exploitation of hyper-realistic synthetic media.

Privacy-Preserving AI Architecture Paradigms: There is a crucial need for ongoing advancement in privacy-preserving AI technology. Conducting studies on cryptographic enclaves, safe computing protocols, federated learning, and differential privacy is crucial. The objective of these technologies is to empower AI systems to analyse data while intrinsically safeguarding user privacy and data ownership.

The development and improvement of policy responses and regulatory frameworks on a worldwide scale are essential as AI technologies continue to impact many industries. Future research should investigate methods to align data governance norms, promote international collaboration, and integrate AI ethics into legislative efforts to mitigate privacy erosion and territorial arbitrage.

There is an urgent need for multidisciplinary research to evaluate the effects of AI surveillance technology on human rights, particularly in marginalised populations. Creating frameworks that include intersectional assessments of gender, ethnicity, accessibility, and socioeconomic variables can help establish fair and inclusive mechanisms for governing AI.

AI Existential Safety and Human Agency Preservation: As AI becomes more capable of achieving Artificial General Intelligence, the dangers of existential threats that might undermine human control and decision-making grow more significant. The research should prioritise the development of ways to safeguard human autonomy, mitigate the dangers of instrumental convergence, and guarantee that advanced AI systems give utmost importance to human privacy, freedoms, and ethical principles.

References

Achara JP, Acs G and Castelluccia C, "On the Unicity of Smartphone Applications," Proceedings of the 14th ACM Workshop on Privacy in the Electronic Society (ACM 2015)

Adjabi I and others, "Past, Present, and Future of Face Recognition: A Review" (2020) 9 Electronics 1188

AlMahamid F and Grolinger K, "Autonomous Unmanned Aerial Vehicle Navigation Using Reinforcement Learning: A Systematic Review" (2022) 115 Engineering Applications of Artificial Intelligence 105321

Almeida D, Shmarko K and Lomas E, "The Ethics of Facial Recognition Technologies, Surveillance, and Accountability in an Age of Artificial Intelligence: A Comparative Analysis of US, EU, and UK Regulatory Frameworks" (2021) 2 AI and Ethics 377

Apene OZ, Blamah NV and Aimufua GIO, "Advancements in Crime Prevention and Detection: From Traditional Approaches to Artificial Intelligence Solutions" (2024) 2 European Journal of Applied Science, Engineering and Technology 285

Babatunde FO and others, "A Review on Waste-Wood Reinforced Polymer Matrix Composites for Sustainable Development" (2021) 1107 IOP Conference Series: Materials Science and Engineering 012057

Bacchini F and Lorusso L, "Race, Again: How Face Recognition Technology Reinforces Racial Discrimination" (2019) 17 Journal of Information, Communication and Ethics in Society 321

Badillo M, "Navigating the Complexities of Facial Recognition for Public Security in Latin America" (International Bar Association, May 9, 2023) <https://www.ibanet.org/facial-recognition-security-latin-america> accessed March 1, 2024

Barker L and others, "IDC FutureScape: Worldwide Smart Cities and Communities 2024 Predictions" (IDC 2023)

Blanchard A and Taddeo M, "The Ethics of Artificial Intelligence for Intelligence Analysis: A Review of the Key Challenges with Recommendations" (2023) 2 Digital Society 1

Brown KN, "Anonymity, faceprints, and the Constitution" (2013) 21 Geo. Mason L. Rev, 409

Brundage M and others, "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation" (2018) ArXiv

Centre for Information Policy Leadership, "Artificial Intelligence and Data Protection: Delivering Sustainable AI Accountability in Practice" (2018)

Clarke R, "Information technology and dataveillance" (1988) 31 Communications of ACM 498

Clarke R, "The Regulation of Civilian Drones' Impacts on Behavioural Privacy" (2014) 30 Computer Law & Security Review 286

Connor BT and Doan L, "Government and Corporate Surveillance: Moral Discourse on Privacy in the Civil Sphere" (2019) 24 Information, Communication & Society 52

Day J, "What Is Wrong About Public Surveillance? I Liberties.Eu" (Liberties.eu, April 25, 2023) <https://www.liberties.eu/en/stories/public-surveillance/44774> accessed February 1, 2024

Dayo-Olupona O and others, "Adoptable Approaches to Predictive Maintenance in Mining Industry: An

Overview" (2023) 86 Resources Policy 104291

Deloitte, "Surveillance and Predictive Policing Through AI" Deloitte <https://www.deloitte.com/global/en/Industries/government-public/perspectives/urban-future-with-a-purpose/surveillance-and-predictive-policing-through-ai.html> accessed February 1, 2024

Díaz-Delgado R and Mücher S, "Editorial of Special Issue 'Drones for Biodiversity Conservation and Ecological Monitoring'" (2019) 3 Drones 47

Directorate-General for Research and Innovation, "Ethics of Artificial Intelligence: Statement of the EGE Is Released" (Research and innovation, March 9, 2018) <https://research-and-innovation.ec.europa.eu/news/all-research-and-innovation-news/ethics-artificial-intelligence-statement-ege-released-2018-03-09_en> accessed February 1, 2024

Donahoe E, Metzger M and Wainscott K, "Global Digital Policy Snapshot: Protecting Human Rights in the Regulation of Facial Recognition Technology" (Stanford University Cyber Policy Center 2020)

ESI ThoughtLab, "Smart City Solutions for a Riskier World" (ESI ThoughtLab 2021)

European Data Protection Supervisor, "Preliminary Opinion on Privacy by Design" (European Data Protection Supervisor, 2018)

European Group on Ethics in Science and New Technologies, "Ethics of Information and Communication Technologies Part C: 5 Recommendations" (2012) 17(1) Jahrbuch für Wissenschaft und Ethik 217

Ezeigweneme CA and others, "Review of telecommunication regulation and policy: comparative analysis USA and Africa" (2024) 5 Computer Science & IT Research Journal 81

Feldstein S, The Global Expansion of AI Surveillance (Carnegie Endowment for International Peace 2019)

Felluga D, "Modules on Foucault: On Panoptic and Carceral Society." Introductory Guide to Critical Theory (Purdue 2011)

Findlay M, Ong LM and Zhang W, Elgar Companion to Regulating AI and Big Data in Emerging Economies (Edward Elgar Publishing 2023)

Finn RL and Wright D, "Unmanned Aircraft Systems: Surveillance, Ethics and Privacy in Civil Applications" (2012) 28 Computer Law & Security Review 184

Fleischer RS, "Bias in, Bias out: Why Legislation Placing Requirements on the Procurement of Commercialized Fascial Recognition Technology Must be Passed to Protect People of Color" (2020) 50 Pub. Cont. L.J. 63

Fontes C and others, "AI-Powered Public Surveillance Systems: Why We (Might) Need Them and How We Want Them" (2022) 71 Technology in Society 102137

Fyfe NR, Images of the Street: Planning, Identity, and Control in Public Space (Routledge 1998)

Grodzinsky FS and Tavani HT, "Privacy in 'the Cloud'" (2011) 41 ACM SIGCAS Computers and Society 38

Haggerty KD and Ericson RV, "The Surveillant Assemblage" (2000) 51 The British Journal of Sociology 605

Himeur Y and others, "Face Mask Detection in Smart Cities Using Deep and Transfer Learning: Lessons Learned from the COVID-19 Pandemic" (2023) 11 Systems 107

Hirose M, "Privacy in public spaces: The reasonable expectation of privacy against the dragnet use of facial recognition technology" (2017) 49 Connecticut Law Review 1591

Information Commissioner's Office, "Big Data, Artificial Intelligence, Machine Learning and Data Protection" (Information Commissioner's Office 2017)

Ioannou A and Tussyadiah I, "Privacy and Surveillance Attitudes during Health Crises: Acceptance of Surveillance and Privacy Protection Behaviours" (2021) 67 Technology in Society 101774

Kaur P and others, "Facial-Recognition Algorithms: A Literature Review" (2020) 60 Medicine, Science and the Law 131

Kaushal H and Bhatnagar A, "Application of Artificial Intelligence in Drones for the Analysis of Agricultural Land Use in the Mining Lease" (2023) 13 International Journal of Environment and Climate Change 1606

Koskela H, "'The Gaze without Eyes': Video-Surveillance and the Changing Nature of Urban Space" (2000) 24 Progress in Human Geography 243

libertés FranceC nationale de l'informatique et des, How Can Humans Keep the Upper Hand?: The Ethical Matters Raised by Algorithms and Artificial Intelligence: Report on the Public Debate Led by the French Data Protectional Authority, CNIL, as Part of the Ethical Discussion Assignment Set by the Digital Republic Bill: December 2017 (CNIL 2018)

Lyon D, Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination (Psychology Press 2003)

Lyon D, Surveillance Society: Monitoring Everyday Life (Open University Press 2001)

Lyon D, Surveillance Studies: An Overview (Polity 2007)

Lyon D, "Surveillance Capitalism, Surveillance Culture and Data Politics 1" Data Politics (Routledge 2019)

Malgieri G, "Automated Decision-Making in the EU Member States: The Right to Explanation and Other 'Suitable Safeguards' in the National Legislations" (2019) 35 Computer Law & Security Review 105327

Manheim K and Kaplan L, "Artificial intelligence: Risks to privacy and democracy" (2019) 21 Yale Journal of Law and Technology 106

Margulis ST, "On the Status and Contribution of Westin's and Altman's Theories of Privacy" (2003) 59 Journal of Social Issues 411

McClellan E, "Facial Recognition Technology: Balancing the Benefits and Concerns" (2020) 15 Journal of Business & Technology Law 2

McGrath JE, Loving Big Brother: Performance, Privacy and Surveillance Space (Psychology Press 2004)

Nwankwo CO and others, "Reviewing the Role of AI in Drone Technology and Applications" (2024) 5 Computer Science & IT Research Journal 741

Nguyen FQ, "The Standard for Biometric Data Protection" (2018) 7 Journal of Law & Cyber Warfare 1

Office of the United Nations High Commissioner for Human Rights, Report on encryption, anonymity, and human rights framework, "A/HRC/29/32: Report on Encryption, Anonymity, and the Human Rights Framework" (OHCHR, May 22, 2015) <https://www.ohchr.org/en/documents/thematic-reports/ahrc2932-report-encryption-anonymity-and-human-rights-framework> accessed February 1, 2024

Ogundairo O and others, "Review on maldi mass spectrometry and its application in clinical research" (2023) 3 International Medical Science Research Journal 108

Olawade DB and others, "Using Artificial Intelligence to Improve Public Health: A Narrative Review" (2023) 11 Frontiers in Public Health 1196397

Ong R, "Privacy and Personal Information Protection in China's All-Seeing State" (2023) 31 International Journal of Law and Information Technology 349

Pagallo U, "The Legal Challenges of Big Data:" (2017) 3 European Data Protection Law Review 36

Papageorgiou M, Can M and Vieira A, "China as a Threat and Balancing Behavior in the Realm of Emerging Technologies" (2024) Chinese Political Science Review

Penfold R, "Review of Surveillance Society: Monitoring Everyday Life; Everyday Surveillance: Vigilance and Visibility in Post Modern Life, by D. Lyon & W. Staples" (2002) 42(1) The British Journal of Criminology 222

Read A, 'Increased Uptake of Surveillance Technologies during COVID-19' (2020) 22 European Journal of Law Reform 448

Rigby MJ, "Ethical Dimensions of Using Artificial Intelligence in Health Care" (2019) 21 AMA Journal of

Ethics 121

Rodrigues R, “Legal and human rights issues of AI: Gaps, challenges and vulnerabilities” (2020) 4 Journal of Responsible Technology 100005

Safari BA, "Intangible privacy rights: How Europe’s GDPR will set a new global standard for personal data protection." (2016) 47 Seton Hall L. Rev. 809

Sætra H, “Freedom under the gaze of Big Brother: Preparing the grounds for a liberal defence of privacy in the era of Big Data” (2019) 58 Technology in Society 101160

Singh A and others, “Disguised Face Identification (DFI) with Facial KeyPoints Using Spatial Fusion Convolutional Network,” 2017 IEEE International Conference on Computer Vision Workshops (ICCVW) (IEEE 2017) <http://dx.doi.org/10.1109/iccvw.2017.193> accessed March 1, 2024

Sloly P, “Emerging Tech That Can Make Smart Cities Safer” (Deloitte Canada, October 3, 2018) <https://www2.deloitte.com/ca/en/pages/public-sector/articles/emerging-tech-smart-cities-safer.html> accessed February 1, 2024

Stanley J and Crump C, Protecting Privacy from Aerial Surveillance: Recommendations for Government Use of Drone Aircraft: Report (American Civil Liberties Union 2011)

Supriyadi D, 'The Regulation of Personal and Non-Personal Data in the Context of Big Data' (2023) 3 Journal of Human Rights, Culture and Legal System 33

Tullu A and others, “Machine Learning Approach to Real-Time 3D Path Planning for Autonomous Navigation of Unmanned Aerial Vehicle” (2021) 11 Applied Sciences 4706

United Nations Human Rights Committee, “General Comment No. 16: Article 17 (Right to Privacy)” (United Nations Human Rights Committee 1998)

Van den Hoven van Genderen R, “Privacy and Data Protection in the Age of Pervasive Technologies in AI and Robotics” (2017) 3 European Data Protection Law Review 338

Van Dijck J, “Datafication, Dataism and Dataveillance: Big Data Between Scientific Paradigm and Ideology” (2014) 12 Surveillance & Society 197

Vayena E, Blasimme A and Cohen IG, “Machine Learning in Medicine: Addressing Ethical Challenges” (2018) 15 PLOS Medicine e1002689

Vincent J, 'France is using AI to check whether people are wearing masks on public transport' (The Verge, 2020)

Yao Y, “Research on facial recognition system based on deep learning” (2024) 34 Applied and Computational Engineering 232

Legislation and Treaties

American Convention on Human Rights.

European Convention on Human Rights

General Date Protection Regulation

International Covenant on Civil and Political Rights

International Principles on the Application of Human Rights to Communications Surveillance

United Nations Human Rights Council Resolution on the Right to Privacy in the Digital Age

The Global Principles on Protection of Freedom of Expression and Privacy

The Universal declaration of Human Right

US Health Insurance Portability and Accountability Act of 1996